ОБСЕ
Организация по безопасности
и сотрудничеству в Европе
Офис программ в Нур-Султане

КРИМИНАЛИСТИКАДАҒЫ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

халықаралық ғылыми-практикалық конференциясының материалдары

2021 жылғы 29 қазан

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Материалы международной научно-практической конференции

29 октября 2021 г.

INNOVATIVE TECHNOLOGIES IN CRIMINALISM

Materials of the international scientific and practical conference

October 29, 2021

ҚАРАҒАНДЫ 2021 КАРАГАНДА

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
Ішкі істер министрлігі
Бәрімбек Бейсенов атындағы
Қарағанды академиясы

РЕСПУБЛИКА КАЗАХСТАН
Министерство внутренних дел
Карагандинская академия
имени Б. Бейсенова

КРИМИНАЛИСТИКАДАҒЫ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

халықаралық ғылыми-практикалық конференциясының материалдары

2021 жылғы 29 қазан

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Материалы международной научно-практической конференции

29 октября 2021 г.

INNOVATIVE TECHNOLOGIES IN CRIMINALISM

Materials of the international scientific and practical conference

October 29, 2021

Қарағанды • 2021 • Караганда

УДК 351/354
ББК 67.401.213
И 90

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының ғылыми кеңесінің шешімі бойынша басылып шығарылады.

Публикуется по решению ученого совета Карагандинской академии Министерства внутренних дел Республики Казахстан им. Б. Бейсенова.

Published by the decision of the Academic Council of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov.

И90

Криминалистикадағы инновациялық технологиялар: Халықаралық ғылыми-практикалық конференциясының материалдары. — Қарағанды: Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы, 2021. — 222 б. = Инновационные технологии в криминалистике: Материалы международной научно-практической конференции. — Караганда: Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2021. — 222 с. = Innovative technologies in criminalism: Materials of the international scientific and practical conference. — Karaganda: Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenova, 2021. — 222 p.

Басылым «Криминалистикадағы инновациялық технологиялар» халықаралық ғылыми-практикалық онлайн-конференциясының материалдарынан тұрады.

Форумның жұмысына белгілі ғалым-заңгерлер, жоғары оқу орындарының оқытушылары, Қазақстан, Ресей, Беларусь, Әзірбайжан, Өзбекстан, Украина, Тәжікстан, Қырғызстан Республикасының Құқық қорғау органдарының практикалық қызметкерлері, сондай-ақ ЕҚЫҰ және Интерпол сарапшылары, Үндістан, Моңғолия, Палестина жоғары оқу орындары мен сараптамалық мекемелерінің өкілдері қатысты.

Практикадағы қызметкерлерге, жоғары оқу орындарының ғылыми қызметкерлеріне, оқытушыларына, курсанттарына, магистранттарына, докоранттарына арналған.

Издание содержит материалы международной научно-практической онлайн-конференции «Инновационные технологии в криминалистике».

В работе форума приняли участие известные ученые-юристы, преподаватели вузов, практические работники правоохранительных органов Казахстана, России, Беларуси, Азербайджана, Узбекистана, Украины, Таджикистана, Кыргызской Республики, а также эксперты ОБСЕ и Интерпола, представители вузов и экспертных учреждений Индии, Монголии, Палестины.

Адресовано практическим работникам, научным сотрудникам, преподавателям, курсантам, магистрантам, докторантам высших учебных заведений.

The publication contains materials of the international scientific and practical online conference «Innovative technologies in forensic science».

The forum was attended by well-known legal scholars, university professors, practitioners of law enforcement agencies of Kazakhstan, Russia, Belarus, Azerbaijan, Uzbekistan, Ukraine, Tajikistan, the Kyrgyz Republic, as well as experts from the OSCE and Interpol, representatives of universities and expert institutions from India, Mongolia, Palestine.

Addressed to practitioners, researchers, teachers, cadets, undergraduates, doctoral students of higher educational institutions.

ISBN 978-601-7589-52-3

УДК 351/354
ББК 67.401.213

ПРИВЕТСТВЕННЫЕ СЛОВА

Тургумбаев Е. З.,
министр внутренних дел Республики Казахстан,
генерал-лейтенант полиции, кандидат юридических наук

Құрметті халықаралық
конференцияға қатысушылар!

Қылмыспен күрес, қоғамдық тәртіпті сақтау — полиция қызметкерлерінің басты міндеті.

Бүгінде заманауи технологиялар жыл сайын дамуда.

Қылмысты болдырмау және оны ашу үшін осы технологияларды қолдану — ішкі істер органдарының басты бағытына айналды.

Мемлекет басшысы Қасым-Жомарт Кемелұлы Тоқаев өзінің халыққа Жолдауында мемлекеттік секторды одан әрі цифрландыру міндеттерін қойды.

Қазір ішкі істер министрлігі жаппай технологияны енгізуді қолға алды.

Алдымен ішкі істер органдары көрсететін онлайн мемлекеттік қызмет түрлері 95 пайызға жетті.

Қылмыстық істерді тергеу **80 пайыз** электронды форматқа ауысты, жылдың аяғына дейін **100 пайыз** болады.

Көшелер мен қоғамдық орындардағы бейнекамералар саны **100 мыңға** жетті.

Азаматтар смартфондарына **«102 қосымшасын»** жүктеу арқылы Жедел басқару орталығына тікелей қосылуға мүмкіндік алды. Қазір бұл қосымшаны 50 мыңға жуық адам қолданады.

Бұл — жасалған жұмыстардың бір парасы ғана.

Нәтижесінде, азаматтармен байланыс электронды форматқа ауысты.

Сыбайлас жемқорлық саны 3 жыл ішінде 2 есе азайды.

Азаматтардың конституциялық құқықтарын қорғау сапасы артты.

Жедел криминалистика саласына білікті IT-мамандарын тартуға септігін тизуде.

Құрметті қонақтар мен әріптестер!

Бүгінгі ғылыми-практикалық конференцияның тақырыбы **«Криминалистикадағы инновациялық технологиялар».**

Ішкі істер органдарының басты мақсаты – халық сенімі.

Сондықтан заманауи технологияларды полиция жұмысына енгізу — біз үшін өзекті мәселе.

Алдағы диалог — криминалистикада цифрлық технологияларды енгізуге ықпал етеді деп ойлаймын.

Жұмыстарыңызға сәттілік тілеймін.

Сейдгапбаров К. С.,
заведующий отделом правоохранительной системы
Совета Безопасности Республики Казахстан

Уважаемые участники конференции, системные изменения, произошли в правоохранительной сфере за 30 лет независимости, составляют единое историческое явление. Их главным предназначением является переход от тоталитарной системы к демократическому государству, главная ценность которого — человек, его права и свободы.

Конечно, такой переход не мог произойти одномоментно, кто застал 90-ые годы прошлого века, прекрасно помнит разгул криминала, рэкет, бандитизм, тотальное недоверие к судам и правоохранительным органам. В тот период главной задачей было обеспечение хотя бы минимального уровня безопасности граждан, чтобы они не боялись ходить по улицам, вести бизнес.

Благодаря мудрой политике Елбасы необходимые для уголовно-правовой сферы реформы произошли планомерно, но в то же время неуклонно. Практически с нуля выстроена судебная система, подготовлены судейские кадры новой формации, и только после этого в уголовном процессе стали появляться элементы судебного контроля. Серьезные изменения произошли и в разграничении полномочий, и на досудебных стадиях уголовного процесса.

Параллельно развивались технологии, и это тоже нашло отражение в реформах. Так, с 2018 г. в Уголовно-процессуальном кодексе официально закреплен электронный формат расследования уголовных дел. В рамках этой работы создана программа «Е – уголовное дело», применение которой исключает саму вероятность подмены материалов, различного рода подчисток.

Очевидно, что за годы Независимости правоохранительная система существенно трансформировалась, и все это было сделано без ущерба для борьбы с преступностью. За последние 25 лет число убийств, тяжких телесных повреждений и разбоев снизилось в несколько раз. Если в 1996 г. было совершено 2 625 убийств, то в 2020 г. — 824, или в 3 раза меньше, тяжких телесных повреждений — в 3, а разбоев — в 12 раз меньше.

В целом, если взглянуть на изменения, которые происходили за эти годы, уместнее говорить о вехах одного большого пути. Стратегический курс этих фундаментальных изменений заложен Первым Президентом РК Н. А. Назарбаевым. В полном соответствии с ним Главой государства К.-Ж. Токаевым поставлены дальнейшие ориентиры, одним из которых является модернизация правоохранительной деятельности в соответствии с самыми передовыми практиками.

В этом контексте особого внимания заслуживает вопрос технологического обновления, и именно здесь на первый план выходит модернизация криминалистики. Стремительное развитие технологий порождает для правоохранительной системы одновременно и новые вызовы, и новые возможности. От того,

насколько мы преуспеем в реализации этих возможностей, зависит результат работы по противодействию преступности.

Поэтому важность и актуальность данной конференции, организованной Министерством внутренних дел, не вызывает никаких сомнений. Символично и то, что это мероприятие проводится под эгидой Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова, которая на протяжении десятилетий по праву считается флагманом ведомственной науки и образования. Представительный состав участников вселяет большую надежду на то, что конференция станет фундаментом серьезнейших научных достижений и заделом целого спектра практических новаций.

Особенно радует, что традиционные направления криминалистической техники, тактики и методологии будут сегодня рассмотрены сквозь призму самых современных тенденций, таких как активное проникновение в нашу действительность цифровых технологий, искусственного интеллекта, фото- и видеофиксации. В связи с этим я хотел бы выразить искреннюю благодарность руководству МВД за организацию данной конференции, а всем ее участникам пожелать успешной и плодотворной работы.

Сабитов Н. М.,
заместитель начальника Службы специальных прокуроров
Генеральной прокуратуры Республики Казахстан

Сәлеметсіздер ме,
құрметті әріптестер!

От лица руководства Генеральной прокуратуры Республики Казахстан и от себя лично рад приветствовать Вас на международной научно-практической конференции, посвященной вопросам применения инновационных технологий в криминалистике. Преступления, совершаемые в сфере высоких технологий, — это серьезный повод для беспокойства на фоне глобальной цифровизации всех сфер жизнедеятельности человека. Противоправные действия среди современных технических новинок влияют на наиболее важные охраняемые законом общественные отношения в сфере прав, интересов личности, общества и безопасности государства.

Незаконное вмешательство в информационную систему способно вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и физическим вредом гражданам. К счастью, наука и практика не стоят на месте. В нашем арсенале появляются новые методы борьбы с данными видами преступлений, их обзору посвящается наш форум. Участие в нем представителей международных организаций, специализированных вузов и ученых подчеркивает важность этой темы.

Международное сотрудничество имеет особое значение для эффективной борьбы. Ярким примером тому служит информация, представленная нам правоохранительными органами, повлекшая привлечение в этом году к уголовной ответственности членов одной транснациональной преступной группы, которые дистанционно (с территории Европы), применяя компьютерные технологии, совершали крупные хищения денежных средств из двух казахстанских банков. Подробно об этом деле в рамках конференции расскажет мой коллега.

Безусловно, что главная цель проведения конференции заключается в обмене передовым опытом в сфере воздействия информационных технологий. Надеюсь, что полученные результаты будут полезны всем участникам, а предложенные рекомендации действительно найдут свое применение в практической деятельности. Только благодаря целенаправленной, системной напряженной работе ученых, практиков, международных экспертов возможна успешная борьба с данным видом преступлений.

Хочу выразить благодарность руководству, профессорско-преподавательскому составу Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова за организацию настоящего мероприятия и возможность участия в нем. Желаю всем плодотворной работы, конструктивного диалога и эффективного взаимодействия.

Малахов Д. М.,
заместитель председателя
Агентства Республики Казахстан
по противодействию коррупции

Здравствуйте,
уважаемые участники!

Поздравляю Вас с открытием международной научно-практической конференции «Инновационные технологии в криминалистике».

Данная конференция, проводимая по инициативе Министерства внутренних дел и поддержке Организации по безопасности и сотрудничеству в Европе (ОБСЕ), является актуальной в свете новых вызовов по более ухищренным способам совершения уголовных правонарушений, в том числе и коррупционных с применением высоких технологий, таких как сокрытие активов, добытых преступным путем, с использованием виртуальных валют (биткоины и другие виды криптовалют).

Считаю, что главная цель проведения конференции заключается в обмене передовым опытом и знаниями в сфере цифровой криминалистики. Надеюсь, что полученные результаты будут полезны всем участникам и предложенные рекомендации действительно найдут свое применение в практической деятельности.

Желаю всем участникам и организаторам конференции плодотворной работы, конструктивного диалога и эффективного взаимодействия!

Елемесов Ж. Ф.,
заместитель председателя
Агентства Республики Казахстан
по финансовому мониторингу

Приветствую вас,
уважаемые участники конференции!

Хочу выразить благодарность за организацию данного мероприятия. Тематика конференции действительно является очень актуальной и востребованной в борьбе с преступностью.

Как вам известно, наше Агентство — относительно новое ведомство, в Агентстве есть 2 службы: подразделение финансовой разведки и служба экономических расследований. Часто в своей деятельности мы используем научно-технические средства и специальные познания сотрудников криминалистического подразделения.

Применение инновационных технологий в криминалистике увеличивает роль специальных знаний по установлению и закреплению доказательств в расследовании преступлений.

Полагаю, что выступления сегодняшних спикеров позволят нам обменяться практикой по направлениям деятельности, а по отдельным вопросам изучить ваш положительный опыт и в дальнейшем использовать его в работе.

Подробнее о роли криминалистического подразделения в Службе экономических расследований расскажет руководитель криминалистического управления Агентства по финансовому мониторингу Умергалиев Марат Серикказыевич.

Желаю участникам конференции успехов и плодотворной работы.

Ким Д. В.,
начальник Сибирского юридического института
МВД России, доктор юридических наук, профессор,
генерал-майор полиции
(Российская Федерация, г. Красноярск)

Уважаемые коллеги! Позвольте мне от коллектива Сибирского юридического института МВД России поприветствовать всех участников научного форума, поблагодарить руководство Министерства внутренних дел Республики Казахстан и Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова за приглашение принять участие в работе международной научно-практической конференции «Инновационные технологии в криминалистике», за возможность рассмотреть актуальные вопросы и проблемы по данной тематике научного мероприятия, обменяться имеющимся опытом с представителями различных международных организаций, коллегами из компетентных органов, а также учеными из России, Азербайджана, Белоруссии, Казахстана, Узбекистана и Индии.

Уверены, что организованная Вами в дистанционном формате международная конференция пройдет как всегда на самом высоком уровне и будет интересной для всех участников, а результаты нашей совместной работы в рамках конференции найдут свое теоретическое и практическое применение в области криминалистики.

Желаем всем участникам успехов и плодотворной работы.

Уиллер Р.,
старший советник
по военно-политическим вопросам
Офиса программ ОБСЕ в г. Нур-Султане

Уважаемые участники и организаторы международной научно-практической конференции «Инновационные технологии в криминалистике»! Позвольте от офиса программ ОБСЕ в г. Нур-Султане Вас поприветствовать и присоединиться к уже озвученным словам благодарности в адрес Карагандинской академии МВД РК, а также всех соорганизаторов данного мероприятия. Хотел бы также поблагодарить всех спикеров и экспертов, которым предстоит поделиться своим опытом и своими знаниями. Уверен, что Ваши доклады будут полезны всем участникам и внесут или уже внесли весомый вклад в развитие столь важного направления в работе правоохранительных органов всех стран.

ОБСЕ в целом, и наш офис, в частности, уделяет большое внимание построению правоохранительных органов Республики Казахстан, особенно в части, касающейся компьютерных технологических исследований, в вопросах и проблемах в отношении DeepFake, использования технологии биометрии, сбора и обработки цифровых доказательств при работе с данными из открытых источников, а также других направлениях. В свою очередь, наш офис совместно с партнерами в текущем году предоставляет поддержку в реализации запланированных мероприятий по данной тематике.

Интернет-преступления вышли на беспрецедентный уровень в связи с пандемией COVID – 19, хотя и до начала пандемии они стали обыденной частью нашей современной жизни. Огромная власть преступной деятельности, которая ранее была ограничена, в основном, личным взаимодействием, сейчас перешла в пространство Интернета и других информационных технологий, что делает уголовное преследование крайне сложным. С каждым годом, к сожалению, объем таких преступлений только растет. В связи с этим инновационные технологии в криминалистике становятся неотъемлемой частью процесса эволюции работы правоохранительных органов. Важнейшую роль в этой связи играет международное сотрудничество и обмен опытом с государствами, которые уже имеют необходимые знания. Данная конференция как раз и является ярким примером такого сотрудничества.

Важно отметить, что данная работа должна осуществляться многосторонне и с соблюдением абсолютно всех законов страны посредством тесного взаимодействия различных государственных учреждений, гражданских и правовых институтов, бизнес-структур и, главное, — образовательных и научно-исследовательских учреждений. С большим удовольствием послушаю выступления всех докладчиков. Желаю всем плодотворной работы и благодарю за возможность участвовать в столь важном мероприятии.

ДОКЛАДЫ
НА ПЛЕНАРНОМ И СЕССИОННОМ ЗАСЕДАНИЯХ

Абенова И. Б.,
Компьютерлік технологиялар бойынша маман
«Тәуелсіз сот сараптамасы және мамандандырылған
зерттеулер альянсы» қоғамдық бірлестігі
(Қазақстан Республикасы, Нұр-Сұлтан қ.)

ЦИФРЛЫҚ КРИМИНАЛИСТИКАНЫҢ МАҢЫЗЫ МЕН ДАМУЫ

Физикалық әлемде біз өзіміздің ізімізді қалдырамыз — саусақ іздері, шаш, киім талшықтары, ДНҚ және т. б. біз адамдармен және объектілермен өзара әрекеттесетін сәтте, сондай-ақ цифрлық салада қолданушылардың кез-келген әрекеті өздері туралы іздер қалдырады. Бұл виртуалды немесе цифрлық іздер — файл фрагменттері, белсенділік журналдары, уақыт белгілері, метадеректер және т. б. — қылмыстық іс бойынша маңызды және кейде маңызды ақпарат ретінде қарастырылуы мүмкін. Мұндай ақпарат құжаттың немесе бағдарламалық жасақтаманың шығу тегін анықтау кезінде, қылмыстық іске қатысатын тараптардың іс-әрекеттерін анықтау кезінде заңды мақсаттарда немесе тіпті жеке деректерді ұрлау сияқты киберқылмыс үшін ресурс ретінде дәлелді болуы мүмкін. Мұндай іздерді ынталандыру, анықтау және бекіту қандай болмасын, есептеу ортасында дәлелдемелерді (іздерді) зерттеу, түсіндіру немесе қайта құру цифрлық криминалистика саласына жатады[1, 11].

Цифрлық криминалистика (сонымен қатар компьютерлік криминалистика немесе киберкриминалистика деп те аталады) — бұл процесс қылмыстық немесе азаматтық тергеуде дәлел ретінде заңды контексте рұқсат етілген деп есептелетін компьютерлерде және желілерде табылған ақпарат туралы есептерді жинау, талдау және құрастырудың тәжірибесі[2]. Цифрлық криминалистикалық операцияларды құқық қорғау органдарында қылмыстарды тергеу кезінде де, коммерциялық, жеке жобаларда да, киберқауіпсіздік жағдайында да қолдануға болады. Жеке компьютерлік жүйелер мен желілерде жүргізілген әрекеттер әдетте «цифрлық із» — электронды-цифрлық іздер қалдырады[3]. Олар веббраузер тарихы мен «cookie» кэштерінен бастап жойылған файлдарға, электрондық пошта тақырыптарына, құжатмета деректеріне, процесс журналдарына және сақтық көшірме файлдарына дейін болуы мүмкін. Кәсіпорынды қорғайтын қауіпсіздік мамандары үшін немесе қылмысты тергеумен айналысатын тергеушілер үшін цифрлық криминалистикалық дәлелдердің кез-келген немесе барлық аспектілері оқиғаны құжаттау, жауап тұжырымдау немесе болашақ операциялардың стратегиясын жасау кезінде маңызды болуы мүмкін.

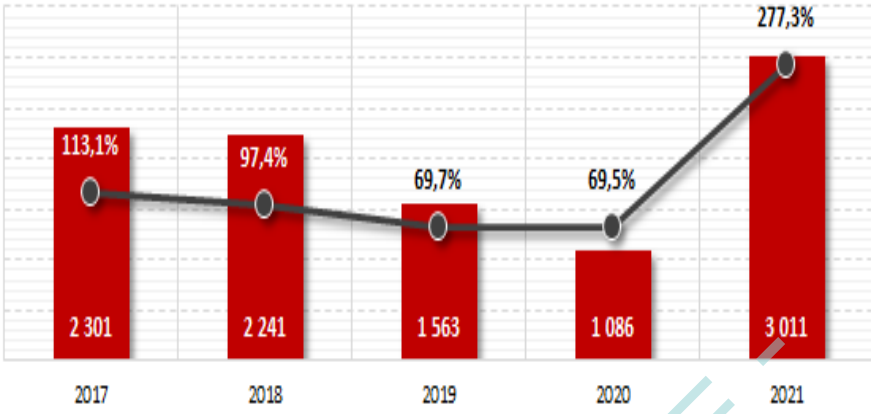
Ғылыми тұрғыдан алғанда, хакерлер мен кибер қылмыскерлердің қызметі мен әдіснамасын зерттеу, олар қолданатын құралдар мен әдістерді цифрлық криминалистикалық талдаумен бірге шабуылдардың басым немесе болашақ бағыттары, киберқылмыскерлердің әрекеттері, желілері және пайда болатын зиянды бағдарламалар штамдары туралы түсінік бере алады. Кәсіпорынның қауіпсіздігі тұрғысынан цифрлық криминалистикалық талдауды қолдану арқылы алынған дәлелдер инциденттерге тез жауап беруге және кибер шабуылдарды немесе деректерді ұрлауды анықтаған кезде жағдайды түзету шараларын қабылдауға көмектеседі. Ақпарат шабуыл бағыттары, зиянды бағдарламалық жасақтаманың жаңа немесе мамандандырылған нысандары бойынша алынуы мүмкін.

Тұрақты және жасырын кибер шабуылдардың бұл түрі бірнеше ай немесе тіпті жылдар бойы байқалмауы мүмкін, шабуылдаушылар желіге қолжеткізу, жүйе арқылы тарату, содан кейін қылмыстық мақсаттарды жүзеге асыру үшін бірқатар түрлі әдістерді қолданады. Киберқылмыскерлерді тергеу барысында кейіннен дәлелдемелік мәнге ие болатын цифрлық криминалистикалық ақпаратты жинау кезінде сақтық таныту керек, бұл үшін криминалистикалық цифрлық талдау үшін жиналатын деректердің мүмкіндігінше дұрыс екендігіне кепілдік беру қажет.

Компьютерлер, ұялы телефондар және Интернет қылмыскерлер үшін ең үлкен өсіп келе жатқан ресурс болғандықтан, құқық қорғау саласында цифрлық криминалистика маңызды болып табылады.

2021 жылдың қаңтар айындағы мәліметтерге сүйенсек Қазақстанда 3 мыңнан астам кибершабуыл жасалды — өткен жылғы қаңтармен салыстырғанда 2,8 есе көп[4].

ҚР-да «Цифрлы Қазақстан» мемлекеттік бағдарламасы іске асырылуда, онда нысаналы индикаторлардың бірі 2018 жылдан бастап 2022 жылға дейінгі кезеңде халықтың цифрлық сауаттылық деңгейін 77 %-дан 83 %-ға дейін арттыру болып табылады. 2019 жылы халықтың цифрлық сауаттылығының нақты деңгейі 82,1 %-ды, жоспарлы 78,5 %-ды құрады.



2021 жылғы 29 маусымда БҰҰ жанындағы Халықаралық Электр байланысы одағының (ХЭО) конференциясы өтті, оның шеңберінде Киберқауіпсіздіктің жаһандық индексі бойынша есептің 4-ші басылымы жарияланды.

Мәселен, БҰҰ МӘС сарапшылары жүргізген талдау нәтижелері бойынша Қазақстан Республикасы Киберқауіпсіздіктің жаһандық индексінде 9 позицияға көтеріліп, 31 — орынды (бұрын 40-шы) иеленді.

Өңірлік рейтингте Қазақстан Ресей Федерациясынан кейін 2-ші орында тұр.

Рейтинг критерийлері: заңнамалық база, техникалық және ұйымдастырушылық іс-шаралар, халықаралық аренадағы қызмет және киберқауіпсіздік саласын дамыту үшін әлеует құру болып табылады[5].

Соңғы бірнеше жыл ішінде цифрлық криминалистика жетекші орынға ие болғанына қарамастан, бүкіл әлемде мобильді құрылғыларды қолданудың күрт өсуі байқалды, бұл мобильді компьютерлік сараптама цифрлық криминалистикалық зерттеулер арасында ең қолайлы таңдау болып табылады. Қылмыстық іс шеңберіндегі мобильді құрылғыларға компьютерлік сараптама әртүрлі жағдайларда криминалистік маңызды ақпаратты ала алады.

Сондай-ақ, мобильді құрылғыларда қылмысты тергеу барысында қолдануға болатын көптеген мәліметтер бар, мысалы, сөйлесу тарихы немесе физикалық орналасқан жер туралы мәліметтер және т. б. физикалық және технологиялық әлем арасындағы тығыз байланыс цифрландыруды қолдана отырып, қылмыстық істерді шешу сияқты мүмкіндіктерді ашқанымен, ол сонымен бірге оны қолданумен байланысты бір қатар ықтимал қауіптерге ие. Ең көп таралған кибершабуылдарға DDoS шабуылдары және VoIP құрылғылары кіреді, олар алдағы жылдардағы цифрлық криминалистиканың даму ауқымын нақты көрсетеді. Алайда, цифрлық криминалистика мамандары үшін үлкен көлемдегі деректерді талдау қажеттіліктерін қанағаттандыра алатын жаңа әдістер мен құралдарды әзірлеуге, сондай-ақ одан әрі тергеуді бағыттай алатын ықтимал цифрлық кеңестер туралы есептер жасауға инвестиция салу әлі де маңызды мәселе болып табылады.

Ақпараттық-коммуникациялық ортадағы қылмыстың көлемін цифрлық түрде білдіру қиын (бұл мемлекеттің ақпараттық және қоғамдық қауіпсіздігінің мәселелері ғана емес, сонымен бірге экономикалық қылмыс) көптеген қылмыстардың жоғары латенттігіне, сондай-ақ жәбірленушілердің өздерінің құқықтық сауатсыздығы мен енжарлығына байланысты. Алайда, біз қылмыс жасау әдістері мен құралдары, сондай-ақ қылмыскерлер қалдырған іздер үнемі өзгеріп отыратындықтан, цифрлық қылмысқа қарсы тұру әдістері дамып келе жатқанын байқаймыз. Белгілі болғандай, маман, тергеуші немесе сарапшы жұмыс істейтін цифрлық іздерді жою оңай. Қиындық сонымен қатар цифрлық дәлелдемелерді зерттеу кезінде адам оларды тікелей, сезім мүшелері арқылы қабылдай алмайды, бұл үшін күрделі бағдарламалық кешендер қажет.

Қазақстанда цифрлық криминалистика саласында бағдарламалық жасақтама жасамайды деп айтса да болады, көбінесе шетелдік бағдарламаларды пайдаланады. IT — өнімдерді пайдаланудың

артықшылықтарын нақты түсінудің болмауына байланысты оларға сұраныс аз. Бұл мәселені айқындау және реттеу технологиялық шешімдерді пайдалануға сұраныс жасауға мүмкіндік береді, бұл стартап жобаларды дамыту үшін негіз қалыптастыратын еді.

Цифрлық криминалистикадағы тағы бір мәселе компьютерлік қылмыстарды заңгерлер тергеуге мәжбүр, ал әлемнің көптеген елдерінде cybercrime — тергеушілері, ең алдымен, қосымша заң білімі бар техникалық сарапшылар болып табылады.

Жоғары технологиялар саласындағы қылмыстарды тергеу қиын, олар құқық қорғау органдарының қызметкерлері тарапынан арнайы білімді, тәжірибе мен ресурстарды қажет етеді. Мемлекеттік сараптама мекемелерінде компьютерлік сараптама жүргізу кезегі, әдетте, бірнеше айдан асады, полицияда кибер-зерттеулер саласындағы мамандар өте аз. Тұрмыстық киберқылмыстардың едәуір бөлігі (әлеуметтік желілерді немесе мессенджерлерді бұзу, үй компьютерлеріне вирустық шабуылдар) көбіне тіркелмейді.

---

[1] Ищенко Е. П. У истоков цифровой криминалистики // Вестн. ун-та им. О. Е. Кутафина. — М., 2019.

[2] Пастухов П. С. Использование информационных технологий для обеспечения безопасности личности, общества и государства / П. С. Пастухов, М. Лосавио // Вестн. Пермск. ун-та. Юридические науки. 2017. Вып. 36. С. 231 – 236.

[3] Бахтеев Д. В. Криминалистическая классификация цифровой доказательственной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): Мат-лы международ. науч.-практ. конф. — М., 2018.

[4] Есептеулер Ranking.kz-тен KZ-CERT мәліметтерінің негізінде.

[5] URL: https://www.gov.kz/memleket/entities/mdai/press/news/details/224025?lang=ru

Айдарбек С. О.,
старший преподаватель кафедры криминалистики,
магистр юридических наук, подполковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Тенденции развития цифровой криминалистики

Высокие темпы развития в Казахстане информационно-коммуникационных технологий актуализируют вопросы защиты соответствующей инфраструктуры, поскольку ее повреждение или разрушение может иметь значительные последствия для безопасности страны. Для организации киберзащиты создан ряд структур (Управление «К» Комитета криминальной полиции МВД, аналогичное специализированное подразделение в КНБ, государственная служба технической защиты информации Министерства транспорта и коммуникаций), принимающих участие в обеспечении информационной безопасности государства. Они занимаются совершенствованием законодательства, изучением и сертификацией технических средств, обеспечением информационной защиты систем органов государственной власти, расследованием преступлений и обнаруженных кибератак, а также принятием мер по их пресечению[1].

В 2020 г. по сравнению с аналогичным периодом прошлого года количество кибератак в казахстанском сегменте Интернета выросло почти в 2,7 раза. В текущем году в связи пандемией и переходом на дистанционные формы работы кибератаки на цифровое пространство страныучастились.

Вопросам развития сферы кибербезопасности в Казахстане уделяется пристальное внимание. За прошедшие годы были выработаны базовые концептуальные подходы к развитию сферы кибербезопасности страны. Разработана и уже утверждена концепция кибербезопасности «Киберщит Казахстана», действие которой рассчитано до 2022 г. Уже вступил в действие целый ряд законодательных актов и большое количество отраслевых приказов. Помимо этого, созданы испытательные лаборатории в сфере информационной безопасности по исследованию вредоносного кода, запущен национальный координационный центр информационной безопасности, частная служба реагирования на компьютерные инциденты (CERT), 7 оперативных центров информационной безопасности (SOC), увеличено число грантов по этой специальности и т. д.[2]

Для дальнейшего улучшения ситуации в сфере информационной безопасности и защите персональных данных Министерством цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан инициирован вопрос о наделении Комитета по информационной безопас-

ности функциями по защите персональных данных, проведения аудита и проверок владельцев информационных систем, в которых обрабатываются персональные данные.

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные. Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных[3].

Стремительная цифровизация всех сфер общества обусловила резкий рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Изучение правоприменительной и судебной практики выявило недостаточную степень использования возможностей цифровой криминалистики для расследования преступлений, что влечет за собой утрату информации, имеющей доказательственное значение по уголовному делу. Особое внимание уделено перспективам применения цифровой криминалистики для выявления цифровых следов и установления обстоятельств совершенного преступления. Целесообразно более тщательно законодательно регламентировать использование цифровых доказательств в процессе доказывания по уголовному делу.

Целью криминалистики является полное и своевременное технико-криминалистическое обеспечение и сопровождение раскрытия и расследования преступлений. Эта цель реализуется на основе всестороннего использования достижений современной науки и техники. Криминалистика обеспечивает деятельность органов дознания, предварительного следствия, суда и сопровождает процесс криминалистической экспертизы научно продуманными средствами, приемами и методами борьбы с преступностью.

Исходя из этого, для развития цифровой криминалистики в Казахстане необходимо разрешить следующие задачи:

- выявление и исследование объективных закономерностей и явлений в практике совершения преступлений и деятельности по их расследованию;
- разработка и совершенствование методов и средств практической деятельности по раскрытию, расследованию и предотвращению преступлений;
- разработка организационных, тактических и методических основ предварительного расследования;
- разработка криминалистических средств и методов борьбы с преступностью.

---

[1] Биекенов Н. А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан. [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=31 554547 (дата обращения: 29.10.2021).

[2] Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахастан, gov.kz/memleket/entities.

[3] Носов В. А. Краткий исторический очерк развития криптографии // Московский университет и развитие криптографии в России, МГУ, 17 – 18 октября, 2002: Мат-лыконф. — М., 2002. С. 20 – 32.

Алесковский С. Ю.,
президент
ОО «Евразийская ассоциация полиграфологов»,
кандидат юридических наук;
Коваленко С. Б.,
ответственный секретарь
ОО «Евразийская ассоциация полиграфологов»,
кандидат юридических наук
(Республика Казахстан, г. Алматы)

Казахстанский полиграф «AQIQAT» — новое криминалистическое средство для расследования и раскрытия преступлений

Выступление с докладом о казахстанском полиграфе на таком представительном форуме, проводимом в Карагандинской Академии МВД Республики Казахстан, имеет под собой исторические предпосылки.

Дело в том, что первые исторические вехи в развитии инструментальной детекции лжи в Казахстане датируются началом 80-х годов прошлого века. Именно в этой альма-матер, называвшейся в то время Карагандинской высшей школой МВД СССР, под руководством ее первого начальника генерала Бейсенова Б. С., сотрудник кафедры криминалистики первый казахстанский полиграфолог Зинкевич И. Б. (Рис. 1) организовал проведение практических опытов использования прототипа полиграфа.

Рисунок 1. Первые опыты с полиграфом в Казахстане проходили в КВШ МВД СССР

Ныне полиграф давно уже стал неотъемлемым средством, используемым в криминалистике при расследовании и раскрытии преступлений. Вспоминается 2002 г., когда в только что вышедшем первом казахстанском учебнике по криминалистической технике[1, 614] полиграфологический метод «скромно» был спрятан в разделе «Нетрадиционные средства получения доказательственной информации при расследовании преступлений». Прошло почти двадцать лет, и инструментальный психофизиологический метод выявления скрываемой информации с применением полиграфа стал обыденностью как для правоохранительных органов Казахстана (в первую очередь, органов внутренних дел), так и для судебной системы.

Как и прогнозировал великий Белкин Р. С., криминалистика превратилась из «потребителя» в «заказчика», то есть стимулятора развития других наук, в данном случае, психофизиологической детекции лжи. Сегодня полиграфологи создают новые и модернизируют старые тесты именно в интересах практики розыскных и следственных подразделений, повышая валидность и надежность методики и исключения ошибочных выводов.

Безусловно, результат работы полиграфолога зависит и от применяемой им техники — полиграфа. Парк используемых ныне моделей полиграфов кажется весьма и весьма обширным и, вроде бы, удовлетворяющим любому, даже самому изысканному вкусу (Рис. 2). Как и в других странах постсоветского пространства, полиграфологи Казахстана в основном работают либо на североамериканских полиграфах Axciton, Lafayette, Stoelting и Limestone, либо на аппаратах российского производства: так называемых варламовских приборах (Барьер – 14, Крис, Риф), производных от аппарата Диагноз (ПиК, Поларг, Диана), модернизациях полиграфа Дельта (Конкорд – М, Энергия, Дельта – Оптима), приборах Эпос (Эпос 7, Эпос 9)[2, 102] и др.

Рисунок 2. Полиграфы мировых брендов

При всем разнообразии перечисленных приборов, у них есть одна общая черта — они созданы либо уже очень давно (15 и более лет назад), либо из старых материалов. Однако прогресс неумолим,

особенно в области электроники, которая за это время ушла далеко вперед. Достаточно посмотреть на наши компьютеры и телефоны и сравнить их с образцами 15-летней давности. Поэтому создание нового качественного прибора по более низкой цене, всегда являлось актуальной задачей.

Казахстан имел в прошлом опыт конструкторских разработок в данной сфере. Еще в конце девяностых — начале нулевых годов научно-конструкторское подразделение одного из правоохранительных органов Казахстана с участием одного из авторов данной статьи подготовило и выпустило собственный полиграф «Адал», а в дальнейшем и «Адал – 2»[3, 23]. К сожалению, в практической деятельности полиграф «Адал» (Рис. 3) использовался очень мало и, в основном, применялся при тестировании абитуриентов юридического вуза г. Алматы для выявления у них факторов риска.

Рисунок 3. Первый казахстанский протополиграф «Адал – 2»

Сразу же вскрылись и существенные недостатки полиграфа «Адал», правильнее даже было бы назвать, «протополиграфа» — очень сложная и утомительная подстройка прибора к физиологическим реакциям каждого обследуемого, которая занимала иногда до 20 – 30 минут. Также практически невозможно было длительное время удерживать стабильную амплитуду сигналов. Естественно, это было неприемлемо для практической работы[4, 5]. Поэтому вскоре протополиграф «Адал» сошел в небытие, не выдержав суровой действительности и испытания практикой.

И лишь в 2019 г. в Казахстане появился первый совместный российско-казахстанский полиграф — одиннадцатиканальный профессиональный компьютерный полиграф «AQIQAT», в котором нашли свое воплощение самые передовые на сегодняшний день конструкторские и программные находки. Полиграф «AQIQAT»является глубоко переработанной и адаптированной для казахстанского рынка моделью ведущего российского полиграфа «Триумф», созданного конструкторской группой под руководством Калафати А. Ю. (Рис. 4).

При разработке самого «Триумф» разработчики ориентировались на законодателей моды в области полиграфных проверок — американских производителей. Первый раз прибор был показан ведущим мировым специалистам на ежегодном семинаре американской ассоциации полиграфологов (APA) в сентябре 2015 г. в г. Чикаго, которые высоко оценили как качество изготовления датчиков, так и качество съема сигнала.

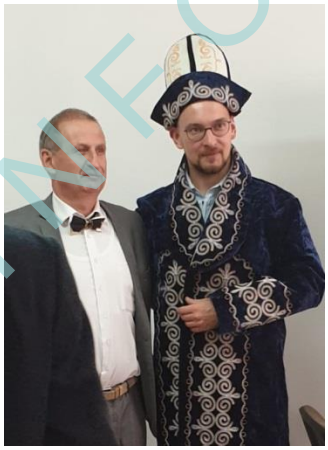


Рисунок 4. Разработчики полиграфа «AQIQAT» — А. Ю. Калафати (справа) и С. Ю. Алесковский

Рисунок 5. Полиграф «Триумф – 2»

Казахстанские полиграфологи Алесковский С. Ю. и Мильштейн М. М. впервые увидели в действии новый полиграф «Триумф» (Рис. 5) именно в Чикаго. Полиграф, действительно, заставил сразу влюбиться в него.

Именно тогда возникло первое желание о создании современного казахстанского полиграфа на основе перспективного «Триумфа».

Однако от идеи до начала работы по осуществлению задуманного прошло еще ровно три года. В октябре 2018 г. во время проходившей в российском городе Сочи 19-ой Международной научно-практической конференции «Научно-теоретические подходы и их прикладное применение в практике инструментальной детекции лжи в борьбе с преступностью и работе с кадрами» состоялось окончательное оформление совместного проекта «Триумф – AQIQAT». Наш казахстанский полиграф «AQIQAT» стал значительно отличаться от своего российского прототипа:

- разработана новая материнская плата с процессорами,
- полностью переработана визуальная часть интерфейса,
- значительно увеличилось количество информативных каналов, регистрирующих физиологические показатели организма,
- полиграф стал полиглотом и работает на нескольких языках: казахской кириллице, казахской латинице, русском, английском и многих других языках,
- установлен двухкомпонентный модуль выявления динамического противодействия и др.

Полиграф»AQIQAT» (Рис. 6) оказался таким удачным продуктом, что вскоре на его основе Калафати А.Ю. выпустил новый полиграф «Триумф – 2».

Очень важно, что в основе полиграфов «Триумф – 2» и «AQIQAT» лежит 24-битный АЦП (аналого-цифровой преобразователь), что делает эти аппараты самыми мощными полиграфами в Евразии.

Только на полиграфах «Триумф – AQIQAT» используется уникальный Компьютерный алгоритм анализа полиграмм «Сокол», не имеющий аналогов в мире (Рис. 7). «Сокол» является первым российским валидизированным алгоритмом и значительно превосходит по точности алгоритм «ChanceCalc» полиграфа «Диана».

Рисунок 6. Сенсорный блок полиграфа «AQIQAT»

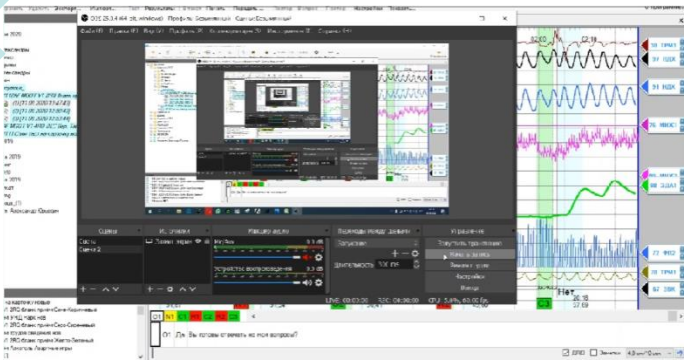


Рисунок 7. Компьютерный алгоритм анализа полиграмм «Сокол»

Совсем недавно для полиграфов «Триумф – AQIQAT» разработан и внедрен в программное обеспечение новый физиологический канал под названием «Интегральный» (Рис. 8), имеющий исключи-

тельную наглядность. При его создании Калафати А.Ю. творчески развил идеи одного из патриархов советской и российской полиграфологии Алексеева Л. Г. Интегральный канал (ИК) получается путем вычисления параметров Кирчера (длина линии дыхания, амплитуды ЭДА и манжеты), а также амплитуды ФПГ на всем протяжении записанного вопроса. При этом учитываются только те значения, которые превышают фоновую физиологическую активность. В других современных полиграфах отсутствует подобный интегральный канал.

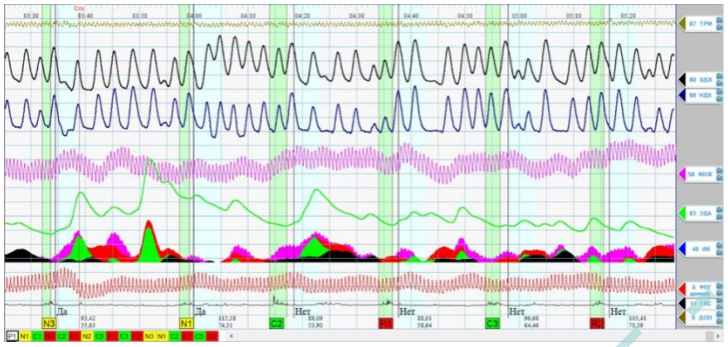


Рисунок 8. Интегральный канал на полиграмме полиграфа «AQIQAT»

Большое значение сегодня полиграфологи уделяют выявлению возможного умышленного противодействия со стороны опрашиваемых лиц, для чего применяются разнообразные датчики тремора. В полиграфе «AQIQAT» используется пять датчиков тремора, что позволяет значительно повысить точность и надежность полиграфной проверки. Это: 1) датчик двигательной активности в тканевом чехле, 2) датчик двигательной активности с металлическими пластинами, 3) универсальный датчик пьезоплетизмограммы и мимики лица, 4) двухкомпонентный модуль выявления динамического противодействия и 5) датчик, фиксирующий тремор жевательной мышцы — «датчик челюстей» (Рис. 9). Часть этих датчиков является уникальной и не применяется на полиграфах других моделей.

Рисунок 9. Датчик тремора «Челюсти»

Таким образом, сегодня полиграф «AQIQAT» (Рис. 10) ни в чем не уступает ведущим мировым полиграфам, а по многим позициям превосходит многие из них. Полиграф «AQIQAT» — это та инновационная продукция, которой может и должен гордиться Казахстан!

Рисунок 10. Одиннадцатиканальный казахстанский профессиональный компьютерный полиграф «AQIQAT»

[1] Криминалистика: Криминалистическая техника: Учебн. для вузов / А. Ф. Аубакиров, С. Ю. Алесковский, С. Б. Коваленко и др. — Алматы, 2002.

[2] Полиграф в Казахстане — избранные страницы: Библиотека полиграфолога / Под ред. С. Ю. Алесковского и Г. А. Алибаевой. — Алматы, 2016.

[3] Алесковский С. Ю. Становление и развитие полиграфа в Казахстане / Эксперт-криминалист: Федеральный научно-практический журнал. — М., 2015. № 4.

[4] Алесковский С. Ю. Детектор лжи в Казахстане — история и современность // NarxozLawandPublicPolicy. — Алматы, 2020. № 1 (1).

Аманжолова Ж.,
магистрант;
Брылевский А. В.,
профессор кафедры уголовного процесса
и криминалистики, кандидат юридических наук
(Костанайская академия
МВД Республики Казахстан им. Ш. Кабылбаева)

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ НАЗНАЧЕНИЯ СУДЕБНОЙ ЭКСПЕРТИЗЫ И СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ ОВД РК

Судебная экспертиза — наиболее квалификационная форма использования специальных знаний в судопроизводстве. Проведение судебной экспертизы является основной частью уголовного, гражданского, административного процесса и относится к предмету процессуально-правового регулирования. Это — процессуальное действие. Состоящее из трех этапов: назначение экспертизы; производство экспертизы; оценка и использование заключение эксперта.

Экспертиза назначается в случаях, когда обстоятельства, имеющие значение для рассматриваемого дела, могут быть получены в результате исследования материалов дела, проводимого экспертом на основе специальных научных знаний. Назначение экспертизы может иметь место при наличии фактических оснований.

Фактическим основанием является потребность разрешения возникающих по делу вопросов использованием специальных научных знаний. Потребность в специальных знаниях является общим основанием производства судебной экспертизы, но не является обязательным, безусловным фактическим основанием производства экспертизы, за исключением особо оговоренных в законе случаев (ст. 271 УПК РК).

Основания производства судебных экспертиз подразделяются на фактические и юридические.

Юридическим основанием производства экспертизы является постановление дознавателя, следователя, суда о ее назначении. Замена его различными, не предусмотренными законом документами (сопроводительное письмо, перечень вопросов эксперту и т. п.) не допустима.

При формулировании вопросов эксперту необходимо учитывать определенные требования. Вопросы не должны выходить за пределы предмета экспертизы.

Соблюдение требования о необходимости использования специальных знаний, а также четкое определение круга вопросов, на которые могут ответить лишь лица, ведущие уголовный процесс, к числу которых должны быть отнесены вопросы, касающиеся виновности лиц, квалификации их действий, относимости, допустимости и достаточности доказательств по делу, применения норм уголовного и уголовно-процессуального законодательства, являются необходимыми условиями[1, 73].

Говоря о вопросах, решаемых экспертом, следует отметить также вопрос о возможности использования предоставленного процессуальным законом права проявлять инициативу. По согласованию с органом, назначившим экспертизу, эксперт вправе давать заключение не только по поставленным вопросам, но и по иным относящимся к его компетенции обстоятельствам, имеющим значение для дела и установленным по инициативе эксперта.

В процессе исследования эксперты часто обнаруживают новые обстоятельства, имеющие значение для дела, и выявляют информацию, выходящую за пределы поставленной перед ними задачи. Экспертная инициатива может иметь место лишь в отношении объектов, указанных в постановлении.

К этапу назначения экспертизы относится также определение вида судебной экспертизы. Лицо, назначающее экспертизу, должно ориентироваться в классификации экспертиз, поскольку неправильное определение вида назначаемой экспертизы может привести к серьезным процессуальным нарушениям порядка ее назначения и производства.

В зависимости от целевого назначения классификация может быть произведена по разным основаниям:

- количеству участвующих экспертов (единоличные и комиссионные);
- характеру используемых специальных знаний (комплексные);
- объему проводимых исследований (основные и дополнительные);
- последовательности проведения (первичные и повторные)[2, 55].

Как показывает анализ экспертной практики, при назначении дополнительной и повторной экспертизы имеют место недостатки, связанные с неверным определением статуса экспертизы. Часто повторная экспертиза определяется лицом, назначившим экспертизу, как дополнительная и наоборот. В этой связи хотелось бы еще раз обратить внимание на признаки, определяющие дополнительную и повторную экспертизу.

Недостаточно полным может быть признано заключение эксперта, если оно основано на исследовании не всех предоставленных объектов или не содержит исчерпывающих ответов на поставленные вопросы. Указанная неполнота сама по себе не ставит под сомнения выводы эксперта.

Устранение неясности либо неполноты заключения эксперта возможно посредством допроса. В случае невозможности устранения неполноты или неясности путем допроса и назначения дополнительной экспертизы появляется необходимость в проведении дополнительных исследований.

Производство дополнительной экспертизы может быть поручено тому же или иному эксперту. При ее назначении в распоряжении эксперта должны быть предоставлены материалы основной экспертизы. Нарушение любого из данных условий является основанием для признания заключения необоснованным.

Мотивами несогласия с заключением эксперта являются:

- сомнения в не компетенции эксперта или незаинтересованности;
- сомнительность исходных данных;
- наличие противоречий между ними и иными доказательствами по делу; ненадлежащее качество проведенного исследования;
- неправильное оформление заключения.

При несогласии с выводами эксперта назначения повторной экспертизы не является обязательным. Следует учитывать наличие в деле иных доказательств по обстоятельствам, являющимся предметом экспертизы.

Назначение повторной экспертизы не обязательно и в случаях, когда по делу принято одно из заключений, при этом необходимо мотивировать свой вывод. В постановлении о назначении повторной экспертизы должны быть приведены мотивы несогласия с результатами предыдущей экспертизы.

Судебная оценка экспертного заключения — завершающий этап деятельности по конституированию заключения как судебного доказательства, в ходе и результате которого и определяется, по существу, доказательственная сила заключения по конкретному делу. Оценивая заключение эксперта, суд проверяет, соблюдены ли требования процессуального закона о специальной правоспособности лица, назначенного экспертом (не было ли оснований для отвода); соблюден ли процессуальной порядок назначения и проведения экспертизы; соблюден ли порядок направления материалов и объектов на экспертизу; соблюдены ли права заинтересованных лиц при назначении и проведении экспертизы; в соответствии ли с законом эксперт реализовал обязанность по даче заключения по форме и содержанию требования закона.

Доказательство признается относящимся к делу, если оно представляет собой фактические данные, которые подтверждают, опровергают или ставят под сомнения выводы о существовании обстоятельств, имеющих значение для дела.

Оценка заключения эксперта как доказательства по уголовному делу включает определение его относимости, допустимости, достоверности и доказательственного значения по делу.

Собственно говоря, в настоящее время в системе уголовного судопроизводства сформировалась устойчивая традиционная максима о том, что заключение эксперта обладает некими достоинствами, которые делают его более предпочтительным, чем заключение специалиста. Именно базируясь на

этом традиционном утверждении лица, ведущие уголовный процесс, считая заключение специалиста неким недостаточным источником доказательств, назначают производство судебной экспертизы по вопросам, по которым ранее уже было проведено, например, криминалистическое исследование. Мы же, в свою очередь, опираясь на положения ст. 25 УПК РК полагаем, что это далеко не так. Исходя из требований ст. 25 УПК РК следует, что «… никакие доказательства не имеют заранее установленной силы…», соответственно, любые утверждения о том, что заключение специалиста ниже по статусу или доказательной способности, как источник доказательств, нежели заключение эксперта не только противоречат логике и здравому смыслу, но и требованиям уголовно-процессуального законодательства.

Более того, если говорить о процессуальном статусе, то никаких различий между специалистом и экспертом кроме наличия у последнего соответствующей лицензии не предусмотрено.

Традиционно основным отличием специалиста от эксперта принято считать наличие у последнего специальных НАУЧНЫХ знаний против специальных знаний у первого. При этом считается, что эксперт в отличие от специалиста при производстве экспертизы использует специализированные методики исследования, которые не может использовать специалист.

Понятно, что если говорить о специалистах вообще, то подобные утверждения может быть и имеют место быть, вместе с тем, если говорить о специалистах специальных государственных органов и ОВД, то они, при производстве исследований, в полной мере используют специализированные методики, не уступающие по своей объективности методикам, утвержденным в Центре судебной экспертизы, а зачастую и являющимися абсолютно идентичными. Более того, если мы будем говорить о применении научно-технических средств в процессе доказывания, например, в процессе производства криминалистических исследований, то в соответствии с требованиями ст. 126 УПК РК «… Применение научно-технических средств признается допустимым, если они… 2) научно состоятельны». Таким образом, говорить о некой ненаучности методик, применяемых, например, специалистами-криминалистами, не имеет смысла. Конечно, далеко не во всех случаях можно обойтись исследованиями специалистов, в ряде случаев законодатель прямо предусматривает обязательность назначения экспертиз, но даже и это не делает процессуальный статус специалиста ниже, чем процессуальный статус эксперта.

То есть, можно сделать вывод о том, что специалист и эксперт в уголовном судопроизводстве не имеют различий в процессуальном статусе, а их заключения не имеют друг перед другом какой либо предопределяющей силы.

На протяжении более чем 70 лет в истории Казахстанских органов внутренних дел сотрудники оперативно-криминалистических подразделений имели статус экспертов и только в конце 90-х годов прошлого века вследствие реформы они этот статус утратили.

Причинами подобной пертурбации стали:

- необходимость придания эксперту более высокого процессуального статуса, обеспечения его процессуальной независимости;

- необходимость передачи функций экспертизы в конкурентную среду.

По прошествии 20 лет можно уверенно сказать, что ни одна из указанных целей не достигнута. Так, конкурентной экспертной среды в Казахстане не существует — большинство экспертных исследований осуществляется в подразделениях ЦСЭ МЮ РК. Ну, соответственно, о какой независимости можно говорить, когда эксперт является сотрудником государственного органа.

В настоящее время судебно-экспертная система РК представлена государственным учреждением «Центр судебных экспертиз МЮ РК», структуру которого составляют 19 научно-исследовательских институтов судебных экспертиз, дислоцированных в крупных городах и областных центрах страны.

При этом все экспертные исследования производимые подразделениями ЦСЭ являются платными, и длительными по времени, что негативно отражается на работе органов внутренних дел, вызывает недовольство со стороны потерпевших, влечет дополнительные расходы бюджетных средств, затрачивается время сотрудников ОВД при назначении судебных экспертиз и затягиваются сороки досудебного расследования.

Следует также отметить, что практически все исследования, производимые экспертами ЦСЭ по назначению ОВД, могут успешно производиться в криминалистических подразделениях МВД.

Таким образом, в заключении, хотим отметить:

В настоящее время отсутствуют какие-либо процессуальные основания считать, что эксперт выше по статусу, чем специалист, а заключение эксперта обладает большей доказательственной способностью, нежели заключение специалиста;

Практика назначения экспертиз по вопросам, по которым ранее произведено криминалистическое исследование в специальных органах или органах внутренних дел является вредной и приводит к существенному росту расходов на правоохранительную деятельность.

Учитывая отсутствие конкурентной экспертной среды, наличие в ОВД возможностей подготовки соответствующих специалистов, использование специалистами криминалистами оперативно-криминалистических подразделений научно обоснованных методик криминалистических исследований, огромные финансовые траты ОВД на производство экспертиз в ЦСЭ, при наличии аналогичных специалистов, мы считаем необходимым инициировать перед законодателем вопрос о возвращении статуса эксперта специалистам-криминалистам ОВД.

[1] Материалы Международной научно-практической конференции «Восток – Запад: партнерство в судебной экспертизе. Актуальные вопросы теории и практики судебной экспертизы» (г. Алматы, 27 октября 2016 г.).

[2] Материалы круглого стола «Проблемы развития судебно-экспертной системы Республики Казахстан» (г. Алматы, 5 – 6 марта 2004 г.).

Angel Joy,
Student
Rashtriya Raksha University Masters in Forensic Science
(Rashtriya Raksha University,
Raksha Shakti Rd, Lavad, Gujarat 382305, India)

FINGERPRINT FORGERY AS A TOOL IN CRIMES: PREVENTION AND MITIGATION

1. Introduction

The fingerprints of each individual are known to be unique and not identical[1]. The use of fingerprints for identification has centuries-old history. Usage of finger friction ridges provided proof of identity in ancient China around 300BC. At the end of the 19th century, fingerprint impressions were a popular tool in solving crimes[2]. Today, fingerprint recognition technology is widely used for various applications, including international border crossings, unblocking smartphones and laptop computers, door locks, financial transactions, forensics, and national ID programs[3]. Capturing a small fingerprint is fast and enjoys a high level of acceptance from users. The result of all those advantages is that fingerprint recognition became widespread, making fingerprints the dominant biometric trait[4]. The extensive use of fingerprints motivates forgers to generate fake fingertips or spoofing fingerprints[2]. Spoofing refers to the act of obtaining fingerprints from a fictitious finger instead of a real one[5]. The first reported fingerprint forgery occurred in the 1920s[2]. The possibility of dealing with forged fingerprints was raised immediately at the turn of the twentieth century when fingerprint evidence obtained from crime scenes gained traction in various jurisdictions[6]. In crime scene forensics, it is invaluable to recognize forged traces to avoid accusing innocent people[7]. One of the main problems with fingerprint authentication is that if someone steals your fingerprints or gains access to the fingerprint database, it is impossible to change the password, unlike any other password system[1]. The fingerprint forgery attacks can be achieved through the use of a variety of methods, including, but not limited to, (i) Gummy fingers, such as fabricated finger-like objects that impersonate another individual fingerprint, (ii) 3D or 2D printed fingerprint targets,(iii) altered fingerprints or damaged original fingerprint patterns and (iv) cadaver fingers. The fingerprint spoofing technique stands out among them by different processes ranging from basic molding and casting to highly sophisticated 2D and 3D printing. Materials commonly available in the market like gelatin, silicone, play-doh are utilized to generate fingerprint spoofs[8]. A systematic study of fingerprint scanners conducted in 2000 by van der Putte and Keuning concluded that they could not accurately differentiate authentic fingers from artificial fingers made from silicone and other materials. The inability of fingerprint devices to detect counterfeits created concerns in the biometrics community. Researchers have proposed several methods in recent years to address this issue[2].

This article addresses identity theft and impersonation, financial fraud, and biometric data breach, and all other security vulnerabilities against fingerprinting technologies in the paper as personal and national securi-

ty risks or threats using some case studies as an example. In addition, this paper offers both security and threat perspectives on the use of artificial fingerprints. Identifying and exposing the truth is critical to keeping people safe when fakes are playing around. Therefore, the paper describes detection methods of fingerprint forgery to identify fakes. Several methods of detection for fake fingerprint identification have been developed over the years by various researchers.

This review paper explores some of them. Without an assessment of prevention methods, stating crimes is insufficient. This review article highlights a few of the prevention methods found in some research studies. An analysis of research papers on fingerprint forgery helped this article to state fingerprint forgery as a tool in crimes. The practice of fingerprint forgery is not new to the world of crime; it dates back to the dawn of crime. However, there were fewer cases of fingerprint forgery at that time. Today, with all the changes and innovations in fingerprint technology, fingerprint forgery has also taken on a new aspect to play a role in modern-day crimes.

2. Threats to national security

Fingerprint-based identification is the most extensively studied and widely used system. Fingerprint-based systems are known to have high recognition accuracy. Therefore, fingerprint biometric systems account for a large proportion of the market and throughout the world. Despite its considerable potential, fingerprint recognition suffers from insufficient accuracy and security concerns[9]. Biometric devices are mainly used to provide non-repudiable identification. Health-care, financial, retail, education, manufacturing, military, and law enforcement agencies rely on these systems for authentication. Applications based on biometrics present several security concerns, including the risk of stolen biometrics, replacing compromised biometrics, administrative fraud, outages, and intrusion. Additionally, the biometric system may falsely accept an impostor or reject a genuine user due to its limitations[10]. In the days before smartphones with embedded fingerprint sensors became available, fake fingers were created to attack the system and ultimately succeeded. A person's fingerprint can be stolen by taking a photo of it from a certain distance[11]. A successful presentation attack allows an adversary to «impersonate» a genuine user and obtain access to confidential data by gaining access to a system[4]. The extensive use of fingerprint sensing biometric devices is worthless if artificial fingerprint replicas can fool biometric devices. This can be misused for illicit purposes. Not only can this pose a threat to society, but it can also mislead criminal investigations[12]. In the event of a biometric spoofing attack on Aadhaar, untold numbers of people could be affected, including companies and governments as now India is possibly the world's largest biometric database[13]. Consider also the United States Office of Biometric Identity Management (US OBIM), which is responsible for supporting the Department of Homeland Security with biometric identification services specifically designed to prevent unnecessary entry into the country by people who pose a threat to the country. The failure to detect spoofs on OBIM systems could result in a deadly terrorist attack[14]. If spoof attacks succeed, emails, bank information, social media content, personal photos, and a plethora of other confidential information can get compromised[5]. Likewise, fingerprint detection is prone to some vulnerabilities concerning forensics, commercial and military applications[15].

3. Mitigation steps, current research and case studies

The need to detect and prevent presentation attacks are predominant due to the high costs and loss of user privacy associated with spoofed systems[14]. The literature mentions several ways to detect presentation attacks to mitigate the costs associated with them[14]. A number of solutions have been proposed to prevent fraudulent attacks by artificial fingers. A range of approaches have been developed to measure fingertip temperature, pulse, blood pressure, electric resistance, or ECG. Dedicated fingerprint hardware is required for these methods. Such hardware is expensive, bulky, and sometimes inconvenient[16]. Chugh et al. (2019) took advantage of the dynamics that is involved in imaging of fingerprint by a touch-based fingerprint reader such as perspiration, changes in colour (blanching), and skin distortion detect spoof fingers on a deep learning touch-based fingerprint reader[3]. Abhishek et al. (2015) discussed a novel method to detect fake fingerprints based on the minutiae count. Using the standard FVC (Fingerprint Verification Competition) 2000 – 2006 dataset, the accuracy of the proposed algorithm was reported to be well above 85 %[17]. Akbari et al. (2012) deployed an algorithm for automation fingerprint recognition on the OCT (Optical Coherence Tomography) fingerprint images and this was based on scanning of the enhanced and segmented OCT images[18]. Pathan et al. (2019) came up with a solution that is based mainly on the fingerprints to prove the user's identity. The idea for this was to store the fingerprints of more than one finger and combine each fingerprint with a secure password. The password consists of the fingers order or sequence in hand add a secure password[19]. Uliyan et

al. (2019) employed Discriminative Restricted Boltzmann Machines to identify fingerprints that are accurately against fabricated materials used for spoofing of fingerprint[20]. Sharma et al. (2012) addressed a prevention method that multi-model biometrics system that uses multiple sensor or biometrics to overcome the limitation of unimodal biometrics system. Like fingerprint can be used with iris, palm, or face can be combined for identification purposes[21]. Saharan et al. (2020) proposed a novel protocol named C stain based chemical method which is developed to recognize forged fingerprints from real ones, on the basis of colour difference. C stain method is an effective way to distinguish forged fingerprints from authentic ones. Even when combined with existing development methods, it works as a distinction tool[22]. Detecting deepfakes is a difficult task due to the rapid development of generative models and the possibility of adversarial countermeasures[23]. Ishfaq et al. (2021) outlined that the paradigm has shifted from conventional hardware-based approaches to deep features-based approaches for detecting fingerprint presentation attacks since 2014. The study also shows the deep learning-based fingerprint presentation attacks detection methods exhibit a trade-off between the time it takes to build the model and the accuracy of its prediction. In the future, the research may focus on developing more robust deep learning models for fingerprint presentation attacks detection[24].

In sept. 2013, shortly after Apple released the iPhone 5s with TouchID fingerprint technology, Chaos Computer Club[2] used a high-resolution photograph of the enrolled user's fingerprint in order to fabricate a spoof fingerprint using wood glue. An arrest was made in 2013 March, when a Brazilian doctor tried to defeat the biometric attendance system at a hospital in Sao Paulo using spoof silicone fingers[8]. Using wax molds casted with wood glue, a gang in Rajasthan, India bypassed biometric attendance systems in 2018 March to provide proxies for Police Academy entrance exams[3]. Police discovered vague fingerprints on a woman whose fidgety behaviour caught their attention in June 2007. The woman admitted that she paid $ 2 000 for a surgery to alter her fingerprints so she could enter the United States illegally. Based on a case in January 2009, in which a woman deceived the system by covering up her true fingerprints with tape-made fake ones, Japan's border control has been upgraded to make fingerprints more reliable[25].

4. Discussion

Using fingerprints for identification is becoming an increasingly common practice, and it serves as a valuable tool around the globe. Forging these inescapable marks is possible with materials that are commonly available in the market. With impersonation of identity with fingerprints is a threat to forensics, commercial and national security. Impersonating own identity or obfuscating fingerprints can lead a person to cross all the security and recognition measures. In 2017, biometrics expert Anil Jain and his team at Michigan state university created the first wearable finger that mimics human skin. The mechanical, optical, and electrical properties match that of a human finger. With this artificial fingerprint, anyone can use it as a password that can be used for different devices while providing a different fingerprint password to use on each. Instead of using original fingerprints that adhere to vulnerability, these artificial fingerprints can make it hard to crack the security. The disadvantage of this fake fingerprint when it comes to forensics, commercial and national security it is vulnerable to identity theft, cross-border terrorism, and financial theft. In 2017, Japan's National Institute of Informatics (NII) researchers announced that they have successfully extracted usable fingerprints from photos of exposed fingers that is taken up to three meters away. Isao Echizen, National Institute of Informatics (NII)'s Digital Content and Media Sciences Research Division researcher, informed that modern phone cameras are powerful enough to capture sufficient fingerprint details, if users expose their fingers to the camera. Researchers took a subject's photo with a high-resolution camera from 9 feet away. They then recreated the subject's fingerprints with 100 % accuracy. And these copied fingerprints could be used to unlock personal devices or sign into bank accounts. On June 2021, Indian police, arrested a biometric spoofing gang for online bank fraud using cloned fingerprints. The use of fingerprints as a security password system is still vulnerable as any other word password.

5. Conclusion

According to several research papers reviewed, there is always the possibility of fingerprint forgery, and that it is a crucial part of crimes. The reviewed literatures shown the detection techniques and prevention methods to tackle fingerprint forgery. But with the improving and developing technologies the methods of forging will also evolve. To conclude, as things develop, fingerprint forgeries are also finding loopholes, so new identification and prevention methods are necessary to combat fingerprint forgeries.

[1] Maro, E., & Kovalchuk, M. (2018). Bypass Mobile Lock Systems with Gelatin Artificial Fingerprint.

[2] Gao, Q. (2014). A Preliminary Study of Fake Fingerprints. International Journal of Computer Network and Information Security, 6, 1 – 8.

[3] Chugh, T., & Jain, A.K. (2020). Fingerprint Spoof Detection: Temporal Analysis of Image Sequence. 2020 IEEE International Joint Conference on Biometrics (IJCB), 1 – 10.

[4] Kauba, C., Debiasi, L., &Uhl, A. (2020). Enabling Fingerprint Presentation Attacks: Fake Fingerprint Fabrication Techniques and Recognition Performance. ArXiv, abs/2012.00606.

[5] Cao, K., & Jain, A. K. (2016). Hacking Mobile Phones Using 2 D Printed Fingerprints.

[6] Champod, C., & Espinoza, M. (2014). Forgeries of Fingerprints in Forensic Science. Handbook of Biometric Anti- Spoofing.

[7] Hildebrandt, M. (2015). Feature space fusion and feature selection for an enhanced robustness of the fingerprint forgery detection for printed artificial sweat. 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 1 – 6.

[8] Chugh, T., Cao, K., & Jain, A. K. (2018). Fingerprint Spoof Buster: Use of Minutiae-Centered Patches. IEEE Transactions on Information Forensics and Security, 13, 2190 – 2202.

[9] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11, 141.

[10] Joshi, M., Mazumdar, B., & Dey, S. (2018). Security Vulnerabilities Against Fingerprint Biometric System. ArXiv, abs/1805.07116.

[11] Goicoechea-Telleria, I., Sánchez-Reillo, R., Liu-Jimenez, J., & Blanco-Gonzalo, R. (2018). Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone? Wirel. Commun. Mob. Comput., 2018.

[12] Nayak, S., Pati, P., Sahoo, S., Nayak, S., Debata, T., &Bhuyan, L. (2019). Artificial finger with dental alginate impression material can fool the sensorof various finger print systems. Journal of Indian Academy of Forensic Medicine, 41, 2.

[13] Rajput, A., & Gopinath, K. (2017). Towards a More Secure Aadhaar. ICISS.

[14] Engelsma, J.J., Cao, K., & Jain, A. K. (2017). RaspiReader: An Open-Source Fingerprint Reader Facilitating Spoof Detection. ArXiv, abs/1708.07887.

[15] Syifaa'Ahmad, A., Hassan, R., & Ahmad, M. N. (2019). Fake Fingerprint Detection Approaches: A Systematic Review.

[16] Tan, B., &Schuckers, S. (2010). Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. Pattern Recognit., 43, 2845 – 2857.

[17] Abhishek, K., & Yogi, A. (2015). A Minutiae Count Based Method for Fake Fingerprint Detection. Procedia Computer Science, 58, 447 – 452.

[18] Akbari, N., & Sadr, A. (2012). Automation of Fingerprint Recognition Using OCT Fingerprint Images. Journal of Signal and Information Processing, 2012, 117 – 121.

[19] Pathan, S. (2019). Fingerprint Authentication Security: An Improved 2-Step Authentication Method with Flexibility. International Journal of Scientific and Engineering Research, 1 – 7.

[20] Uliyan, D. M., Sadeghi, S., &Jalab, H. A. (2020). Anti-spoofing method for fingerprint recognition using patch based deep learning machine. Engineering Science and Technology, an International Journal, 23, 264 – 273

[21] Sharma, M. (2014). Detection and Prevention of Fingerprint Altering / Spoofing Based on Pores (Level-3) With the Help of Multimodal Biometrics.

[22] Saharan, S., Yadav, A., & Yadav, B. (2020). Novel C stain-based chemical method for differentiating real and forged fingerprints. Egyptian Journal of Forensic Sciences, 10, 1 – 8.

[23] Yu, N., Skripniuk, V., Abdelnabi, S., & Fritz, M. (2020). Artificial Fingerprinting for Generative Models: Rooting Deepfake Attribution in Training Data.

[24] Ishfaq, R., Selwal, A. K., & Sharma, D. (2021). Fingerprint Spoofing Attacks and their Deep Learning-enabled Remediation: State-of-the-art, Taxonomy, and Future Directions. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), 22 – 28.

[25] Jain, A. K. (2009). Fingerprint Alteration.

Арыстанбеков М. А.,
ведущий научный сотрудник
Научного центра правовых, экономических
и социологических исследований, д-р юрид. наук, доцент
(Академия «Bolashaq», Республика Казахстан, г. Караганда)

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Рассмотрение перспектив использования искусственного интеллекта в рамках борьбы с преступностью представляет неподдельный интерес.Научные изыскания в данной области направлены на создание информационно-поисковых, справочно-аналитических систем и баз данных, оказывающих влияние на построение версий их проверку в различных типичных следственных ситуациях, на проведение следственных действий и на построение частных методик расследования[1].

В целях оптимизации процесса расследования разрабатываются следующие направления использования искусственного интеллекта:

- моделирование ранее совершенного преступления и его следов;

- оценка достаточности добытых доказательств;
- прогнозирование и профилактика совершения преступлений;
- стратегическое исследование оперативной обстановки и т. д.[2]

Исходя из указанных направлений использования искусственного интеллекта, в криминалистике разрабатываются различные проекты для решения некоторых задач, возникающих в процессе раскрытия и расследования преступлений.Одним из известных проектов является база данных, в которую занесены основные элементы криминалистической характеристики[3]. Другим проектом является система позволяющая формировать наиболее перспективные версии о личности преступника[4].

Эти проекты ориентированы на выдвижение вероятных версий. Однако созданные программы работают с типичными версиями достаточно успешно, но при выдвижении нетипичных версий их возможности значительно уменьшаются.И этому есть оправдание, возможность создания программ во всем многообразии следственных ситуаций, с которыми сталкивается следователь в своей повседневной деятельности при решении нестандартных задач раскрытия и расследования преступления, в полном объеме невозможно и они недоступны для компьютерной обработки.

Но здесь и возникает вопрос о создании не только программных комплексов, но и о создании искусственных нейронных сетей, как класса методов искусственного интеллекта. При этом, искусственный интеллект необходимо рассматривать, не только как программный комплекс обработки данных.

Основным качеством искусственного интеллекта и в частности нейронных сетей является способность к адаптивному ситуационному обучению за счёт применения решений множества сходных задач. Тем самым его возможности могут быть приближены к мышлению лиц, осуществляющих расследование.

Это выражается в том, что создатель сети задает помимо общих правил анализа данных, данные для ее обучения. Последние должны быть непротиворечивыми и предельно достоверно отображать характеристики анализируемого процесса или явления. К таким данным можно отнести сведения: о раскрытых и нераскрытых преступлениях; механизме и обстановке их совершения; наличие и характеристику связей между преступником и потерпевшим и т. д.[5]

При этом сам процесс создания искусственной нейронной сети состоит из нескольких этапов.На первом этапе происходят сбор и обобщение данных, которые впоследствии будут использованы для обучения сети. Информацию необходимо загружать в сеть так, чтобы ее нельзя было перепутать. В противном случае возможна ошибка при анализе ситуации. Сложность решаемой задачи заключается в обработке большого массива схожих уголовных дел и других материалов, а также ее трансформация в цифровую форму для детализации и анализа.

На втором этапе осуществляется подбор параметров обучения. Они должны быть настроены на постоянное обновление алгоритмов обучения путем вмешательства разработчика и путем самостоятельного развития по заранее заданным параметрам.

На третьем этапе происходит проверка соответствия сети ее целям создания[6].

После этого возможности искусственных нейронных сетей могут быть реализованы:
- в оценке исходной информации в целях выдвижения следственных версий и их проверки;
- в моделировании события преступления и его следовой картины;
- в реконструкции способа совершения преступления и его сокрытия;
- в выявлении признаков повторяемости в условиях информационной недостаточности;
- в распознавание образов — автоматическое распознавание лиц и др.;
- в дополнительной оценке достаточности собранных доказательств;
- в прогностических целях развития оперативной обстановки и совершения преступления в будущем и т. д.[7]

Помимо этого, искусственные нейронные сети могут быть адаптированы для решения специфических задач: для выявления следственных ошибок процессуального и тактического характера; выявления ошибок по применению технико-криминалистических средств и методов; неиспользованных возможностей судебных экспертиз и т. д.

Однако одна из главных проблем, связанная с искусственным интеллектом, состоит в том, что зачастую механизмы его работы непрозрачны, и в случае ошибки невозможно определить, что к ней привело и как избежать ее повторения в будущем. При этом понятно, что разработчиками самообучающихся систем и их потребителями должны быть должностные лица правоохранительных и судебных органов, имеющих соответствующее образование и положительный опыт работы в данной сфере

деятельности, для того чтобы исправить допущенные сетью ошибки, и для того чтобы информация по уголовному делу не распространилась в социальных сетях.

В ближайшем будущем вполне возможна более широкая интеграция рассмотренной технологии в следственную практику, где сети будут выступать как вспомогательные возможности для обеспечения эффективности расследования, и любые типы искусственного интеллекта могут быть апробированы к процессу расследования, а почему нет? Однако для этого требуется дальнейшее изучение возможностей искусственных нейронных сетей и способы их внедрения в процесс расследования.

---

[1] Грицаев С. И., Помазанов В. В., Заболотная Ю. А. Компьютеризация целеопределения и планирования расследования // Научн. журн. КубГАУ. — 2015. — № 108. — С. 491 – 499.

[2] Лабинский А. Ю., Подружкина Т. А. Особенности использования генетических алгоритмов и нейронных сетей // Природные и техногенные риски (физико-математические и прикладные аспекты). — 2015. — № 4. — С. 56 – 61.

[3] Нелюбин К. А. Некоторые вопросы создания и использования электронной базы данных на основе криминалистической характеристики убийств // Российский следователь. — 2014. — № 13. — С. 3 – 5.

[4] Фесик П. Ю. Технология использования криминалистической характеристики в раскрытии убийств: Автореф. дис. ... канд. юрид. наук. — Н. Новгород, 2011.

[5] Василова Д. И. Искусственный интеллект в криминалистике // Информационные технологии в науке и образовании: Мат-лыВсеросс. науч.-практ. конф. [Электронный ресурс]. — Режим доступа: http://econf.rae.ru/article/11543 (дата обращения: 01.11.2021).

[6] Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. — 2018. — С. 44 – 45.

[7] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел. — М., 2005.

Аубакирова А. А.,
профессор кафедры уголовного права, уголовного процесса
и криминалистики, доктор юридических наук,
профессор, полковник полиции
(Алматинская академия МВД Республики Казахстан им. М. Есбулатова)

Инновационные технологии в криминалистике

«Стремительные, динамичные изменения в социальной структуре общества порождаются лавинообразным процессом инноваций, материализованных научных идей, научных открытий, технических изобретений и разработок, с принципиально новыми технологическими процессами»[1, 7 – 8]. Данный тезис был высказан профессором Михаилом Гавриловичем Лазаром еще в конце 70-х годов, но остается остро актуальным и в настоящее время.

Р.С. Белкин справедливо отмечал, что криминалистика резко увеличивает свой научный потенциал и повышает практическую эффективность в условиях «информационного взрыва». При этом причинами ускоренного развития криминалистики автор назвал:

- возрастающий объем фундаментальных и прикладных исследований в криминалистике, о чем свидетельствует увеличение количества монографий и диссертационных работ;
- ускоренное развитие тех отраслей знаний, данные которых используются в криминалистике;
- повышение общественной значимости криминалистики в связи с растущей актуальностью проблемы борьбы с преступностью;
- растущий в силу объективных факторов, порожденных научно-техническим прогрессом, потенциал криминалистики как науки[2].

В настоящее время существует множество направлений, в которых инновации помогают в раскрытии и расследовании уголовных правонарушений, среди которых можно назвать и алгоритм распознавания лиц, и анализ отпечатков пальцев, и микробиологическая идентификация человека и многие другие.

В рамках моего выступления на сегодняшней конференции мне хотелось бы остановить на законодательном регулировании некоторых инновационных проектов, имеющихся в Республике Казахстан.

Закон Республики Казахстан «О дактилоскопической и геномной регистрации» от 30 декабря 2016 г. № 40-VI ЗРК. Согласно данному закону, дактилоскопическая и геномная информация относится к персональным данным ограниченного доступа. Отсюда следует, что защита дактилоскопической и геномной информации осуществляется в соответствии с законодательством Республики Казахстан об информатизации, о персональных данных и их защите, государственных секретах, в том числе в

форме административной и уголовной ответственности. Несмотря на принятие данного закона, до настоящего времени он не вступил в законную силу, так как некоторые положения до сегодняшнего дня не урегулированы и его действие начнется не раньше 2023 г.

С одной стороны — мощный рывок в законодательном плане, обязывающий граждан РК, иностранцев и лиц без гражданства пройти обязательную дактилоскопическую и геномную регистрацию, с другой стороны — активное противодействие исполнению норм данного закона.

Вторая проблема — использование беспилотных летательных устройств. К аэросъемке прибегают для «фиксации масштабных мест происшествий, таких как места крушения воздушных судов, обширных мест техногенных происшествий, то есть тех мест, которые сложно полностью запечатлеть несколькими кадрами с земли, для формирования полного представления об обстановке происшествия»[3]. Приказом и. о. Министра индустрии и инфраструктурного развития Республики Казахстан «Об утверждении правил эксплуатации беспилотных летательных аппаратов в воздушном пространстве Республики Казахстан» от 31 декабря 2020 г. № 706 регламентировано то, что согласование выполнения полетов и выдача разрешений на использование воздушного пространства беспилотных летательных аппаратов категории операций «специфическая» для всех видов авиации производится центрами при предоставлении плана полета в порядке, предусмотренном специфическими Правилами. То есть каждое применение должно осуществляться квалифицированным сотрудником, имеющим не только специальные разрешения, но и опыт, играющий немаловажную роль в получении достоверного результата, эффективности любого следственного действия, проводимого в рамках расследования уголовного дела, что также приводит к детальной правовой регламентации, которая в настоящее время отсутствует.

Третья проблема — применение полиграфа в расследовании уголовных правонарушений. Постановлением Правительства Республики Казахстан «Об утверждении Правил прохождения полиграфологического исследования в правоохранительных органах Республики Казахстан» от 19 июня 2014 г. № 683 регулируется порядок прохождения полиграфологического исследования гражданами, а также сотрудниками правоохранительных органов Республики Казахстан. Основной целью прохождения исследования является получение дополнительной информации и проверка достоверности сведений, сообщаемых гражданами, принимаемыми на службу в правоохранительные органы, на учебу в организации образования правоохранительных органов и сотрудниками правоохранительных органов Республики Казахстан для использования данного прибора в кадровой службе. Однако всем известно, что широкое применение полиграфа в раскрытии и расследовании преступлений порой имеет очень большое значение. Более того Законом «О правоохранительной службе» было определено применение полиграфа в следующих случаях:

В отношении граждан желающих поступить на службу в правоохранительные органы РК — ст. 6, п. 5: «Принимаемые на службу в правоохранительные органы граждане в обязательном порядке для определения пригодности к службе проходят в военно-врачебных комиссиях медицинское и психофизиологическое освидетельствования и полиграфологическое исследование в соответствующем подразделении правоохранительного органа...».

В отношении сотрудников правоохранительных органов при прохождении очередной аттестации — ст. 47 п. 5, пп. 3-1: «Аттестация включает в себя ряд последовательных этапов: … прохождение полиграфологического исследования».

А в отношении сотрудников правоохранительных органов при осуществлении служебных расследований — ст. 58, п. 1: «… По необходимости при проведении служебного расследования проводится полиграфологическое исследование» (пункт исключен 03.07.14 г. № 227-V).

Инновации, которые можно было бы применять в правоприменительной практике с криминалистической точки зрения ввиду их несоответствия ст. 126 УПК РК «Научно-технические средства в процессе доказывания» не согласуются с нормами закона. Согласно ч. 3 ст. 126 УПК РК применение научно-технических средств признается допустимым, если они:

1) прямо предусмотрены законом или не противоречат его нормам и принципам;

2) научно состоятельны;

3) обеспечивают эффективность производства по уголовному делу;

4) безопасны.

То есть ссылка законодателя на прямое предусмотрение законом научно-технического средства сильно ограничивает правоприменителя в использования инноваций в криминалистике и судопроизводстве.

В соответствии с приказом Генерального Прокурора Республики Казахстан «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий» от 22 сентября 2014 г. № 91 полагается, что «фиксация хода и результатов следственных действий возможна лишь при условии применения аудио/видеозаписывающих устройств».

Интересен в этой связи выход, предложенный профессором Е. Н. Бегалиевым в монографии «Новеллы в современной криминалистике». Он пишет, что «… в целях успешного раскрытия и расследования преступлений, представляется необходимым систематическое освещение тактико-технических характеристик и алгоритмов применения отдельных разновидностей НТС, в структуре интегрированного реестра технических средств, в формате программного продукта или мобильного приложения, с обязательным предоставлением доступа сотрудникам правоохранительных органов и экспертных подразделений»[4].

Не будем отрицать, что в условиях тотальной цифровизации всех сторон жизни, в том числе и уголовного судопроизводства, внедрение в практику раскрытия и расследования отдельных видов преступлений современных достижений научно-технического прогресса, а также адаптированных из естественно-технических наук, позволили в значительной степени материально оснастить оперативную, следственную и экспертную деятельность подразделений правоохранительных и специальных органов. На наш взгляд, является вполне оправданным развитие и внедрение технологий в предметную область криминалистической техники, путем адаптации цифровых средств передачи информации, с возможностью ее дальнейшей фиксации и исследования.

---

[1] Лазар М. Г., Лейман И. И. НТР и нравственные факторы научной деятельности. — Л., 1978.

[2] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. — М., 2001. С. 17, 68 – 91.

[3] Иванов Д. С. Применение правоохранительными органами беспилотных летальных аппаратов при раскрытии и расследовании преступлений // Исследования молодых ученых: Мат-лы XIV Международ. науч. конф. (г. Казань, ноябрь 2020 г.). — Казань, 2020. С. 37 – 39. [Электронный ресурс]. — Режим доступа: https://moluch.ru/conf/stud/archive/382/16088/ (дата обращения: 07.10.2021).

[4] Бегалиев Е. Н. Новеллы в современной криминалистике» монография. — Алматы, 2020.

Бекжанов М. А.,
доцент, полковник национальной безопасности
(Академия КНБ Республики Казахстан, г. Алматы)

ИНФОРМАЦИОННЫЕ СЕТИ КАК ЭЛЕМЕНТ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ, УЯЗВИМЫХ В ТЕРРОРИСТИЧЕСКОМ ОТНОШЕНИИ

В целях снижения рисков совершения актов терроризма, минимизации и ликвидации их последствий в нашей стране выстроена система противодействия терроризму, важным элементом которой является сфера антитеррористической защиты объектов, уязвимых в террористическом отношении (далее — объекты УТО).

На указанных объектах, в соответствии с п. 1 ст. 10-3 Закона Республики Казахстан «О противодействии терроризму»[1], с 2013 г. в обязательном порядке исполнялись требования по организации их антитеррористической защищенности, которые являются предметом государственного контроля.

Руководители или иные должностные лица объектов УТО, независимо от форм собственности, с целью предупреждения террористической деятельности, а также антитеррористической защиты объектов и соблюдения должного уровня их безопасности обязаны реализовывать мероприятия по:

1) обеспечению соответствующего пропускного режима, оснащению объектов современным инженерно-техническим охранным оборудованием в соответствии с предъявляемыми к ним требованиями;

2) разработке на основе типового паспорта — паспорта антитеррористической защищенности вверенных им объектов;

3) проведению профилактических и учебных мероприятий по обучению персонала технике осмотра помещений, выявлению возможных мест закладки взрывных устройств;

4) планированию и отработке совместных действий с заинтересованными государственными органами и организациями по ликвидации угроз техногенного характера, возникших в результате совершенного акта терроризма;

5) организации защиты информационных сетей объекта, обеспечения информационной безопасности.

В соответствии с Законом РК «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам противодействия легализации доходов, полученных преступным путем и финансированию терроризма»[2] внесены изменения в Закон РК «О противодействии терроризму» которые исключили норму (пп. 5 п. 1 ст. 10-3) связанную с организацией защиты информационных сетей объекта и обеспечению информационной безопасности. Отсюда возникает проблема, которая выражается в том, что при организации антитеррористической защиты объектов УТО не обеспечивается их информационная безопасность. Изложенное приводит к противоречию, которое формируется между необходимостью обеспечения надежного уровнябезопасности объекта, и несовершенством нормативной правовой базы, которая не учитывает современные террористические угрозы, среди которых кибератаки на информационные системы.

Актуальность проблемы обусловленавозрастающими угрозами террористической деятельности для объектов УТО, совершенствованием тактики, форм и методов реализации актов терроризма. Риски также увеличивает и пандемия коронавируса, которая способствовала переводу режима работы персонала большинства объектов на дистанционный формат, открывая возможности по проникновению в информационные сети, тем самым не исключая нанесение ущерба нормальному функционированию объектов УТО.

В сегодняшнем высоко технологически и индустриальном мире, сложно представить объекты, не имеющие информационные системы. Наряду с широкими возможностями информатизация, включая глобальную, создает широкий спектр глобальных проблем: от дестабилизации обществ на фоне цифрового неравенства, до криминализации технологий и даже их использованию в качестве оружия. Крупнейшие кибератаки последних лет вызывали подрыв систем жизнеобеспечения, компрометацию замыслов правоохранительных и специальных служб, обнародованию персональных данных и личных тайн, и, как правило, носили политический характер.

Почему же тогда указанную норму исключили из сферы антитеррористической защиты объектов УТО?Начнем с того, что ранее защита информационных сетей, являясь обязанностью, как бы «перекладывалась» на руководителя объекта УТО, нос практической стороны, например, в процессе государственной проверки объектов сотрудниками полиции, по сравнению с другими обязанностями, не контролировалась.

Происходило это потому, что компоненты системы антитеррористической защиты (инженерно-техническая укрепленность периметра, система видеонаблюдения, охранной сигнализации, контроля и управления доступом, освещения, оповещения, связи) являются как бы «материальными», т. е. их наличие, работоспособность, соответствие требуемым параметрам может визуально проконтролировать любой сотрудник полиции, даже не обладающий знаниями в сфере антитеррористической защиты объектов УТО (достаточно «Проверочного листа в сфере государственного контроля за состоянием объектов УТО», где все прописано, только ставь галочки (после изменений тоже утратил силу).

Для проверки же информационной безопасности необходимо обладать специфическими знаниямив сфере IT-технологии. У МВД имеются подразделения, занимающиеся данным направлением, но это уже дополнительная функция, а это значит отвлечение сил и средств.

Кроме того, согласно ст. 15 Закона «О национальной безопасности»[3], в Республике Казахстан существует уполномоченный орган в сфере обеспечения информационной безопасности, который разрабатывает правовые, административные и иные меры по обеспечению информационной безопасности, осуществляет контроль их реализации и соблюдения, а также межведомственную координацию деятельности по обеспечению информационной безопасности.

В настоящее время сфера информационной безопасности (далее — ИБ) регламентирована следующими основными нормативными правовыми актами: Законом РК «Об информатизации», постановлениями Правительства РК «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуника-

ционной инфраструктуры», «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

Согласно данным правовым актам устанавливаются единые требования обязательные для исполнения в области информационно-коммуникационных технологий и обеспечения ИБ госорганами, органами местного самоуправления, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрированных с информационными системами госорганов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры[4].

Таким образом, для объектов УТО, попадающих под вышеперечисленные категории, уполномоченным органом выработаны требования к ИБ и осуществляется соответствующий контроль.

В этой связи, для устранения дублирования правовых норм и контрольных функций госорганов, данное направление вывели из-под контроля по линии антитеррористической защиты и оставили под контролем уполномоченного органа в сфере обеспечения информационной безопасности.

Но при этом образовалась ниша, в которую попали объекты УТО, не обладающие значимой информационно-коммуникационной инфраструктурой, для которых требования к ИБ компетентными органами не разрабатывались и никем не контролируются.(Справочно: по состоянию на 1 сентября 2020 г. в РК зарегистрировано 17 381 объект УТО: из них 10 680 (61 %) — объекты, подведомственные государственным органам, 6 701 (39 %) объектчастной формы собственности)[5].

Среди указанных имеются объекты, затрагивающие практически все сферы жизнедеятельности человека и общества, от мест массового скопления до стратегических и опасных производственных предприятий. Получается, чтообеспечивать их информационную безопасность не обязательно, зачем руководителю отвлекать на это дополнительныефинансовые ресурсы. (Справочно: информационные сети международной специализированной выставки ЭКСПО – 2017 (объект УТО) были размещены за «Единым государственным шлюзом» доступа к интернету, что потребовало значительных финансовых средств).

В рамках статьи изучен зарубежный опыт по вопросам антитеррористической защиты объектов, в частности Российской Федерации. Так, в Законе РФ «О противодействии терроризму»[6] заложены организационно-правовые основы, регламентирующие эту сферу, которые развиваются в подзаконных правовых актах, а именно в постановлении Правительства РФ «Об антитеррористической защищенности объектов (территорий)»[7], где расписаны меры, которые должны быть учтены при разработке требований к системе защиты объектов той или иной отрасли. На основе этого документа были разработаны и утверждены постановления Правительства по сферам деятельности. В частности, требования к антитеррористической защищенности объектов спорта, мест массового пребывания людей и т. д.

В указанных правовых актах отмечено, что руководитель является ответственным за антитеррористическую защищенность объекта. Однако перечень обязанностей должностных лиц, включая защиту информационных сетей, не прописан. При этом в требованиях указано, что для каждой категории объектов (территорий) устанавливается комплекс мер, соответствующих степени угрозы совершения террористического акта и его возможным последствиям.

Подобное примечание отражено и в постановлении Правительства РК № 305 «Требований к организации антитеррористической защиты объектов, уязвимых в террористическом отношении» (далее — Требования)[8]. В данном постановлении прописан шаблон единых требований к организации антитеррористической защиты объектов УТО, на основании которого каждый государственный орган обязан разработать «Инструкцию по организации антитеррористической защиты объектов» (далее — Инструкция) и подробно прописать эти требования применительно к своей отрасли.

В частности, одним из общих принципов антитеррористической защиты объекта является заблаговременность (превентивность) проводимых мероприятий — который подразумевает комплекс мер, разрабатываемых заранее с учетом характера и специфики террористических угроз (комплексность также присутствует).

Это означает, что на объекте УТО должна применяться комплексная система безопасности, с интегрированными между собой подсистемами и компонентами внутри них. На таких объектах информация о нарушении защиты поступает в пункт централизованной охраны не только от классических (контроля доступом, видеонаблюдение, сигнализации и др.), но и от смежных систем (инженерных,

информационных, контрольно-измерительных, автоматизированного управления технологическими процессами и т. д.), а это подразумевает обязательный учет всех возможных видов угроз (несанкционированного входа на объект, доступа в информационные системы, вывод из строя оборудования, нарушения технологического, иных процессов и многое др.).

Учитывая, что в настоящее время идет активная фаза разработки каждым государственным органом Инструкции по организации антитеррористической защиты, следует отразить в них вопросы, связанные с принятием мер по обеспечениюзащиты информационных сетей и информационной безопасности на объекте УТО (не обязательно, чтобы она подпадала под контроль сотрудников полиции, главное соблюдение требований). Так как не все руководители объектов до конца понимают содержание выражения «характер и специфику террористических угроз» (в их классическом понимании это взрыв, захват заложников, отравление, автотаран и др.).Так же, как это прописано в п. 80 Параграфа 2 Требований к объектам, для которых актуальны угрозы, связанные с доставкой и применением средств террора посредством беспилотных летательных аппаратов, рекомендуется предусматривать системы противодействия беспилотным летательным аппаратам.

Защитив внутренние информационные сети, руководитель тем самым обеспечивает и информационную безопасность комплексной системы защиты объекта, основу которойсоставляет единая аппаратно-программная платформа, с многоуровневой структурой, имеющей общий центр управления.

Кроме того, принимая во внимание, что затраты на информационную безопасность постоянно возрастают и во избежание риска несанкционированного доступа или нанесения преднамеренного ущерба, необходимо также отразить вопросцелесообразности подключения/отключениявнутренней информационной сети объекта кинтернету /оттнтернета.

В свою очередь при прохождении процедуры согласования, контролирующие органы в лице КНБ и МВД РК должны учитыватьналичие указанных норм вотраслевых Инструкциях.

Приняв такие меры, государство донесет до руководителей объектов УТО идею о том, что информационная безопасностьявляется неотъемлемой составляющей обеспечения национальной безопасности, которая в сочетании с концепцией «Киберщит Казахстана» позволит предупредить террористические угрозы в киберпространстве.

---

[1] Закон Республики Казахстан «О противодействии терроризму» от 13 июля 1999 г. № 416-I. [Электронный ресурс]. — Режим доступа: http: online.zakon.kz/Document/dosid=1013957 (дата обращения: 01.11.2021).

[2] Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 13 мая 2020 г. № 325-VI. [Электронный ресурс]. — Режим доступа: http: adilet.zan.kz/Z200000325 (дата обращения: 01.11.2021).

[3] Закон Республики Казахстан «О национальной безопасности» от 6 января 2012 г. № 527-IV. [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=311068 60 (дата обращения: 01.11.2021).

[4] Справочный материал заседания АТЦ РК. Штаб АТЦ РК, апрель 2018 г.

[5] Статистические сведения по объектам УТО РК. Штаб АТЦ РК, сентябрь 2020 г.

[6] Закон Российской Федерации «О противодействии терроризму» от 6 марта 2006 г. № 35-ФЗ. [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_58840/ (дата обращения: 01.11.2021).

[7] Постановление Правительства Российской Федерации «Об антитеррористической защищенности объектов (территорий)» от 25 декабря 2013 г. № 1244. [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=31490451 (дата обращения: 01.11.2021).

[8] Постановление Правительства Республики Казахстан «Требования к организации антитеррористической защиты объектов, уязвимых в террористическом отношении» № 305 от 6 мая 2021 г. [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id= 36723888 (дата обращения: 01.11.2021).

Брушковский К. Б.,
ассоциированный профессор кафедры «Юриспруденция»
Высшей школы права «ӘДІЛЕТ», кандидат юридических наук;
Алмаганбетов П. А.,
ассоциированный профессор кафедры «Юриспруденция»
Высшей школы права «ӘДІЛЕТ», кандидат юридических наук
(Каспийский общественный университет,
Республика Казахстан, г. Алматы)

КРИМИНАЛИСТИЧЕСКАЯ ОДОРОЛОГИЯ — СОВРЕМЕННАЯ ВОЗМОЖНОСТЬ ИДЕНТИФИКАЦИИ ЧЕЛОВЕКА

Совершаемые преступления в Республике Казахстан нередко носят характер хорошо продуманных и организованных, что заставляет криминалистов изыскивать нетрадиционные средства и методы для использования в их раскрытии и расследовании. Установление лица, оставившего свои следы на месте преступления, занимает при этом центральное место в теории криминалистической идентификации и в методике расследования преступлений. Обыденной практикой становится изъятие с мест происшествий следов человека биологического происхождения (следы крови, запаха, пота, волосы и др.).

В решении идентификационных задач определенное место отводится и одорологическому исследованию следов человека, проводимой ольфакторным (обонятельным) методом с использованием непривычных в криминалистике биологических датчиков — специально подготовленных собак-детекторов. Данный метод все активнее внедряется в практику оперативно-криминалистических подразделений органов внутренних дел РК он уже доказал перспективность при расследовании особо опасных преступлений. Использование сенсоров живых существ в химии и биологии считается одним из эффективных научных подходов в решении сложных исследовательских задач. Но использование животных в криминалистической практике вызывает противоречивые мнения в связи с не всем понятным их статусом, казалось бы, размывающим привычные представления о субъекте проводимого исследования. Не меньше вопросов возникает также в связи с природой запаховых следов человека, их выявлением и анализом, ролью специалистов в этом процессе, наличием и объемом требуемых для этого специальных знаний. Многие положения «криминалистической (судебной) одорологии» требуют взвешенной оценки.

Руководством МВД РК прилагаются усилия по расширению практики использования данного метода. Это определяет актуальность разработки проблемы, требуется, в частности, решить ряд вопросов по улучшению условий работы созданных ранее отделений (групп) исследований и экспертиз пахучих следов человека в РК. За последнее десятилетие с помощью одорологических исследований были раскрыты многие опасные преступления, такие как убийства, изнасилования, кражи, грабежи, причем не только в г. Алматы, но и в других городах Казахстана. Имеется большое число положительных отзывов на подобные исследования, что говорит об эффективности и целесообразности расширения и применения на практике данного вида криминалистических исследований. На сегодняшний момент такого рода исследования все чаще назначаются следователями и судами, несмотря на то, что ученые до сих пор не могут прийти к единому мнению о целесообразности и обоснованности проведения одорологических исследований.

В следственной практике встречаются ситуации, когда на месте совершения преступления остаются лишь запаховые следы человека и зачастую этих следов впоследствии достаточно для изобличения виновных лиц в совершении конкретного преступления. Обнаруженный запах может и должен быть использован для установления субъекта совершения преступления по оставленным им на месте преступления следам биологического происхождения.

Эта задача реализуется в ходе производства криминалистических исследований и экспертиз. Их результаты помогают расследованию и изобличению лиц, совершивших преступления, и в целом количество таких исследований и экспертиз с каждым годом увеличивается. Но, к сожалению, удельный вес доказательств, полученных в результате проведения одорологических исследований, является незначительным. Работники органов, ведущих уголовный процесс относятся к запаховым следам зачастую пренебрежительно, а иногда и даже отрицательно. Возможно, это связано с недооценкой доказа-

тельственного значения одорологических следов, и слабого представления процесса их собирания. Все это способствует представлению о «нетрадиционности» следов одорологического происхождения, несмотря на то, что они давно и успешно используются в деле борьбы с преступностью[1].

Анализ специальной литературы и результаты изучения следственной и экспертной практики позволяют выделить комплекс проблем, связанных с криминалистической одорологией:

- во-первых, до настоящего времени дискутируется вопрос о возможности отнесении одорологического исследования к криминалистической экспертизе, отдельные ученые считают, что одорологическое исследование следует рассматривать в качестве самостоятельного следственного действия или мероприятия под названием «оперативно-следственная выборка»;

- во-вторых, не в полной мере разработана методика одорологического исследования. Отсутствует конкретный перечень действий, которые необходимы в ходе исследования. Регламентировано лишь то, что необходимо вынести постановление о назначении одорологической экспертизы и, что после ее проведения эксперт составляет заключение[2]. Для того чтобы судебная одорология получила официальное закрепление в практике, необходимо четко определить ее статус в процессе расследования и раскрытия преступлений, создать более детальную регламентацию методики одорологического исследования;

- в-третьих, существует проблема собирания одорологических следов в ходе следственного осмотра. С целью изъятия следов следователю необходимо совершить ряд дополнительных действий: вызвать на место происшествия кинолога с собакой, ограничить доступ кого-либо на место происшествия, потому что могут остаться посторонние запахи. Так же необходимо правильно изъять запаховые следы, чтобы в дальнейшем их можно было использовать при проведении одорологической экспертизы. Все это усложняет следственный осмотр, поэтому практические работники зачастую пренебрегают возможностью изъятия запаховых следов, так как на один только осмотр места происшествия затрачивается значительное количество сил и времени и поэтому им проще собирать «традиционные» следы преступления.Решение данной проблемы видится во включении в оперативно-следственную группу помимо специалиста-криминалиста, специалиста, обладающего знаниями в области собирания запаховых следов, что в свою очередь облегчит работу следователя и исключит возможные ошибки в их обнаружении, фиксации и изъятии;

- в-четвертых, пожалуй, одной из самых серьезных проблем является спор о том, можно ли использовать результаты одорологических исследований в качестве доказательства. Одни ученые и практические работники считают, что результаты исследований и одорологической выборки достоверны и могут использоваться как доказательства по уголовному делу, другие, напротив, относятся к данным результатам отрицательно, аргументируя это тем, что экспертизу «проводят собаки», пусть даже и специально обученные, и результаты, которые получают в ходе одорологического исследования при помощи собак, очень сомнительны, так как не исключена возможность подсказки кинолога[3].

Разумеется, могут быть допущены ошибки, собака может указать не на тот образец, но ошибочными могут быть и доказательства, в частности, показания допрашиваемых лиц, они вообще могут быть ложными, или какой-либо документ, его можно подделать, и другое. И в данном аспекте оформленные в установленном порядке результаты одорологических исследований никак не могут быть менее достоверными, чем другие доказательства. Как и все доказательства, они должны рассматриваться в совокупности с имеющимися доказательствами по делу.

Таким образом, полноценное использование запаховых следов в уголовном судопроизводстве возможно лишь при разрешении выше изложенного понимания проблем, необходимо, чтобы: криминалистическая одорология получила официальное закрепление в практике, создать детальную регламентацию методики одорологического исследования, добавить в оперативно-следственную группу специалиста, который обладает знаниями в области собирания запаховых следов, результаты одорологических экспертиз использовались как полноценные доказательства по уголовному делу.

Идея использования результатов одорологического метода в доказывании основывалась на появившейся возможности осуществлять идентификацию по запаху уже не только на этапе интенсивного проведения оперативно-розыскных мероприятий в начале расследования, но практически в любой момент производства по делу[4].

Противники этой идеи ограничивают сферу применения одорологии лишь оперативно-розыскной деятельностью. В доказательство своей правоты они приводят следующие доводы:

- применение собаки является оперативно-розыскной мерой непроцессуального характера;

- поведение собаки никакого процессуального значения не имеет и судебным доказательством по делу не является, ибо уголовно-процессуальное законодательство не предусматривает такого доказательства, как указание собаки-ищейки на определенное лицо или место;

- не существует гарантий достоверности поведения собаки при указании ею определенного лица или места;

- индивидуальность и неизменяемость запаха человека никем и ничем не доказаны;

- выборка человека по запаху с помощью собаки унижает его достоинство.

В проблеме одорологического метода Р. С. Белкин выделяет четыре аспекта: естественно-научный и технический, процессуальный, этический и тактический[5, 264].

Естественнонаучный и технический аспект проблемы. Вопреки утверждениям противников одорологии признано, что индивидуальность и относительная неизменяемость запаха человека относится к числу бесспорно установленных закономерностей, несмотря на отсутствие общепринятой теории запаха. Это положение подтверждено исследованиями биологов, медиков, кинологов и разделяется большинством криминалистов.

Запаховый след человека представляет собой сложный комплекс запахов, включающий:

1) местные запахи — запахи отдельных мест тела, обладающие определенными обонятельными признаками, а именно: область кожи, лишенная волос (подошвы ног, ладони рук), участки кожи со слабым волосяным покровом (подмышечная и лобковая области), кожа с хорошо развитым волосяным покровом (голова);

2) индивидуальный запах — запах человеческого тела, в который включается сумма всех местных запахов;

3) общий запах — запах человека в одежде, включая профессиональный запах и побочные запахи (духов, мыла, зубной пасты, табака и др.).

Таким образом, запаховый след человека состоит из его индивидуального запаха, различных бытовых, производственных и прочих запахов. Уже сам весьма сложный состав запахового следа обеспечивает его индивидуальность.

Поскольку индивидуальный запах человека зависит в первую очередь от источников его выделений: потовых желез, «пахучих» и жировых желез, жизнедеятельность которых подвержена известным возрастным изменениям, относительная неизменяемость запаха лежит в меньшем временном интервале, чем скажем, признаков почерка. Однако продолжительность периода, в течение которого запах человека остается неизменным, как свидетельствует обширная практика, достаточен для широкого использования одорологии в раскрытии и расследовании преступлений.

Технический аспект проблемы выдвигает задачу разработки инструментальных методов анализа и сравнения запахов. В настоящее время ее еще нельзя считать решенной, несмотря на известные успехи, полученные при использовании масс-спектрометрии, газовой и жидкостной хроматографии.

Тактический аспект проблемы. Тактические приемы проведенияодорологической выборки должны обеспечить объективность, достоверность, убедительность и наглядность ее результатов. Ознакомление с отечественной практикой проведения одорологических выборок, с практикой органов внутренних дел других стран в этой области показывает, что указанные задачи могут быть решены путем применения специально разработанных тактических приемов.

1. Использование при выборке лишь специально дрессированных собак. Так, собаки, применяемые для работы со следами на месте происшествия, никогда не используются для выборки и наоборот. Там разработана специальная система дрессировки собак, предназначенных для выборки. Она основана на определенных ограничениях в режиме животного, сочетаемых с поощрительными стимулами.

2. Применение унифицированных предметов-запахоносителей, не отличающихся друг от друга своим внешним видом, что гарантирует выборку исключительно по запаху. Это делает излишней трудновыполнимую рекомендацию подбирать для выборки хотя и однородные, но каждый раз различные предметы (шапки, носовые платки и т. п.) Чаще других такими унифицированными предметами являются куски специальной ткани, обладающей повышенной способностью адсорбировать запахи (например, некоторые сорта детских пеленок фабричного изготовления).

3. Сведение роли кинолога при выборке к минимуму, а именно: даче собаке проверяемого объекта-запахоносителя, подаче команд на выборку и возврат в исходное положение. Кинолог не должен приближаться к объектам выборки, собаку следует применять без поводка.

4. Неоднократное повторение выборки с переменой мест предъявляемых объектов и разными собаками.

5. Исключение воздействия на собаку во время выборки посторонних раздражителей, в том числе организация наблюдения за ходом выборки таким образом, чтобы это не влияло на поведение собаки.

Сама выборка производится в режиме технической процедуры. Если она проводится в процессе доказывания, необходимо присутствие незаинтересованных наблюдателей, выполняющих, по существу, функции понятых, а по возможности – и лица, производящего расследование. Составляемая о выборке справка должна содержать подробное описание не только результатов, но и условий, и процесса выборки.

Этический аспект проблемы. Веским считается довод об унижении достоинства людей, подвергаемых выборке, как подозреваемого, так и тех, заведомо непричастных к делу, кого предъявляют вместе с ним. Как и при решении вопроса о самой допустимости применения одорологического метода, подход к определению его этичности носит двоякий характер: если метод применяется в процессе оперативно-розыскной деятельности, нравственный его характер не вызывает сомнений. Но та же выборка при доказывании недопустима нетерпима и оскорбительна.

Нравственная оценка одного и того же действия не должна зависеть от того, осуществляется ли это действие в сфере оперативно-розыскной деятельности или в сфере доказывания. Стало быть, нравственная оценка выборки человека не может быть связана с вопросом о доказательственном ее значении.

Кроме того, сомнения в нравственности выборки сейчас потеряли всякий смысл, поскольку она осуществляется по стандартным запахоносителям без участия подозреваемого или обвиняемого, так что они могут наблюдать за действиями собак, не подвергаясь никаким унижениям.

Процессуальный аспект проблемы. Центральным пунктом дискуссии по проблеме одорологического метода является вопрос о доказательственном значении результатов его применения. При решении проблемы необходимо учитывать, что в доказывании особое место занимают правила допустимости доказательств. Эти правила должны обеспечить достоверность средств доказывания и тем самым создать надежный фундамент для признания доказанными или недоказанными определенных обстоятельств. Закон допускает следующие условия признания доказательства допустимым:

1. Доказательство должно быть получено надлежащим субъектом, правомочным по данному делу проводить то процессуальное действие, в ходе которого получено доказательство;

2. Фактические данные должны быть получены только из источников, перечисленных и указанных в законе;

3. Доказательство должно быть получено с соблюдением правил проведения процессуального действия, в ходе которого получено доказательство;

4. При получении доказательства должны быть соблюдены все требования закона при фиксировании хода и результата следственного действия.

Результаты проведенного нами исследования свидетельствуют о том, что несмотря на различные противоречий в применении возможностей криминалистической одорологии в раскрытии, расследовании и предупреждении преступлений в практических органах этот нетрадиционный метод применяются, более того, во многих подразделенях органов внеутренних дел республики имеются современные одорологические лаборатории с соответствующим специальным оборудованием и структурой для работы с такими объектами , подготовлены специалисты (криминалисты, биологии, кинологы и др.), имеющие специальную подготовку по работе со следами запахов на месте происшествия.

Таким образом, на наш взгляд, назрела необходимость в разработке теоретических,процессуальных и тактических вопросов применения одорологии в судопроизводстве Казахстана, которая должна осуществляться комплексно: процессуалистами,криминалистами, с участием биологов,химиков и других специалистов[6].

---

[1] Аистов И. А. Использование следов биологического происхождения при расследовании преступлений: Учеб. пос. — М., 2002.

[2] Баев О. Я. Основы криминалистики: Курс лекций. — М., 2010.

[3] Ищенко Е. П., Топорков А. А. Криминалистика: Учебн. для студ. вузов. Изд. 2-е, испр. и доп. — М., 2006.

[4] Использование возможностей экспертизы запаховых следов человека при раскрытии и расследовании краж из квартир. — Киров, 2004.

[5] Белкин Р. С. Частные криминалистические теории. — М., 1978.

[6] Современное состояние и перспективы развития одорологии в РК: Мат-лы круглого стола. — Алматы, 2012.

Бычков В. В.,
декан факультета повышения квалификации,
кандидат юридических наук, доцент;
Вепрев С. Б.,
заведующий кафедрой информационных технологий,
доктор технических наук, старший научный сотрудник;
Прорвич В. А.,
профессор кафедры уголовного процесса,
доктор юридических наук, доктор технических наук, профессор
(Московская академияСледственного комитета Российской Федерации)

К ВОПРОСУ О ФОРМИРОВАНИИ ЕДИНОЙ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ АЛГОРИТМОВ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОГО ХАРАКТЕРА, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ»

На фоне улучшения в Российской Федерации за последние два десятилетия общей криминогенной обстановки фиксируется стабильный рост преступлений экстремистского характера, в общем, и совершаемых с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», в частности[1; 2]. К сожалению, противодействие данному виду преступлений как в форме выявления и раскрытия, так и расследования, не достаточно эффективно[3].

Для успешного выявления, раскрытия и расследования преступлений указанного вида необходимо применение научно обоснованного, юридически выверенного и проверенного практикой методического обеспечения, основанного на нескольких группах алгоритмов, объединенных в единую иерархическую систему[4].

Первый модуль единой системы алгоритмов составляет группа алгоритмов, нацеленная на формирование развернутой уголовно-правовой характеристики конкретных экстремистских преступлений. Этот модуль можно также назвать базовым, поскольку все рассматриваемые действия нацелены именно на выявление и расследование преступлений рассматриваемого вида. Чтобы не совершить соответствующих юридических ошибок, обращение к алгоритмам данного модуля предусмотрено от всех других модулей единой иерархической системы.

Для надлежащего раскрытия бланкетных, отсылочных и смешанных диспозиций уголовно-правовых норм, устанавливающих уголовную ответственность за преступления рассматриваемого вида, необходимо использовать не только соответствующие алгоритмы данного модуля, но и специально сформированный инструментарий: электронные библиотеки соответствующих положений специального законодательства, а также необходимые информационные технологии для согласования различающихся терминов на основе проблемно-ориентированных тезаурусов.

При этом необходимо применение ряда критериев и соответствующих информационных технологий для контроля формирования развернутой уголовно-правовой характеристики преступлений рассматриваемого вида и внесение своевременных корректировок, обеспечивающих строгое выполнение требований уголовного законодательства. Это позволит гарантировать, что итоговый вариант развернутой уголовно-правовой характеристики конкретного преступления не выйдет за рамки уголовного права, обеспечив адекватность всей сформированной с помощью данных алгоритмов совокупности обязательных и факультативных признаков состава данного преступления.

Второй модуль единой системы алгоритмов составляет группа алгоритмов, нацеленная на использование специальных знаний на различных стадиях процессуально регламентированных действий по структурированию всего комплекса информации, связанной с преступлением, и ее параметрического анализа для выявления преступлений экстремистского характера, их раскрытия и расследования. Прежде всего, речь идет о применении специальных знаний специалистов высшей квалификации для дачи разъяснений по вопросам, входящим в их профессиональную компетенцию. Соответствующие алгоритмы используются и для информационно-методического обеспечения процессуально регламентированных действий при выявлении и фиксации следов преступлений рассматриваемого вида, а также при подготовке к назначению судебных экспертиз, включая постановку вопросов экспертам и

подготовку необходимых материалов уголовного дела в качестве объекта конкретной судебной экспертизы. Особая группа алгоритмов использования специальных знаний специалистов высшей квалификации предназначена для выполнения надлежащей проверки и оценки собранных доказательств по делу.

Несколько групп алгоритмов данного модуля предназначены для надлежащего информационно-методического обеспечения судебно-экспертных исследований. Данные алгоритмы могут применяться на разных стадиях уголовного судопроизводства.

Третий модуль единой системы алгоритмов включает в себя группу алгоритмов, нацеленных на надлежащее информационно-методическое обеспечение процесса квалификации конкретного экстремистского преступления и позволяющих сформировать необходимую для этого систему юридических тождеств. Левая часть каждого тождества, входящего в данную систему, содержит одно или несколько первичных сведений о преступном деянии. Правая часть каждого из юридических тождеств формируется на основе конкретных признаков состава преступления, сформированного на основе его развернутой уголовно-правовой характеристики. При этом сведения, включенные в левую и правую часть каждого из юридических тождеств системы, приводятся к единому информационному формату, чтобы избежать ошибок при установлении их взаимного соответствия.

Четвертый модуль единой иерархической системы алгоритмов включает в себя группу алгоритмов, нацеленных на формализацию всего комплекса информации, связанной с преступлением, и ее параметрического анализа для выявления признаков преступных деяний в различных сферах традиционной и цифровой криминалистики. Для ее надлежащего применения важно сопряжение с другими группами алгоритмов, обеспечивающими формирование развернутой уголовно-правовой характеристики преступлений рассматриваемого вида и выделение совокупностей обязательных и факультативных признаков составов конкретных преступлений, а также применение для этого необходимых специальных знаний.

Кроме этого, в данный модуль включены алгоритмы, обеспечивающие надлежащее информационное обеспечение оперативно-розыскных мероприятий по выявлению преступлений рассматриваемого вида, а также средства их информационной поддержки в виде библиотеки информационных характеристик данных преступлений. Многие из них имеют не статичный, а динамический характер, отражая особенности перехода цепочки нарушений гражданского и специального законодательства в новое качество уголовных преступлений, а также средства необходимого контроля, позволяющего избежать соответствующих юридических ошибок.

Пятый модуль единой системы алгоритмов включает в себя группу алгоритмов, нацеленных на надлежащее информационно-методическое обеспечение процессуально регламентированных действий в рамках доследственной проверки имеющихся сведений о преступном деянии экстремистского характера с использованием компьютерной техники и информационных технологий. В составе этих алгоритмов предусмотрены средства их сопряжения с первым модулем алгоритмов, позволяющих осуществить идентификацию признаков конкретного преступления, сформировать базовую совокупность признаков состава данного преступления, а затем выполнить его предварительную квалификацию.

Важной отличительной особенностью данного модуля является наличие нескольких блоков сопряжения с алгоритмами первого модуля, что позволяет уточнять уголовно-правовую характеристику конкретного экстремистского преступления по мере необходимости. Кроме этого, в данном модуле имеются и блоки сопряжения с алгоритмами третьего модуля, позволяющие реализовать несколько вариантов предварительной квалификации преступлений, причем в условиях недостаточности необходимых сведений о совершенном деянии. Это обуславливает необходимость применения в рамках данного модуля специальной группы алгоритмов, сориентированной на оценку рисков принятия решения о возбуждении уголовного дела либо об отказе в его возбуждении в условиях недостатка информации о совершенном деянии.

Шестой модуль единой иерархической системы алгоритмов включает в себя группу алгоритмов, нацеленных на надлежащее информационно-методическое обеспечение следственных действий на первоначальном этапе расследования уголовного дела. Его отличительной особенностью являются не только те группы алгоритмов, которые отражают особенности организации неотложных следственных действий «традиционного» характера, но и структурирования всего комплекса информации, связанной с преступлением, систематизации собранных доказательств, выдвижения предварительных

следственных версий, а также блоков сопряжения с алгоритмами второго модуля, позволяющими выполнить надлежащую проверку и оценку собранных доказательств. Необходимо обратить внимание и на те группы алгоритмов, которые позволяют формализовать различные виды неотложных следственных действий по преступлениям в сфере как традиционной, так и цифровой криминалистики, а также тех видов преступлений в сфере традиционной криминалистики, которые были совершены с использованием компьютерной техники, электронных документов и информационных технологий.

Прежде всего, речь идет об алгоритмах такого следственного действия, как обыск, который при расследовании уголовных дел по преступлениям в сфере цифровой криминалистики нередко приходится производить в виртуальном пространстве компьютерных сетей, вскрывая хранилища электронных документов в облачной памяти. Такого рода следственные действия кажутся, на первый взгляд, просто фантастическими, не имеющими отношения к реальной действительности. Вместе с тем, в результате подобных действий преступников в виртуальном пространстве ежедневно совершаются незаконные операции на миллиарды реальных рублей.

Седьмой модуль единой системы алгоритмов включает в себя группу алгоритмов, нацеленных на надлежащее информационно-методическое обеспечение следственных действий на последующем этапе расследования уголовного дела. Его отличительной особенностью являются не только те группы алгоритмов, которые отражают особенности организации следственных действий «традиционного» характера, выдвижения и проверки следственных версий, проверки и оценки собранных доказательств, их систематизации и уточнения выполненной ранее квалификации преступления. При этом также используются блоки сопряжения данных алгоритмов с алгоритмами первого, второго и третьего модулей.

Вместе с тем, при расследовании уголовных дел о преступления экстремистского характера, совершенных с использованием электронных документов и информационных технологий, оказывается необходимым использования ряда следственных действий в «виртуальном пространстве» сети Интернет. При этом алгоритмы следственных действий должны быть сформированы с соблюдением цифровых прав субъектов, связанных с соответствующими информационными системами. Специальная группа алгоритмов предназначена для выявления и фиксации «цифровых» или «электронных» следов преступлений, обнаруженных следователем при выполнении следственных действий в сетевом информационном пространстве, а затем формирования на их основе необходимых доказательств по расследуемому уголовному делу. Эти доказательства также должны пройти проверку и оценку с применением специальных алгоритмов, упоминавшихся выше.

Восьмой модуль единой системы алгоритмов включает в себя группу алгоритмов, нацеленных на надлежащее информационно-методическое обеспечение следственных действий на завершающем этапе расследования уголовного дела. Его отличительной особенностью являются блоки сопряжения практически со всеми описанными выше модулями алгоритмов. Это позволяет не только систематизировать все собранные по расследуемому делу доказательства, прошедшие надлежащую проверку и оценку, но и сформировать итоговый вариант системы юридических тождеств для квалификации преступления.

Кроме того, наличие или отсутствие пробелов в сформированной следователем системе юридических тождеств может использоваться в качестве критерия для завершения расследования уголовного дела. Если информационные пробелы в системе юридических тождеств носят неустранимый характер, а получение доказательств, соответствующих хотя бы одному из признаков состава преступления, оказывается невозможным, то это может стать основанием для прекращения уголовного дела и уголовного преследования за отсутствием состава преступления. Но если информационные пробелы отсутствуют, то это дает основание следователю для признания в соответствии со ст. 88 УПК РФ собранной совокупности доказательств достаточной и выполнения процессуально регламентированных действий по ознакомлению обвиняемого с материалами уголовного дела и подготовки обвинительного заключения в установленном порядке.

Важно обратить внимание на упоминавшиеся выше ситуации, когда в ходе расследования уголовного дела выясняется, что было совершено не одно, а два преступления с определенными формами «перекрестного» соучастия их субъектов. Особенно сложные ситуации возникают в случаях, когда экстремисты используют технологию блокчейн либо определенные виды криптовалют для финансирования экстремистской деятельности.

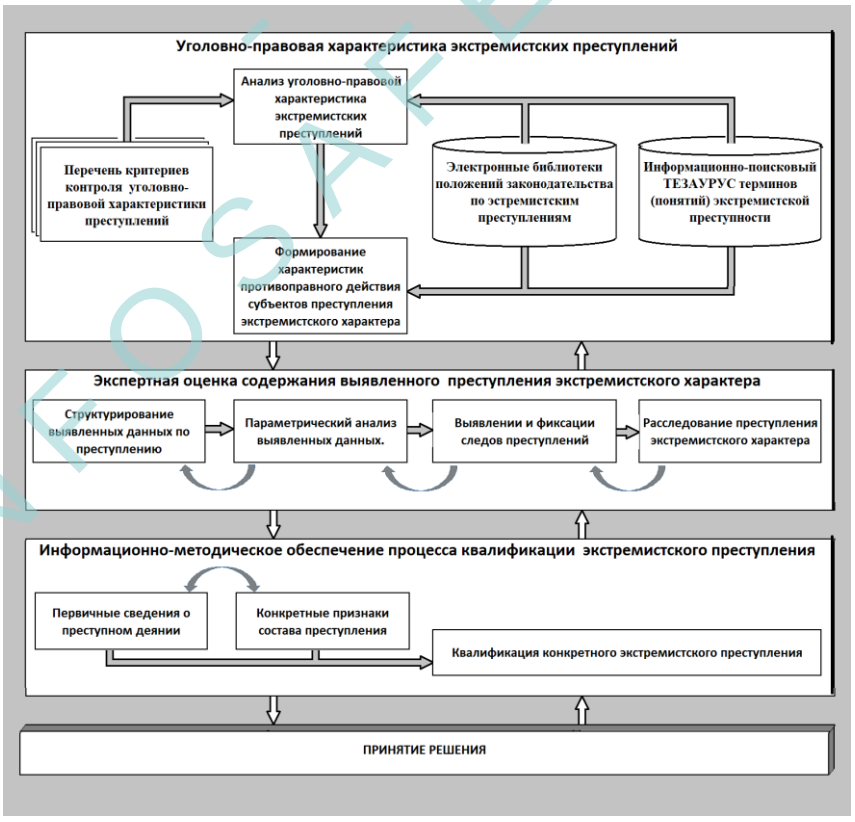
Определенные совокупности алгоритмов из описанных выше модулей могут быть использованы также руководителями следственных органов для повышения эффективности контроля за надлежащим расследованием уголовных дел о преступлениях экстремистского характера. Аналогичный вывод можно сделать и в отношении прокуроров, осуществляющих надзор за надлежащим расследованием данных уголовных дел. Они могут использоваться также судьями для надлежащего информационно-технологического обеспечения судебного следствия.

Для объединения усилий разработчиков алгоритмов различного вида, входящих в состав перечисленных выше модулей единой иерархической системы алгоритмов информационного обеспечения следственных и иных процессуально регламентированных действий по преступлениям рассматриваемого вида, необходимо создание и использование соответствующего юридического алгоритмического языка. Иначе добиться полного взаимопонимания ученых и специалистов высшей квалификации в различных отраслях юридических наук уголовно-правового блока друг с другом, а также с практика, то есть сотрудниками правоохранительных органов, крайне сложно, если вообще возможно.

Но даже если соответствующие алгоритмы будут разработаны отечественными учеными, а на их основе будут созданы соответствующие интерактивные экспертные системы, сориентированные на их использование следователями, дознавателями, прокурорами и судьями, либо подобные программные средства будут закуплены у иностранных производителей, неизбежно возникнут вопросы организации их эффективного использования. Для этого пользователям соответствующих интерактивных экспертных систем также будет необходимо овладеть соответствующим алгоритмическим языком[5].

Первоочередной проблемой, которую необходимо решить для создания единого алгоритмического языка, позволяющего разрабатывать и наиболее эффективно применять весь комплекс современных информационных технологий для надлежащей организации выявления, раскрытия и расследовании преступлений экстремистского характера, является формирование его интегрированного научного фундамента.

Блок-схема
алгоритмов информационного обеспечения выявления,раскрытия
и расследования преступлений экстремистскогохарактера, совершаемых
с использованием информационно-телекоммуникационных сетей



[1] Бычков В. В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремисткой направленности // Вестн. Московск. акад. Следственного комитета Российской Федерации. 2020. № 3. С. 43 – 46.

[2] Бычков В. В., Ротов В. А. Понятие и виды преступлений экстремисткой направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. — 2020. — № 3. — С. 26 – 31.

[3] Бычков В. В., Прорвич В. А. Проблемы выявления, раскрытия и расследования преступлений экстремистского характера, совершенных с использованием информационно-телекоммуникационной сети «Интернет», и их решение // Российский следователь. — 2021. — № 2. — С. 3 – 6.

[4] Бычков В. В., Прорвич В. А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети «Интернет» // Российский журнал правовых исследований. — 2021. — Т. 7. — № 1. — С. 1 – 8.

[5] Бычков В. В., Прорвич В. А. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета // Правопорядок: история, теория, практика. — 2021. — № 2 (29). — С. 92 – 97.

Веремейчик В. М.,
государственный судебный эксперт,
кандидат биологических наук;
Кузуб Н. Н.,
заместитель начальника отдела генетических экспертиз
(Государственный комитет судебных экспертиз
Республики Беларусь, г. Минск)

Уровень мутаций в 7 новых (non-CODIS) аутосомных STR-локусах у населения Республики Беларусь

Аутосомные STR-локусы получили широкое распространение в экспертной практике из-за их высокого дискриминирующего потенциала и простоты в использовании. Сведения об уровне мутаций для каждого из используемых локусов необходимы для корректной интерпретации генетических профилей при идентификации личности и установлении биологического родства. В продолжение начатой нами работы проведен расчет уровня мутаций в 7 новых (non-CODIS) аутосомных STR-локусах на основе анализа 3 860 случаев установления биологического отцовства, проведенных в лабораториях Беларуси с 2005 по 2021 гг. В общей сложности было выявлено 35 пошаговых мутаций в 6 локусах и 1 мутация типа «нуль-аллель» в локусе D22S1045. В локусе SE33 наблюдался наибольший уровень мутаций (0,00572), в локусе D2S441 — наименьший (0,00020).

Autosomal loci with short tandem repeats (STR) are widely used for the human identification. Knowledge about the locus-specific mutation rates of STRs improves forensic probability calculations for the correct interpretation of diversity data and appropriate evaluation of genetic evidence in parentage and forensic analyses. Mutations of 7 new (non-CODIS) STRs were studied in 3,860 paternity cases carried out during 2005 – 2021 in Belarus. In total, 35 slippage mutations were identified at 6 loci and 1 null-allele mutation at locus D22S1045. The highest mutation rate was observed at SE33 (0.00572), and the lowest at D2S441 (0.00020).

В современных криминалистических исследованиях локусы с короткими тандемными повторами (STR-локусы) стали важным ДНК-инструментом вследствие характерной для них короткой длины аллелей, что важно при работе с деградированным материалом, а также значительного полиморфизма, обеспечивающего возможность с высоким уровнем достоверности идентифицировать личность и установить биологическое родство. Однако в связи с тем, что высокополиморфные STR-локусы постоянно подвергаются мутационному процессу, интерпретация генетических профилей при идентификации личности и установлении биологического родства требует сведений об уровне мутаций для каждого из используемых локусов. Для STR-локусов характерны два основных типа мутаций: 1) вставка/выпадение тандемного повтора (пошаговая мутация, когда изменяется длина амплифицированного фрагмента) и 2) замена нуклеотида в месте посадки праймера (приводит к отсутствию продукта амплификации и полученный генетический профиль считывается как ложно гомозиготный — «нуль-аллель»). Основным мутационным механизмом, ведущим к изменению длины микросаттелита, является так называемое «проскальзывание» полимеразы[1; 2]. В процессе репликации повторяющегося региона нити ДНК диссоциируют, а затем под воздействием определенных факторов могут некор-

ректно реассоциировать, что приводит к вставке или выпадению повторяющихся единиц (тандемных повторов) и образованию аллеля с новым, альтернативным, размером.

Мутации STR-локусов в паре «родитель – ребенок» выявляются, когда наблюдается несогласование аллельных вариантов в одном (или двух) исследуемых локусах[3]. В большинстве судебно-генетических экспертиз проводится прямое сравнительное исследование генетических профилей, выявленных на вещественных доказательствах и у проходящих по делу лиц, и уровень мутаций не играет важной роли. Однако, при проведении исследований по установлению родства (отцовства/материнства) по гражданским делам, а также при идентификации жертв массовых катастроф, наличие мутационного события может сыграть важную роль (особенно в случаях предположительного исключения отцовства) и серьезно повлиять на окончательный вывод о подтверждении биологического родства.

В Республике Беларусь ранее был рассчитан уровень мутаций для 17 аутосомных STR-локусов, широко применяемых в экспертной практике[4]. Для расчета уровня мутаций в 7 новых (non-CODIS) аутосомных STR-локусах, входящих в состав новейших наборов для генотипирования производства фирм AppliedBiosystems, Promega и QIAGEN, нами было проанализировано 3 767 подтвержденных случаев установления биологического родства (отцовства и материнства), проведенных в лабораториях Беларуси с 2005 по 2021 гг., с использованием локусов D1S1656, D2S441, D10S1248, D12S391, D22S1045, SE33 и D6S1043. При этом трио «отец – ребенок – мать» составили 2 787, пары «отец – ребенок» — 393 и пары «мать – ребенок» — 587.

Наличие мутации, ее тип и родительский источник мутантного аллеля определялись согласно методам, описанным в литературе[5; 6; 7]. Так, при существовании двух возможностей, наиболее вероятным предполагалось мутационное событие, в ходе которого наблюдалось наименьшее изменение количества тандемных повторов (самый короткий мутационный шаг). Если оба гетерозиготных родительских аллеля (например, «11/13») показывали одинаковую разницу в числе тандемных повторов при сравнении с новым аллелем («12»), тип мутации считался неопределенным (либо вставка, либо выпадение). При наличии возможности исключения родства для обоих родителей декларировалось, что источник мутации не определен (либо отцовский, либо материнский). В случае несогласования аллельных вариантов между гомозиготным родителем и гомозиготным ребенком предполагалось наличие «нуль-аллеля». Расчет уровня мутаций в исследованных STR-локусах проводился путем прямого подсчета. Данные были проанализированы с помощью программного обеспечения Microsoft Office Excel.

Всего было исследовано 31 978 переносов аллелей при мейозе в 7 аутосомных STR-локусах. В общей сложности было выявлено 35 пошаговых мутации в 6 локусах и 1 мутация типа «нуль-аллель» в локусе D22S1045.

В локусе SE33 было выявлено наибольшее число мутаций (15), в локусах D6S1043 и D2S441 — наименьшее (по одной). На основе полученных данных были рассчитаны частоты мутаций для каждого из исследованных STR-локусов у населения Беларуси, приведенные в таблице 1. При этом средний уровень мутаций составил 0.11 %, что согласуется с литературными данными.

Мутационные изменения у мужчин наблюдались чаще, чем у женщин: 26 мутаций имели отцовское происхождение и только 5 — материнское. Для 4 случаев источник мутации не определен. Большинство мутаций (97,14 %) оказались одношаговыми, при этом соотношение вставка/выпадение повтора составило 1:1, а в 3 случаях эти события были равновероятны (таблица 2). Мультишаговая мутация с изменением размера на 2 повтора наблюдалась 1 раз.

Точечная мутация в месте посадки праймеров наблюдалась только в локусе D22S1045 и имела отцовское происхождение. При использовании праймеров с другой структурой ложно гомозиготный профиль оказался гетерозиготным.

Для судебно-геномной экспертизы очень важен учет мутационных событий, а накопление данных об уровне мутаций в аутосомных STR-локусах необходимо для адекватной интерпретации генетических профилей при идентификации личности, а также для определения критериев исключения при установлении биологического родства.

Таблица 1 — Уровень мутаций аутосомных STR-локусов у населения Беларуси

Локусы	Число мейозов		Число мутаций			Частота мутаций		
	отцовских	материнских	отцовских	материнских	источник не определен	отцовских	материнских	всего
D1S1656	2294	2623	4	1	0	0,00174	0,00038	0,00102
D2S441	2294	2623	0	1	0	0,00000	0,00038	0,00020
D10S1248	3099	3297	2	1	1	0,00065	0,00030	0,00063
D12S391	2294	2623	5	1	3	0,00218	0,00038	0,00183
D22S1045	3099	3297	0	0	0	-	-	-
SE33	1248	1375	14	1	0	0,01122	0,00073	0,00572
D6S1043	847	965	1	0	0	0,00118	0,00000	0,00055
Всего	15175	16803	26	5	4	среднее 0,00171	среднее 0,00030	среднее 0,00109

Таблица 2 — Характеристика выявленных мутаций аутосомных STR-локусов

	Вставка	Выпадение	Вставка либо выпадение	Всего
±1 повтор	16	15	3	34
±2 повтора		1		1
отцовские	13	12	1	26
материнские	2	3		5
источник не определен	1	1	2	4
Всего	16	16	3	35

[1] Farrall M., Weeks D. E. Mutational mechanisms for generating microsatellite allele-frequency distributions: an analysis of 4,558 markers / M. Farrall and D. E. Weeks // Am. J. Hum. Genet. — 1998. — Vol. 62. — P. 1260 – 1262.

[2] Jeffreys A. J., Neil D. L., Neumann R. Repeat instability at human minisatellites arising from meiotic recombination / A. J. Jeffreys, D. L. Neil, R. Neumann // Embo. J. — 1998. — Vol. 17. — P. 4147 – 4157.

[3] Mutation rate in human microsatellites: influence of the structure and length of the tandem repeat / B. Brinkmann [et al.] // Am. J. Hum. Genet. — 1998. — Vol. 62. — P. 1408 – 1415.

[4] Veremeichyk, V. M. Mutation rates at 17 STR loci in the Belarusian population / V. M. Veremeichyk, S. R. Borovko, N. N. Kuzub // Forensic Sci Int: Genetics Supplement Series. — 2015. — Vol. 5. — P. e314 – e316.

[5] The evaluation of forensic DNA evidence // Committee on DNA Forensic Science: an Update. National Research Council. — Washington D.C.: National Academy Press., 1996. — 272 p.

[6] Guidance for Standards for Relationship Testing Laboratories 8th ed. // AABB Committee. — Maryland: Amer Assn of Blood Banks, 2008. — 157 p.

[7] Weber J. L., Wong, C. Mutation of human short tandem repeats / J. L. Weber, C. Wong // Hum. Mol. Genet. — 1993. Vol. 2. — P. 1123 – 1128.

Волынский А. Ф.,
профессор кафедры криминалистики,
доктор юридических наук, профессор
(Московский университет МВД России им. В. Я. Кикотя);
Прорвич В. А.,
профессор кафедры уголовного процесса,
доктор юридических наук, доктор технических наук, профессор
(Московская академия Следственного комитета России)

Роль криминалистики в системе уголовно-правовой защиты субъектов цифровых прав от современного криминала

В условиях перехода к информационному обществу и экономике знаний[1] происходят существенные изменения в действующем законодательстве, отражающие кардинальные изменения общественных отношений. В частности, в гражданское законодательство два года назад была введена система цифровых прав, а затем и цифровых финансовых активов. Для уголовно-правовой защиты субъектов таких прав перед правоохранительными органами встают принципиально новые задачи, требующие выработки новых подходов к их решению.

Поскольку цифровые права были связаны законодателем с определенными информационными системами и их правилами, то первоочередной задачей становится выявление и фиксация следов соот-

ветствующих преступлений в электронной документации и иных сведениях из информационных систем различного вида, с последующим формированием доказательств по уголовному делу на их основе. Необходимо отметить, что ч. 3 ст. 1641 УПК РФ регламентирует первую часть соответствующих следственных действий по изъятию соответствующей электронной документации путем ее копирования на электронный носитель информации следователя и приобщения его к материалам уголовного дела. Но дальнейшие следственные действия со многими тысячами и даже миллионами электронных документов, отражающих различные особенности транзакций с цифровыми финансовыми активами, совершенными, к примеру, определенными брокерами на биржах, в клиринговых центрах, с участием банков, держателей электронных реестров и других участников рынка эмиссионных ценных бумаг или производных финансовых документов, процессуальное законодательство пока не регламентирует.

В связи с этим особую роль в выявлении, раскрытии и расследовании преступлений, связанных с общественно опасными правонарушениями в системе цифровых прав и цифровых финансовых активов, и создании соответствующих методик и информационных технологий должна играть криминалистика. Однако в последнее время даже некоторые ведущие ученые-криминалисты с упорством, достойным лучшего применения, тратят свои силы на споры о том какие следы оставляют преступники при совершении подобных деяний — цифровые, электронные, электронно-цифровые или виртуальные.

Не вдаваясь в детали, используемой при этом аргументации, следует обратить внимание на то, что следы как таковые для выявления, раскрытия и расследования преступления не имеют самостоятельного значения. Работа с ними необходима для формирования в установленном порядке следователем на их основе доказательств по уголовному делу, изобличающих определенное лицо в совершении данного преступления. Поэтому при разработке соответствующих криминалистических методик, нацеленных на выявление и фиксацию следов преступлений рассматриваемого вида в электронной документации, хранящейся в информационных системах различного вида, необходимо акцентировать внимание на последующие процессуальные действия, позволяющие следователю получить необходимые доказательства по уголовному делу.

В свою очередь, при получении доказательств в рамках расследования уголовного дела о преступлениях рассматриваемого вида, соответствующие криминалистические методики должны быть нацелены на то, чтобы собранная совокупность этих доказательств позволяла следователю установить в деянии состав преступления в соответствии с требованиями ч. 1 ст. 24 УПК РФ, а также предмет доказывания, включающий всю совокупность обстоятельств, подлежащих доказыванию в соответствии со ст. 73 УПК РФ. При этом для получения многих доказательств оказывается необходимым использование специальных знаний и профессиональных компетенций судебных экспертов и специалистов. Здесь также встает ряд вопросов о создании соответствующих экспертных методик, сориентированных на обеспечение необходимых экспертных исследований и обосновании выводов по поставленным вопросам.

Что касается характера таких криминалистических и экспертных методик, то они должны обеспечивать принципиально новые возможности обработки электронных документов различного вида без их преобразования в документы на бумажных носителях. Во многих исследованиях, посвященных особенностям криминалистических и экспертных методик, отмечалось, что по своим структурно-содержательным характеристикам такие методики представляют собой программы соответствующих следственных либо экспертных действий, взаимно связанных в определенной последовательности[2].

По сути, речь идет о соответствующих алгоритмах обработки документированной информации при организации жесткого контроля за обеспечением правового статуса промежуточных и итоговых результатов обработки данной информации. Соответственно, подобные алгоритмы могут использоваться и для обработки электронных документов, имеющихся в уголовном деле[3]. При этом оказывается необходимым выделить ту часть информации, которая имеет признаки криминальной, на фоне намного большей по объему информации, отражающей правомерные действия законопослушных субъектов. Необходимо обратить внимание и на другие особенности таких алгоритмов.

Во-первых, поскольку речь идет о целенаправленной обработке электронной документации, изъятой следователем из определенных информационных систем, чтобы выявить в ней признаки криминального характера, то вполне понятно, что и соответствующие следы также носят закодированный соответствующими компьютерными программами информационный характер.

Во-вторых, такие следы могут носить не информационно замкнутый характер, поддающийся интерпретации для установления определенных фактов и обстоятельств, имеющих значение для уголовного дела, а фрагментарный характер, не отражающий характеристику определенного события, которое может идентифицироваться, как криминальное. При этом такие фрагменты могут быть рассеяны по различным электронным документам, а для их идентификации и установления информационного следа определенного криминального события оказывается необходимой целенаправленная, проблемно-ориентированная обработка определенных групп документов, в том числе, с использованием информационных эталонов законопослушной деятельности.

В-третьих, электронные документы создаются, хранятся, передаются и преобразовываются, в том числе, в другие электронные документы, с помощью определенных компьютерных программ, которые принято называть также компьютерными кодами. Соответственно, определенные фрагменты криминальной информации, которые могут быть выявлены и зафиксированы в некоторой совокупности электронных документов, по своей сути могут быть идентифицированы, как закодированные информационные следы преступлений рассматриваемого вида. Однако для повышения эффективности таких методик необходимо формирование соответствующих «информационных эталонов», причем не только о надлежащей подготовке и совершении соответствующих сделок законопослушными субъектами, но и о типичных способах совершения преступлений, связанных с цифровыми финансовыми активами.

В-четвертых, с помощью соответствующих алгоритмов, на основе выявленных в определенной совокупности электронных документов и зафиксированных следователем закодированных информационных следов преступлений могут быть идентифицированы их связи с соответствующими информационными системами и их обладателями. Это позволяет сформировать на их основе доказательства, изобличающие определенных лиц в причастности к преступлениям рассматриваемого вида.

В-пятых, алгоритмы обработки электронных документов могут сочетаться с алгоритмами обработки документации на бумажных носителях информации, а также с алгоритмами выполнения других видов следственных, а также иных процессуально регламентированных действий. Это позволяет установить прямые и обратные связи таких действий, что позволяет повысить эффективность расследования соответствующих уголовных дел.

В-шестых, криминалистические алгоритмы обработки электронной и иной документации должны разрабатываться с учетом необходимости установления фактов и обстоятельств, характеризующих деятельность подозреваемых лиц до и после совершения транзакций с цифровыми финансовыми активами определенного вида. Причем, речь идет не только о «полном комплексе» соответствующих транзакций, но и об их определенных частях. Здесь важно подчеркнуть наличие взаимных связей криминалистики с оперативно-розыскной деятельностью, существенно расширяющих возможности как самой криминалистики, так и оперативно-розыскной деятельности в борьбе с высокотехнологичным криминалом.

В-седьмых, при разработке системы криминалистических алгоритмов для целенаправленной обработки электронной и иной документации, имеющей отношение к подготовке и совершению сделок с цифровыми финансовыми активами, необходимо учитывать и те возможности, которые дает применение для этого специальных знаний в различной форме. Речь идет не только о судебной экспертизе, но и о специалистах, обладающих соответствующими специальными знаниями и профессиональными компетенциями. Особенно важно привлечение к разработке таких алгоритмов и их практическому применению таких специалистов, которые обладают комплексом специальных знаний и профессиональных компетенций высокого уровня в нескольких областях. К примеру, речь идет о специальных знаниях в сфере финансового права и экономико-математических моделях, гражданском праве, информатики и т. п.[4]

Кроме перечисленных выше, можно отметить и ряд других особенностей криминалистических алгоритмов, с помощью которых могут быть обеспечены новые возможности работы следователей с электронной документацией, используемой для подготовки и совершения всего комплекса транзакций с цифровыми финансовыми активами. При этом необходимо обратить внимание на следующие особенности организации такой работы.

Прежде всего, речь идет о применении для обработки электронной документации специализированных компьютерных программ, с помощью которых и происходит практическое применение описанных выше и иных «криминалистических» алгоритмов. Однако при полностью автоматизирован-

ной обработке электронных документов с помощью таких программных средств невозможно обеспечить правовой статус результатов их обработки. Соответственно, слепое доверие следователя к результатам автоматизированной обработки электронной документации может привести к юридическим ошибкам, которые весьма сложно выявить, не говоря уже об их исправлении.

Поэтому при практической реализации данных криминалистических алгоритмов необходимо ориентироваться не на применение уже известных или создание новых компьютерных программ для автоматизированной обработки электронных документов, а на создание программного обеспечения для интерактивных экспертных систем. С их помощью создается ряд возможностей не только для обеспечения постоянного диалога следователя со своим «компьютерным помощником» при обработке документированной информации, но и его личного контроля за сохранением правового статуса промежуточных и итоговых результатов обработки электронных документов. В частности, для этого следователю может быть предоставлено право электронной подписи результатов обработки электронной документации, выполненной под его контролем.

Безусловно, при этом следует обратить внимание и на ряд принципиальных отличий не только соответствующих криминалистических методик, но и всей организации работы следователя с применением новой криминалистической тактики, техники и методики. Соответственно, необходимо существенно модернизировать и теоретические основы криминалистики как науки, приблизив их к современным потребностям информационного общества к созданию эффективной системы уголовно-правовой защиты прав и законных интересов его субъектов всех видов и уровней в новых условиях.

По результатам проведенных исследований можно сделать ряд выводов о том, что первоочередное значение приобретают проблемы общенаучного характера, связанные с применением определенных языковых конструкций субъектами нового, информационного общества, которые пользуются повышенным вниманием криминала. При этом речь идет совсем не о тех новообразованиях и иностранных заимствованиях, которые появляются в русском языке в связи со все более широким вовлечением в общение с помощью Интернета и различных социальных сетей большей части российских граждан. Речь идет о проникновении все большего количества элементов алгоритмических языков, используемых для написания компьютерных программ, в сферу экономики и финансов, а также в ряд других сфер общественных отношений нового типа.

Поэтому встает весьма актуальная задача создания основ для нового языка правоохранителей и правоприменителей — алгоритмического юридического языка, позволяющего использовать те возможности, которые уже созданы для этого в рамках документальной информатики и других отраслях информатики, математики и кибернетики. С точки зрения развития теоретических основ современной криминалистики необходимо обратить внимание и на ряд разработок, нацеленных на создание основ правовой информатики и компьютерной криминалистики, которые ведутся не только учеными, но и постулируются в нормативных правовых актах, подготовленных на уровне высшего руководства страны[5].

В заключение необходимо подчеркнуть два важнейших аспекта, характеризующих складывающиеся тенденции в формировании системы уголовно-правовой защиты субъектов информационного общества от атак высокотехнологичного криминала. С одной стороны, речь идет о явных проявлениях «научного сепаратизма» среди некоторых представителей наук уголовно-правового блока[6], играющих разрушительную роль в мобилизации всех представителей научного знания в борьбе с современной преступностью. Но с другой стороны, в последнее время можно отметить и все возрастающую интегрирующую роль криминалистики в системе всех наук уголовно-правового блока, экономики, информатики и других отраслей научного знания, для оснащения уголовного судопроизводства современным инструментарием, позволяющим обеспечить эффективную уголовно-правовую защиту всех субъектов информационного общества и экономики знаний[7].

---

[1] Стратегия развития информационного общества Российской Федерации на 2017 – 2030 годы. Утверждена Указом Президента РФ от 9 мая 2017 г. № 203. [Электронный ресурс]. — Режим доступа: https://base.garant.ru/71670570/ (дата обращения: 02.11.2021).

[2] Организация и методика расследования отдельных видов экономических преступлений: Учеб. пос. / Под ред. А. И. Бастрыкина, А. Ф. Волынского, В. А. Прорвича. — М., 2016.

[3] Волынский А. Ф., Прорвич В. А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: Монография. — М., 2020.

[4] Судебно-экономическая экспертиза в уголовном процессе / Под ред. А. Ф. Волынского и В. А. Прорвича. Изд. 2-е, перераб. и доп. — М., 2021.

[5] Волынский А. Ф., Прорвич В. А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): Монография. — М., 2019.

[6] Волынский А. Ф. Предмет криминалистики и «научный сепаратизм»: последствия и возможности их преодоления // Тр. Акад. управл. МВД России. 2018. № 1 (45). С. 175 – 185.

[7] Волынский А. Ф., Прорвич В. А. Особенности формирования интегрированного правового фундамента электронного судопроизводства по преступлениям в сфере экономики // Российский журнал правовых исследований. — 2019. — Т. 6. — № 1 (18). — С. 149 – 158.

Гайдамашев А. В.,
директор компании Lie detection KZ,
сертифицированный специалист-полиграфолог,
ассоциированный член Международного сообщества
полиграфологов (ISOPE)
(Республика Казахстан, г. Алматы)

ФОРМЫ ПРИМЕНЕНИЯ РЕЗУЛЬТАТОВ ПОЛИГРАФОЛОГИЧЕСКОГО ТЕСТИРОВАНИЯ В ДОКАЗЫВАНИИ ПО УГОЛОВНО-ПРОЦЕССУАЛЬНОМУ ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ КАЗАХСТАН

Применение психофизиологического тестирования с использованием полиграфа (детектора лжи) имеет достаточно большую историю. Уже более 100 лет этот метод находит свое применение в уголовном судопроизводстве разных стран мира. И везде использование результатов полиграфологических тестирований вызывало споры и критику, связанные с диагностической природой этого метода и вероятностностью выводов.

Впервые сомнения в доказательственном значении данных, полученных в ходе тестирования на полиграфе, возникли в практике судов США в 1923 г. При рассмотрении дела об убийстве суд отказался принять в качестве доказательства результаты тестирования на полиграфе. Суд мотивировал это тем, что в тот период в научной среде не были выработаны твердые и надежные принципы тестирования на полиграфе, которые признавались бы авторитетными учеными в области психологии и физиологии. По итогам судебного разбирательства, на 70 лет был сформулирован стандарт, получивший название Fryerule, или прецедент Фрая. Джеймса Фрая обвиняли, в том, что он стрелял в Роберта В. Брауна, который от полученных ран скончался. Сначала Д. Фрай признался в том, что именно он стрелял в потерпевшего, но позже отказался от своих показаний и был подвергнут тестированию с использованием полиграфа. Результаты тестирования подтверждали, что Фрай говорил правду, утверждая, что не стрелял в Брауна. Суд исключил из дела результаты тестирования на полиграфе как недопустимое доказательство. Однако присяжные вынесли вердикт о виновности Фрая в убийстве второй, а не первой степени. Таким образом, он избежал смертной казни и получил пожизненное заключение. Апелляционный суд округа Колумбия, состоявшийся по инициативе стороны защиты Фрая, поддержал решение судьи об исключении результатов тестирования подсудимого на «лайдетекторе» из разбирательства дела[1].

После принятия этого прецедента практика использования результатов тестирования на полиграфе в качестве доказательств в судах США долгие годы была разнородной. На уровне различных судов штатов принимались компромиссные решения. При этом тестирование на полиграфе достаточно широко использовалось в качестве оперативного полицейского расследования. Оставались и проблемы придания результатам тестирований на полиграфе доказательственного значения. В специальной литературе США 50-х годов XX столетия звучало следующее мнение: «Для того чтобы суды США принимали результаты таких испытаний как достоверные доказательства, — говорится в решении верховного суда штата Пенсильвания, — нужно, чтобы с большей определенностью была установлена научная надежность и непогрешимость полиграфа и других методов психологического выявления обмана»[2, 602].

В 1993 г. в решении по делу Daubert v. MerrelDowPharmaceuticals, Inc (прецедент Дауберта) Верховный суд США подчеркнул, что стандарт, согласно которому достижения в области науки, с помощью которых добыто доказательство, должны быть общепризнанными в соответствующей научной сфере, не так важен, важно то, могут ли показания эксперта помочь судье и присяжным заседателям

разобраться в фактических обстоятельствах дела. При разрешении этого вопроса суд должен принять во внимание следующие обстоятельства:

1) верифицируемы ли те достижения в сфере науки и техники, с помощью которых получено доказательство;

2) подвергнуты ли эти данные проверке научным сообществом;

3) какова известная или потенциальная степень ошибки при использовании этих данных;

4) подтверждаются ли эти данные научным сообществом[3].

Таким образом, прецедент Дауберта отменил прецедент Фрая. Стоит отметить, что прецедент Дауберта не был прямо связан с использованием полиграфа. В суде разбирались клинические свойства медицинского препарата «Бендектин». Поводом к появлению этого прецедента послужили показания экспертов, которые противоречили общепризнанной точке зрения. Прецедентом Дауберта Верховный суд США расширил возможности привлечения большего числа различных экспертов, которым разрешено выступать в судах[4]. Частота применений полиграфологических тестирований в качестве доказательств в судах США возросла.

Следует упомянуть, что Американская Ассоциация полиграфологов (APA), являясь одним из крупнейших сообществ, занятых научными исследованиями в области полиграфа, в начале 2000-х годов инициировала ряд научных исследований. Эти исследования были направлены на повышение уровня научного подхода в деятельности полиграфологов и стандартизации методических подходов к полиграфологическому тестированию. Результатом научных исследований APA явилось Мета-аналитическое исследование критериальной точности обоснованных методов 2011 г. Таким образом, можно говорить, что были обобщены научные исследования в области инструментальной детекции лжи и в целом уровень научной разработанности этого метода возрос.

В США за долгие годы сформировалось и устоялось две формы использования результатов полиграфологического тестирования в доказывании:

1. Использование результатов полиграфологического тестирования при оперативном полицейском расследовании. Специалист, обладающий специальными познаниями, проводит тестирование с использованием полиграфа. Далее полученная информация используется в доказывании как ориентирующая и позволяющая собрать дополнительные доказательства по делу. Стоит упомянуть, что в США фактически отсутствует такая стадия уголовного процесса, как предварительное следствие.

2. Использование полиграфа в судах, в качестве исследования, проведенного экспертом, обладающим специальными познаниями в области полиграфологии. В ходе судебного разбирательства дела стороны привлекают к полиграфологическому тестированию эксперта, обладающего специальными познаниями. Результаты тестирования всесторонне исследуются и оцениваются судом и присяжными в соответствии с принципами прецедента Дауберта.

Первая форма применяется гораздо чаще, чем вторая. Вторая форма в отдельных штатах до сих пор запрещена.

Отдельной похвалы заслуживает уже упомянутый Мета-анализ, проведенный APA в 2011 г. В нем были стандартизированы методические подходы, используемые в различных формах использования полиграфа в доказывании. Так, все обоснованные (валидные) методы, в зависимости от своих критериальных характеристик точности, доли неопределенных результатов, чувствительности и специфичности разделены на три группы: доказательные методы, методы парного тестирования[5], следственные методы. Более жесткие требования по критериям точности предъявляются к Доказательным методам и Методам парного тестирования, так как они применяются при второй форме использования полиграфа в доказывании. К следственным методам предъявляются гораздо более демократичные требования по точности[6]. Такой подход обоснован тем, что в ходе расследования имеется возможность проверить полученные в ходе тестирования выводы другими методами, собрать и исследовать дополнительные доказательства.

Безусловно, американский опыт использования результатов полиграфологических тестирований в судопроизводстве без адаптации к реалиям казахстанской системы процессуального права перенять не представляется возможным. Однако общие принципы использования в доказывании результатов полиграфологических тестирований учесть и перенять просто необходимо.

В Советском Союзе применение полиграфа в судопроизводстве принималось в штыки. По мнению Р. С. Белкина, в процессуальной науке и криминалистике возобладала точка зрения Н. Н. Полянского, его аргументы оказали влияние на формирование в советской юридической науке в конце 40-х годов

резко отрицательного отношения к применению полиграфа в целях судопроизводства[7, 571 – 572] Аналогичной, критической точки зрения придерживался И. Ф. Пантелеев[8, 227]. Критический подход к использованию полиграфа в судопроизводстве главенствовал долгие годы. Дело доходило до объявления полиграфа орудием пыток, причиняющих испытуемому «неимоверные физические страдания»[9, 89]. Использование полиграфа клеймили как «псевдонаучный и реакционный способ «установления истины»[10, 76]. М. С. Строгович проводил прямые параллели между инквизиционным процессом и полиграфом[11, 674].

Была и более взвешенная точка зрения ученых Быховского И. Е. и Ратинова А. Р., Злобина Г. А. и Яни С. А., Андреева Г. Г. и Любарского М. Г. Эти ученые видели рациональное зерно в использовании результатов тестирования на полиграфе в судопроизводстве. Были в те времена и «белые вороны», которые пытались проводить научные исследования в области полиграфа и внедрять его использование в практику раскрытия и расследования преступлений. Примером такой «белой вороны» является И.Б. Зинкевич, который занимался проблематикой полиграфа в Карагандинской высшей школе МВД СССР еще в 70-х годах XX столетия[12].

Накануне и после развала СССР на проблему использованию полиграфа в судопроизводстве ученые и практики стали смотреть проще. Закономерно выдвигались идеи придания полиграфу статуса технико-криминалистического средства. Стали звучать предложения о выделении криминалистической полиграфологии в самостоятельный раздел криминалистической техники[13; 14]. Звучали предложения по использованию полиграфологического тестирования в форме участия специалиста-оператора научно-технического средства полиграфа в рамках такого следственного действия, как допрос. Однако эта форма использования полиграфологического тестирования немыслима в силу методических ограничений психофизиологического метода инструментальной детекции лжи. Рассматривались научные гипотезы о формировании нового процессуального действия — опроса с использованием полиграфа[15, 243 – 244].

К сегодняшнему дню в странах, бывших частью Советского Союза, в практике раскрытия и расследования преступлений сложились следующие три формы использования результатов полиграфологического тестирования при расследовании преступлений.

1. Полиграфологическое тестирование в форме гласного опроса с использованием научно-технического средства — полиграфа, в рамках проведения оперативно-розыскной деятельности. Полученная в ходе подобного тестирования информация носит характер гласной оперативно-розыскной информации;

2. Полиграфологическое тестирование в форме привлечения специалиста-полиграфолога, который приобретает статус лица, обладающего специальными познаниями, для проведения тестирования с использованием полиграфа. Полученная доказательственная информация приобретает форму заключения специалиста и может быть использована в качестве доказательства;

3. Полиграфологическое тестирование в форме судебной экспертизы. Полиграфолог приобретает статус судебного эксперта, а полученная в результате экспертизы информация может быть использована в качестве доказательства.

По большому счету, все три формы использования результатов полиграфологического тестирования в доказывании не противоречат законодательству Республики Казахстан.

Использование полиграфа при опросе в рамках ОРД вполне укладывается в регламентацию Закона Республики Казахстан от 15 сентября 1994 г. № 154-XIII «Об оперативно-розыскной деятельности»[16, 80].

Применение полиграфологического тестирования для целей раскрытия и расследования преступлений в форме участия специалиста в уголовном процессе не противоречит требованиям ст. 80 УПК РК. А правильно оформленное заключение специалиста в соответствии со ст. 117 УПК РК будет являться источником доказательств.

На первый взгляд, и третья форма использования полиграфа в доказывании — в качестве судебной экспертизы — не противоречит УПК РК. Однако в утвержденном в Республике Казахстан перечне видов судебных экспертиз, такой вид экспертизы отсутствует. В перечне видов работ и услуг, определяемых для выдачи лицензии на право судебно-экспертной деятельности, полиграфологические тестирования не значатся. Следовательно, провести судебную экспертизу с использованием полиграфа не представляется возможным. В то же время, перечисленные барьеры могут быть легко сняты ведомственными нормативно-правовыми актами.

На наш взгляд, использование результатов полиграфологического тестирования в доказывании в форме судебной экспертизы нецелесообразно и по методическим ограничениям метода. Психофизиологический метод инструментальной детекции лжи, хотя и является научным, но основан на эмпирических наблюдениях и статистических закономерностях. Кроме того, этот метод носит диагностический характер. Представляется, что указанные ограничения не позволяют отнести специальные знания в области инструментальной детекции лжи к категории специальных научных знаний.

Таким образом, использовать результаты полиграфологического тестирования в уголовном судопроизводстве Республики Казахстан целесообразно в форме опроса в рамках ОРД и в форме участия специалиста в уголовном процессе, в соответствии со ст. 80 УПК РК.

---

[1] Frye v. United States. 54 App. D. C. 46, 293 F. 1013 [1923].

[2] J. Criminal Law, Criminology and Police Science. 1955. Nov. Dec. # 4.

[3] Daubert v. Merrel Dow Pharmaceuticals, Inc. 509 U. S. 579 (1993).

[4] Гольцов А. Т. «Детектор лжи» в уголовном судопроизводстве США // Журнал российского права. — 2009. — № 4. — С. 72 – 85.

[5] Парное тестирование или «Протокол Марина» — практика тестирования с использованием полиграфа, предложенная Джонатаном Марином. С 2004 г. являетсястандартомсудопроизводства ASTM. См.: Marin, J. He said / She said: Polygraph evidence in court. Polygraph. 2000, 29(4). P. 299 – 304.

[6] См.: Голашевский М. Обоснованные методы и модели числовой оценки для анализа результатов тестирования на полиграфе // Избранные публикации из журнала «Европейский полиграф»: Сб. / Отв. ред. А. Б. Пеленицын. Вып. 1. — М., 2019. С. 24 – 39.

[7] Белкин Р. С. Курс Криминалистики: Учеб. пос. для вузов. — 3 изд., доп. — М., 2001.

[8] Пантелеев И. Ф. Некоторые вопросы психологии расследования преступлений // Тр. ВЮЗИ. 1971. Вып. XXIX.

[9] Резенблит С. Инквизиционные методы допроса подозреваемых в США // Соц. Законность. — 1954. — № 4.

[10] Каминская В. И. Рецензия на кн. Н. Н. Полянского «Доказательства в иностранном уголовном процессе: вопросы и тенденции нового времени» // Сов. книга. — 1947. — № 7.

[11] Строгович М. С. Курс советского уголовного процесса. — М., 1958.

[12] Алесковский С. Ю. Предыстория казахстанского полиграфа // Полиграф в Казахстане — избранные страницы: Библиотека полиграфолога / Под ред. С. Ю. Алесковского и Г. А. Алибаевой. — Алматы, 2016. С 3 – 10.

[13] Криминалистика/ Под ред. д-ра юрид. наук проф. В. А. Образцова. — М., 1997. С. 319 – 329.

[14] Холодный Ю. И. Криминалистическая полиграфология как новое направление раздела «Криминалистическая техника» // Теория и практика криминалистики и судебной экспертизы: Сб. ст. Акад. управл. МВД России. — М., 2003.

[15] Комиссарова Я. В. Профессиональная деятельность эксперта в уголовном судопроизводстве: теория и практика: Монография. — М., 2014.

[16] См.: Аубакирова А. А. Нормативное регулирование применения полиграфа в Республике Казахстан и России // Первые итоги и основные направления использования полиграфа в Казахстане: Мат-лымеждународ. науч.-практ. конф. Академии экономики и права и Евразийской ассоциации полиграфологов (17 марта 2014 г.). – Алматы, 2014.

Галяшина Е. И.,
профессор кафедры судебных экспертиз,
доктор юридических наук, доктор филологических наук, профессор
(Московский государственный юридический университет им. О. Е. Кутафина,
Российская Федерация)

ИСПОЛЬЗОВАНИЕ ЮРИДИКО-ЛИНГВИСТИЧЕСКИХ ТЕХНОЛОГИЙ В КРИМИНАЛИСТИЧЕСКОМ ОБЕСПЕЧЕНИИ МЕДИАБЕЗОПАСНОСТИ[1]

Современные инновационные технологии, глобальные коммуникационные сети охватывают практически все сферы деятельности человека и общества. Они на глазах меняют качество жизни людей, способствуют глобализации экономики и гуманитарного пространства. Однако развитие глобальных телекоммуникационных систем вызвало к жизни и новые угрозы безопасности и стабильности суверенных государств и мирового сообщества. Информационно-коммуникационные технологии нередко используются в преступных целях, в том числе для проведения компьютерных атак на информационные ресурсы, совершения преступлений в сфере компьютерной информации, мошенничества, в экстремистских и террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников; а также для вмешательства во внутренние дела суверенных государств[2].

В глобальной сети на отдельных сайтах ведется пропаганда терроризма и экстремизма, ксенофобии и религиозной вражды, размещается детская порнография и т.д. Контент интернет-ресурсов, нацеленных на продвижение идеологии экстремизма и терроризма, носит агрессивно-наступательный

характер, отличается разнообразием методов информационно-психологического воздействия на пользователей.

К таковым относятся:

- информационно-психологическое воздействие на население России, направленное на дестабилизацию внутриполитической и социальной ситуации в стране, подрыв суверенитета и нарушение территориальной целостности Российской Федерации;

- информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей;

- информационное воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

Новые медиа сегодня превратились в мощный инструмент манипуляции сознанием и поведением молодых людей, способный эффективно влиять на общественное мнение как в России, так и за рубежом. Специфика коммуникации в глобальной сети предоставляет такие преимущества, как простота доступа, независимость от географического расположения, неограниченная потенциальная аудитория, высокая скорость передачи информации, трудности в осуществлении контроля со стороны правоохранительных органов и другие.

Всеобъемлющая цифровизация и многообразие каналов коммуникации требует не только детальной правовой регламентации возникающих в связи с этим общественных отношений, но и разработки инновационных решений для эффективного противодействия распространению в медиапространстве фейковой, вредоносной (деструктивной) и криминогенной информации.

К угрозам медиабезопасности в интернет-среде можно отнести:

- деструктивную радикальную пропаганду и провокацию антиконституционных настроений (в том числе через идеи сепаратизма, насильственного свержения власти и др.);

- массовое тиражирование контента, связанного с популяризацией экстремистских идей (национализма, неофашизма, религиозного экстремизма т. п.);

- открытую либо закамуфлированную вербовку в радикально настроенные террористические группы и деструктивные сообщества через социальные сети и т. д.;

- распространение фальшивой (фейковой), клеветнической, диффамационной, оскорбительной информации в социальных сетях и мессенджерах (в отношении органов государственной власти, должностных лиц, отдельных граждан и юридических лиц);

- возбуждение ненависти, вражды и унижение по мотивам социальной принадлежности: языку, полу, национальности, расе, религиозным убеждениям и др.

Российское законодательство ограничивает распространение информации, которая относится к категории запрещенной. К данной категории причислена информация, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иная информация, за распространение которой предусмотрена уголовная или административная ответственность (ч. 6 ст. 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Важно отметить, что необходимость в противодействии криминогенным речевым действиям для обеспечения информационно-мировоззренческой безопасности основывается не только на действующих нормах законодательства, но и на положениях таких документов, как «Доктрина информационной безопасности Российской Федерации»[3] и «Стратегия национальной безопасности Российской Федерации»[4].

Указанные документы позволяют конкретизировать социокультурную сущность криминализированных речевых действий, что облегчает толкование формулировок приведенных в кодексах составов правонарушений (преступлений), однако, как показывает практика, их также явно недостаточно. Поскольку речевое действие входит в объективную сторону правонарушения, необходимы инновационные методы и средства исследования информационных материалов (и оценки результатов данных исследований), разработанные исходя из социокультурной и коммуникативной сущности противоправного речевого действия.

С одной стороны, недопустима цензура и ограничение прав людей на высказывание своего мнения, с другой — недопустимо злоупотреблением этими правами. Для этого нужно вооружить право-

охранительные органы объективной криториологией, позволяющий выявлять, пресекать и предупреждать речевые правонарушения в цифровой медиасреде. Значительная часть распространяемой криминальной информации выражается вербально, поэтому для правильной юридической квалификации речевого деяния нужны специальные юридико-лингвистические знания.

В целях выработки инновационного подхода к обеспечению медиабезопасности с 2019 года по трехлетнему гранту РФФИ нами разрабатывается научный проект «Концептуализация противодействия информационным угрозам в интернет-среде с использованием специальных юридико-лингвистических знаний». В его рамках определены понятийные основы криминалистического учения об информационно-мировоззренческой безопасности в интернет-среде, сформулирована криториология, позволяющая детерминировать вредоносный, криминогенный и деструктивный характер информационных материалов, свободно распространяемых в интернет-среде, конструированы типовые криминалистические диагностические комплексы признаков криминогенного речевого действия и его видовых представителей.

Разработанные типовые криминалистические диагностические комплексы признаков криминогенных речевых действий представляют собой модели криминогенных речевых действий — образцы-эталоны для сравнительной стадии диагностического исследования. Они являются основным средством для проведения криминалистических диагностических исследований криминогенных и деструктивных информационных материалов и разработаны для решения типовых задач по исследованию следов криминогенных речевых действий с целью установления в речевом продукте специальных признаков объективной стороны преступления (правонарушения)[5].

На основе обобщения судебной и судебно-экспертной практики (в том числе по делам, решениями по которым материалы включались в Федеральный список экстремистских материалов, по делам, решениями по которым сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, включались в Единый Реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещен), практики Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора), анализа нормативных правовых актов, устанавливающих ответственность за криминогенные речевые действия, а также междисциплинарного анализа научных публикаций, посвященных проблемам деструктивного информационного воздействия в сети Интернет, впервые был сформулирован новый классификатор и на его основе была произведена классификация форм репрезентации девиантного и деликвентного речевого поведения в цифровой среде, а именно было осуществлено разграничение контентных и коммуникационных рисков[6].

Исследование носит междисциплинарный интеграционный характер, обеспечивая синергетический эффект от комплексирования положений материального и процессуального права, информационного права, криминологии, криминалистики, судебной экспертологии, с одной стороны, и прикладной лингвистики — судебного речеведения (судебной лингвистики), психологии, девиантологии, педагогики и андрагогики, политологии и смежных наук, с другой стороны. Полученные на данном этапе исследования результаты, имеют значение не только для развития криминалистики, судебной экспертологии, судебного речеведения, но и для практики криминалистического обеспечения собирания цифровых следов при назначении судебных экспертиз криминогенных информационных материалов[7].

Комплексный юридико-лингвистический подход к криминалистическому обеспечению медиабезопасности в цифровой среде позволяет определить правовые рамки для регламентации интернет-среды в целях соблюдения баланса права человека на свободу слова и плюрализм мнений и защиту от вредоносной и криминогенной информации.

---

[1] Выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00190.

[2] Указ Президента РФ «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» от 12 апреля 2021 г. № 213. [Электронный ресурс]. — Режим доступа: http://www.garant.ru/products/ipo/prime/doc/40 0473497/ (дата обращения: 02.11.2021).

[3] Доктрина информационной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // СЗ РФ. — 2016. — № 50. — Ст. 7074.

[4] Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» от 9 мая 2017 г. № 203. [Электронный ресурс]. — Режим доступа: https://base.garant.ru/71670570/ (дата обращения: 02.11.2021).

[5] Галяшина Е. И., Никишин В. Д., Богатырев К. М. Типовые криминалистические диагностические комплексы криминогенных речевых действий // Судебная экспертиза. — 2021. — № 1 (65). — С. 16 – 31.

[6] Галяшина Е. И., Никишин В. Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lexrussica. — 2021. — Т. 74. — № 6 (175). — С. 79 – 93.

[7] Никишин В. Д., Галяшина Е. И. Юридико-лингвистический подход к исследованию поликодовых текстов криминогенной коммуникации в цифровой среде в целях обеспечения информационной (мировоззренческой) безопасности // Актуальные проблемы российского права. — 2020. — Т. 15. — № 6. — С. 179 – 193.

Дубик К. М.,
начальник отдела трасологических экспертиз
Управления автотехнических и трасологических экспертиз
Главного управления криминалистических экспертиз
центрального аппарата Государственного комитета
судебных экспертиз Республики Беларусь;
Гордынец С. И.,
инженер-программист
Республиканского унитарного предприятия
«Белсудэкспертобеспечение»;
Жолудева Д. В.,
научный сотрудник лаборатории технических
и криминалистических исследований научного отдела технических,
криминалистических и специальных исследованийНаучно-практического центра
Государственного комитета судебных экспертиз Республики Беларусь»,
магистр юридических наук
(Республика Беларусь, г. Минск)

К ВОПРОСУ АВТОМАТИЗАЦИИ УЧЕТА ТРАСОЛОГИЧЕСКИХ СЛЕДОВ

В Государственном комитете судебных экспертиз Республики Беларусь (далее — ГКСЭ) ведется учет трех видов трасологических следов — обуви, шин транспортных средств и статических следов орудий взлома. Ведение учетов еще до недавнего времени осуществлялось картотечным способом на бумажных носителях. Информационная карта представляла собой бумажный бланк, на одной из сторон которого имелись графы для ручного заполнения, на другую сторону наклеивались фотоснимки следов. Картотеки велись на двух уровнях — территориальном и региональном. При пополнении картотеки необходимо было путем ручного перебора провести сверку вновь помещаемого следа с имеющимся массивом (до 2 600 карт).Основными недостатками данного способа ведения учета являлись его архаичность и невозможность оперативно провести проверку по имеющемуся массиву карт. Кроме того, одним из постоянно отмечаемых недостатков являлось качество помещаемых фотоснимков с точки зрения их носителей — бумаги, способа печати.Поиск оптимального решения по автоматизации учета трасологических следов велся экспертными подразделениями Республики Беларусь с конца 90-х годов — с момента внедрения автоматизированной дактилоскопической идентификационной системы (далее — АДИС). Проблемы, сформировавшиеся в процессе поиска путей автоматизации трасологических учетов, условно подразделяются на две группы: объективного и субъективного характера.

К объективным проблемам относятся:

1) невозможность ввести математические методы обсчета следов (принцип действия АДИС);

2) кодировка изображений объектов для проведения сравнения с получением достоверного результата является коммерческой тайной, ее решение публичного распространения не имеет;

3) особенности и вариативность отображения следов, разнообразие трасологических следов и их признаков, а также достаточно редкая встречаемость среди них идеальных.

К проблемам субъективного характера относились отказ от финансирования разработки без гарантированного результата и невозможность планирования сроков реализации проекта из-за отсутствия технических решений.

К середине 2010-х годов в ГКСЭ изучены зарубежные продукты (компаний «Криммедтех», Россия, «Foster&Freeman's», Великобритания), а также имелись некоторые собственные наработки. Силами сотрудников (лиц гражданского персонала) управления ГКСЭ по Витебской области разработана автоматизированная база данных «Shoes» (далее — АБД «Shoes»). Апробация АБД «Shoes» проводилась в 2015 г. в управлениях ГКСЭ по Гродненской, Могилевской областям и г. Минску.В ходе апробации выявлены требующие доработки недостатки программного продукта, а также возникла необходимость в разработке переносной версии АБД «Shoes».Управлением ГКСЭ по г. Минску предлагалась к использованию автоматизированная информационно-поисковая система «Следопыт» (далее — АИПС «Следопыт»), которая является интегрированным модулем автоматизированной информационно-поисковой системы «Электронный журнал эксперта». При этом АИПС «Следопыт» признана менее продуктивной и уступающей по возможностям АБД «Shoes».

Ключевым моментом и поворотным событием в вопросе автоматизации учета трасологических следов явилось заседание коллегии ГКСЭ в ноябре 2016 г., постановлением которой решено автоматизировать данный вид учета.Во исполнение указанного решения главным управлением криминалистических экспертиз (далее — ГУКЭ) центрального аппарата ГКСЭ совместно с главным управлением финансов и тыла(далее —ГУФиТ) центрального аппарата ГКСЭ, РУП «Белсудэкспертобеспечение» в 2017 – 2019 гг. проведен комплекс мероприятий по организации разработки и внедрению в деятельность органов ГКСЭ автоматизированных информационно-поисковых систем (далее — АИПС) «TRACE», «TRACE-шина» и «TRACE-взлом» с целью автоматизации ведения учета трасологических следов — следов обуви, шин транспортных средств и статических следов орудий взлома соответственно.

Основным недостатком используемой системы АИПС «TRACE» была обособленность локальных баз в регионах: выгрузка в единый массив осуществлялась один раз в месяц, соответственно, сличение следов и оттисков в различных регионах становилось возможным только после консолидации баз, иными словами, происходило со значительным временным отставанием.

Последним словом в автоматизации трасологических учетов стала разработка новой автоматизированной информационно-поисковой системы «СЛЕД» (далее — АИПС «СЛЕД»), тестовая эксплуатация которой проведена в январе-марте 2021 г. Указанный программный продукт предназначен для ведения автоматизированным способом учета трасологических следов (обуви, шин транспортных средствиорудий взлома). АИПС «СЛЕД» разработана РУП «Белсудэкспертобеспечение» на основании технического задания, подготовленного ГУКЭ, в установленном порядке прошла соответствующую проверку в отделе организации технической защиты информации ГУФиТ.Ведение учета с использованием АИПС «СЛЕД» организовано на трех уровнях — республиканском, региональном и территориальном. Вся база учетных данных располагается на едином сервере в центральном аппарате ГКСЭ. Операторы АИПС «СЛЕД» территориальных органов ГКСЭ наделяются правами доступа в пределах компетенции и не имеют возможности изменить, скопировать либо выгрузить данные. Центральный аппарат ГКСЭ является администратором АИПС «СЛЕД», осуществляет контроль за формированием и ведением учета на региональном и территориальном уровнях в режиме онлайн.

Система позволяет осуществлять поиск объекта исследования, добавление нового объекта, изменение существующего объекта, его просмотр, создание отчета по существующему объекту исследования, просмотр пользователей и управление ими, а также создание резервной копии данных в базе данных.

Требуемые характеристики сервера (100 и более человек в системе):

- процессор: минимум 8 ядер с частотой от 3 ГГц;
- оперативная память: 16 ГБ, можно больше и быстрее;
- жесткий диск: современный SSD от 256 ГБ и больше;
- интернет-канал (DOWN/UP): 1 Gb/s и быстрее.

При разработке АИПС главной задачей было формирование принципа распознавания и сличения следов и оттисков. Формат распознавания изображения как такового был признан нецелесообразным из-за особенностей и вариативности отображения следов, их неидеальности, разных условий при проведении экспертами фотосъемки, ведущих к различному изображению объектов. АИПС «СЛЕД» работает по принципу сличения описаний элементов и их локализации в различных зонах, т.е. на эффективность работы системы напрямую влияет тщательное описание элементов следов, их расположения в следе, в процессе их занесения в базу.

Результаты сопоставления искомого следа с уже содержащимися в базе можно увидеть на рисунках № № 1 – 3.

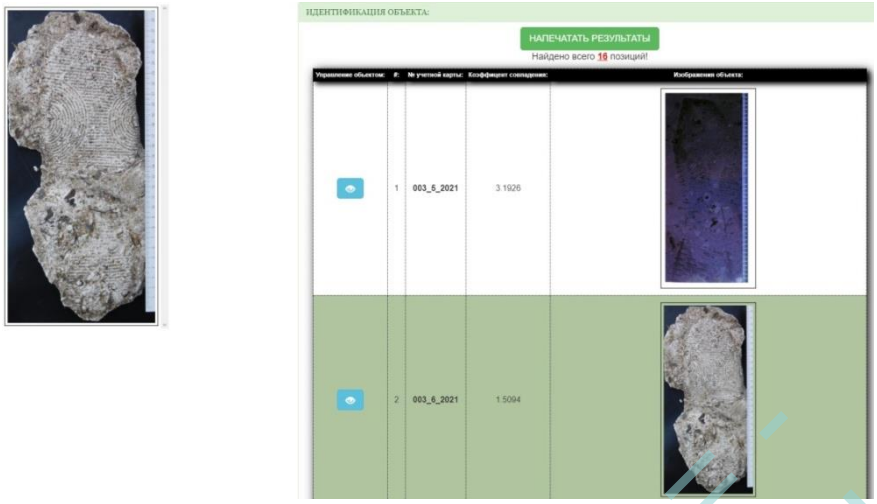


Рис.1. Результат сопоставления в АИПС «СЛЕД»

Рис. 2. Искомый след

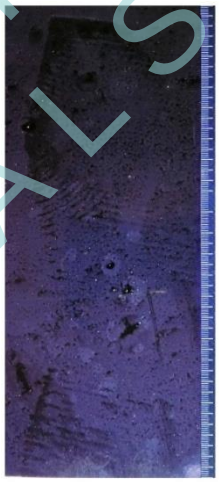


Рис. 3. Найденный след

Конкретные статистические данные по увеличению количества совпадений после внедрения АИПС «СЛЕД» представляют собой информацию, предназначенную исключительно для служебного пользования и запрещенную к распространению в открытой печати, однако, можно отметить, что резко возросшее количество совпаденийдает возможность оценить эффективность работы АИПС «СЛЕД» в 98 %.

Также следует отметить, что РУП «Белсудэкспертобеспечение» разработаны иные автоматизированные информационно-поисковые системы:

- «Маркировка транспортных средств» (учет результатов исследований идентификационных номеров транспортных средств (VIN);
- «Документ» (учет денежных знаков, бланков документов и ценных бумаг, изготовленных не предприятиями, осуществляющими их выпуск);
- «Запаховые следы человека»(ведение журнала экспертиз, проведенных по запаховым следам человека, изъятых с мест происшествий, учет иной информации);
- «Зарегистрированное оружие» (учет результатов отстрела нарезного оружия, находящегося в собственности юридических лиц и граждан).

Ералинов А. Б.,
главный криминалист Оперативно-криминалистического департамента
МВД Республики Казахстан, магистр технических наук, майор полиции;
Хасенов А. Ж.,
криминалист Оперативно-криминалистического департамента
МВД Республики Казахстан, капитан полиции;
Майленова А. Т.,
магистрант Евразийского национального университета им. Л. Н. Гумилева
(Республика Казахстан, г. Нур-Султан)

Исследование геномного полиморфизма аутосомной ДНК казахстанской популяции

Введение

Согласно официальным данным Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан по состоянию на 1 января 2021 г. численность населения Республики Казахстан составляет 18 879 552 человека. По этническому составу население Казахстана представлена в следующем соотношении, казахи составляют большую часть населения (69,01%), далее идут русские (18,42 %), узбеки (3,29 %), уйгуры (1,48 %), украинцы (1,36 %), татары (1,06 %) и другие[1]. Этническое разнообразие населения Казахстана весьма интересно с точки зрения генетики, так как данный факт является свидетельством генетического разнообразия казахстанской популяции, т. е. ее гетерогенности.

В экспертной и криминалистической практике среди лиц, в отношении которых проводятся молекулярно-генетические исследования, встречаются представители разных национальностей. Кроме того, сложностью при исследовании объектов, изъятых на месте происшествия является тот факт, что этническая принадлежность лиц, чьи следы изъяты с место происшествия нам неизвестна. Поэтому для получения достоверно значимого результата и проведения вероятностно-статистической обработки выявленных генотипов необходимо изучение генофонда всех этносов или крупных из них, проживающих на территории Республики Казахстан. Целью нашего исследования является исследование геномного полиморфизма аутосомной ДНК казахстанской популяция и определение частот встречаемости аллелей аутосомных STR-локусов.

Материалы и методы

Основным методом исследования является метод ПЦР в мультиплексном формате. Исследование STR-локусов казахстанской популяции проводили посредством использования метода прямой амплификации с применением наборов реагентов: «Globalfiler Express PCR Amplification Kit» и «Power Plex Fusion 6C System», производства компании «Applied Biosystems» и «Promega Corporation» в соответствии с прилагаемыми протоколами[2; 3]. Объектом исследования служили образцы буккальных эпителии (образцы слюны с ротовой полости человека), отобранные на специальный аппликатор с картами-носителями (Copan, Bode и FTA-карты). Исследование проводили на генетических анализаторах 3500/3500xl, производства компании «AppliedBiosystems»[4]. Сбор полученных данных, а именно выявленных генотипов осуществлялся в программе MS Excel. Выбор данной программы обусловлен гибкостью и удобством в работе с числовыми и текстовыми данными. Статистическая обработка результатов исследования проводилась посредством использования формул программы MS Excel с учетом закона Харди-Вайнберга.

Результаты и обсуждение

В ходе исследования были получены генотипы 5 839 представителей казахстанской популяции, включающих в себя 19 этносов, проживающих на территории Республики Казахстан. Количественное соотношение казахстанской популяции по этническому составу представлено следующим образом: казахи (55,39 %), русские (29,70 %), украинцы (3,25 %), узбеки (2,40 %), немцы (2,33 %), татары (1,68 %), белорусы (0,98 %), азербайджанцы (0,77 %), корейцы (0,53 %), цыгане (0,45 %), уйгуры (0,43 %), молдаване (0,38 %), чеченцы (0,38 %), таджики (0,29 %), башкиры (0,26 %), армяне (0,24 %),

ингуши (0,21 %), каракалпаки (0,19 %), курды (0,17 %). По половой принадлежности, соотношение мужчин и женщин составляет 88,06 % и 11,94 % соответственно. Исследование казахстанской популяции проводилось по следующим аутосомным STR-локусами: CSF1PO, D3S1358, vWA, D16S539, TPOX, D8S1179, D21S11, D18S51, D19S433, TH01, FGA, D5S818, D13S317, D7S820, D2S1338, D1S1656, D2S441, D10S1248, D12S391, D22S1045, PentaD, PentaE, SE33. Этимология наименования указанных генетических маркеров и их краткая характеристика представлена в[5]. Основными показателями, наиболее часто использующимися для характеристики полиморфизма является число наблюдаемых аллелей в STR-локусе и частота их встречаемости, а также степень гетерозиготности.

В ходе исследования установлены генотипы представителей казахстанской популяции по 23 аутосомным STR-локусам, включающие в себя в совокупности 403 аллеля (см. Таблица № 1). Наибольшее количество аллелей, и соответственно наибольшее значение полиморфизма характерна для STR-локуса SE33 (53 аллеля). Здесь самое наибольшее значение частоты встречаемости характерна для аллеля 19 (0,1516), а самое низкое – для аллелей 6, 6.3 и 15.2 (0,0002). Самое низкое количество аллелей и соответственно самое низкое значение полиморфизма у STR-локусов D13S317 и D5S818 (10 аллелей). Вместе с тем, наибольшее значение полиморфизма характерно для таких STR-локусов, как D18S51 (27 аллелей), D19S433 (21 аллель), D21S11 (23 аллеля), FGA (26 аллелей), Penta E (22 аллеля). А наиболее низкое значение полиморфизма характерна для STR-локусов, как D10S1248, D3S1358, TPOX (по 11 аллелей).

Таблица № 1. Аутосомные STR-локусы и их частоты встречаемости

1		2		3		4		5		6	
CSF1PO		D10S1248		D12S391		D13S317		D16S539		D18S51	
Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости
7	0,0010	8	0,0002	14	0,0007	7	0,0012	7	0,0007	7	0,0005
8	0,0031	10	0,0012	15	0,0411	8	0,3124	8	0,0322	8	0,0015
9	0,0743	11	0,0086	16	0,0324	9	0,2024	8,3	0,0003	9	0,0012
10	0,4768	12	0,0757	17	0,2067	10	0,2026	9	0,3126	10	0,0101
10,2	0,0002	13	0,4609	17,3	0,0252	11	0,4973	9,3	0,0003	11	0,0218
10,3	0,0002	14	0,4869	18	0,3632	12	0,3980	10	0,1904	11,2	0,0003
11	0,4821	15	0,3924	18,3	0,0224	12,3	0,0003	10,3	0,0002	12	0,1386
11,3	0,0003	16	0,2535	19	0,3011	13	0,1331	11	0,4401	12,2	0,0002
12	0,5604	17	0,0639	19,3	0,0120	14	0,0563	11,3	0,0003	12,3	0,0002
13	0,1219	18	0,0039	20	0,2723	15	0,0029	12	0,4730	13	0,2660
14	0,0259	19	0,0003	20,3	0,0014			13	0,2915	13,2	0,0002
15	0,0046			21	0,1913			14	0,0538	13,3	0,0002
16	0,0002			21,3	0,0002			15	0,0043	14	0,3554
				22	0,1661					14,2	0,0002
				23	0,1185					15	0,2864
				24	0,0533					16	0,2715
				25	0,0207					17	0,1738
				26	0,0050					17,2	0,0002
				27	0,0007					18	0,1204
										19	0,0966
										20	0,0562
										21	0,0365
										22	0,0271
										23	0,0084
										24	0,0051
										25	0,0026
										26	0,0003

7		8		9		10		11		12	
D19S433		D1S1656		D21S11		D22S1045		D2S1338		D2S441	
Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости
6,2	0,0005	8	0,0003	24,2	0,0002	6	0,0002	13	0,0002	8	0,0012
9,2	0,0003	9	0,0002	24,3	0,0002	9	0,0007	14	0,0002	9	0,0092
10	0,0009	10	0,0021	25	0,0009	10	0,0019	15	0,0005	10	0,3977
10,2	0,0003	11	0,1546	26	0,0026	11	0,3768	16	0,0497	11	0,6184
11	0,0089	12	0,1634	27	0,0281	12	0,0332	17	0,2507	11,3	0,0769
11,2	0,0002	13	0,1331	27,2	0,0003	13	0,0045	18	0,1889	12	0,1427
12	0,1267	14	0,1565	28	0,1990	14	0,0831	19	0,2980	12,3	0,0024
12,2	0,0051	14,3	0,0015	28,2	0,0048	15	0,4830	20	0,2574	13	0,0428
13	0,4263	15	0,3429	29	0,3985	16	0,4785	21	0,0581	13,3	0,0003
13,2	0,0558	15,3	0,0538	29,2	0,0041	17	0,2029	22	0,0731	14	0,3571
14	0,5316	16	0,3275	29,3	0,0002	18	0,0308	22,2	0,0002	15	0,0594
14,2	0,1094	16,3	0,0629	30	0,4765	19	0,0048	23	0,2447	16	0,0077
15	0,2387	17	0,1218	30,2	0,0714	20	0,0009	23,2	0,0002		
15,2	0,1726	17,3	0,1851	30,3	0,0014			24	0,2163		
16	0,0598	18	0,0116	31	0,1639			24,2	0,0002		
16,2	0,0492	18,3	0,0951	31,2	0,1505			25	0,1889		
17	0,0087	19	0,0017	32	0,0274			26	0,0402		
17,2	0,0125	19,3	0,0240	32,2	0,2156			27	0,0091		
18	0,0009	20,3	0,0010	33	0,0041			28	0,0031		
18,2	0,0062			33,2	0,0762						
19,2	0,0002			34	0,0002						
				34,2	0,0084						
				35,2	0,0015						

13		14		15		16		17		18	
D3S1358		D5S818		D7S820		D8S1179		FGA		Penta D	
Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости
9	0,0005	6	0,0002	5	0,0002	6	0,0021	15	0,0002	5	0,0002
11	0,0009	7	0,0325	7	0,0224	8	0,0147	16	0,0007	6	0,0295
12	0,0015	8	0,0027	7,3	0,0002	9	0,0110	17	0,0010	7	0,0096
13	0,0036	9	0,1048	8	0,3626	10	0,1545	18	0,0259	8	0,0358
14	0,1668	10	0,1807	8,2	0,0002	11	0,1237	18,2	0,0003	9	0,4282
15	0,5109	11	0,5946	9	0,2081	12	0,2572	19	0,1103	10	0,2430
16	0,4835	12	0,5301	9,3	0,0002	12,3	0,0007	19,2	0,0002	11	0,2980
17	0,3855	13	0,2699	10	0,4167	13	0,5235	19,3	0,0002	12	0,2773
18	0,2019	14	0,0188	11	0,4165	13,3	0,0003	20	0,1666	13	0,2512
19	0,0139	15	0,0026	11,2	0,0002	14	0,4021	20,2	0,0019	14	0,0962
20	0,0010			11,3	0,0003	15	0,2303	21	0,2757	15	0,0283
				12	0,3100	16	0,0738	21,2	0,0057	16	0,0089
				13	0,0629	17	0,0122	22	0,3095	17	0,0009
				14	0,0055	18	0,0033	22,2	0,0128		
				15	0,0003	19	0,0003	23	0,3148		
								23,2	0,0101		
								24	0,3269		
								24,2	0,0053		
								25	0,2064		
								25,2	0,0014		
								26	0,0723		
								26,2	0,0003		
								27	0,0137		
								28	0,0027		
								29	0,0002		
								30	0,0003		

Продолжение таблицы № 1

19		20		21		22		23	
Penta E		SE33		TH01		TPOX		vWA	
Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости	Аллель	Частота встречаемости
5	0,0927	6	0,0002	3	0,0005	5	0,0002	8	0,0003
6	0,0007	6,3	0,0002	5	0,0017	6	0,0009	12	0,0007
7	0,1639	8	0,0019	6	0,3483	7	0,0026	13	0,0053
8	0,0253	9	0,0005	6,3	0,0005	8	0,8036	14	0,1952
9	0,0240	10	0,0005	7	0,3756	9	0,1988	15	0,1572
10	0,1570	11	0,0015	7,3	0,0010	10	0,0957	16	0,3656
11	0,1639	12	0,0075	8	0,2053	11	0,4585	17	0,4936
12	0,2079	12,2	0,0009	8,3	0,0009	12	0,0663	17,3	0,0002
13	0,1499	13	0,0123	9	0,4520	13	0,0053	18	0,3920
14	0,1245	13,2	0,0005	9,3	0,3869	15	0,0002	18,3	0,0015
15	0,1464	14	0,0380	10	0,0188	16	0,0002	19	0,1692
16	0,1454	14,2	0,0019	10,3	0,0003			20	0,0259
17	0,1362	14,3	0,0009	11	0,0005			21	0,0024
18	0,1045	15	0,0507					22	0,0002
19	0,0531	15,2	0,0002						
20	0,0332	15,3	0,0010						
21	0,0176	16	0,0856						
22	0,0206	16,2	0,0003						
23	0,0120	16,3	0,0017						
24	0,0034	17	0,1070						
25	0,0007	17,2	0,0017						
26	0,0007	18	0,1351						
		18,2	0,0005						
		19	0,1516						
		19,2	0,0027						
		19,3	0,0005						
		20	0,1267						
		20,2	0,0128						
		21	0,0817						
		21,2	0,0200						
		22	0,0259						
		22,2	0,0406						
		23	0,0046						
		23,2	0,0517						
		24	0,0009						
		24,2	0,0671						
		25	0,0003						
		25,2	0,0872						
		26	0,0009						
		26,2	0,0904						
		27	0,0031						
		27,2	0,1202						
		28	0,0015						
		28,2	0,1237						
		29	0,0009						
		29,2	0,1230						
		30	0,0005						
		30,2	0,0897						
		31	0,0003						
		31,2	0,0582						
		32	0,0010						
		32,2	0,0284						
		33	0,0053						

Выводы

Полученные в ходе исследования результаты, содержащие частоты встречаемости аллелей 23-х аутосомных STR-локусов актуальны и значимы для практического применения в судебной экспертизе и криминалистике для получения достоверно значимых результатов исследования ДНК при генетической идентификации и установлении биологического родства.

---

[1] Официальный сайт Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан: https://stat.gov.kz.

[2] Руководство пользователя набора реагентов «Globalfiler Express PCR Amplification Kit», производства компании «Applied Biosystems» (Globalfiler™ Express PCR Amplification Kit Userguide).

[3] Руководство пользователя набора реагентов «Power Plex Fusion 6C System», производства компании «Promega Corporation» (Technical manual PowerPlex® Fusion 6C System for Use on the Applied Biosystems® Genetic Analyzers).

[4] Руководство пользователя генетического анализатора 3500/3500xl (Applied Biosystems 3500/3500xl Genetic Analyzer User Guide).

[5] Jaiprakash G. Shewale, Ph. D., Ray H. Liu. Forensic DNA Analysis Current Practices and Emerging Technologies. Taylor & Francis Group, LLC CRC Press. 2014 PP. 185 – 191.

Есимбетова Б. Е.,
докторант факультета послевузовского образования
(Академия МВД Республики Узбекистан,г. Ташкент)

К ВОПРОСУ ОКРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИЧИНЕНИЕМ ТЕЛЕСНЫХ ПОВРЕЖДЕНИЙ

Как известно, задача построения в Узбекистане демократического государства, основанного на верховенстве закона, требует создания эффективного механизма обеспечения прав и свобод человека во всех сферах жизни. В этом процессе совершенствование уголовного и уголовно-процессуального законодательства является основной целью уголовно-правовой политики как приоритет проводимых реформ по демократизации общества и модернизации страны.

Каждая характеристика представляет собой описание существенных сторон, свойств, закономерностей отражаемого в ней объекта реальной действительности в целом или каких-то его компонентов, фрагментов, которыми он отличается от других объектов окружающего мира.

Своеобразие криминалистической характеристики преступлений определяется двумя моментами: во-первых, особенностями отражаемой в ней реалии ее признаков; во-вторых, спецификой целей подобного отражения. Существует три уровня (типа) криминалистической характеристики: уровень отдельного, а также особенный и общий уровни. Существенное значение для оптимизации деятельности по расследованию и раскрытию той или иной категории преступлений имеет криминалистическая характеристика преступлений[1, 22].

Криминалистическая характеристика преступления представляет собой совокупность таких данных об общественно опасном деянии, которые способствуют быстрому и полному раскрытию преступления, включает сведения об особенностях подготовки, совершения и сокрытия преступлений[2, 369].

Как справедливо отмечает А. Ю. Головин, криминалистическая характеристика выступает в роли информационной модели преступления, отражающей типичные закономерности механизма его совершения[3, 91].

Данная научная категория направлена на изучение и систематизацию криминалистически значимых признаков определенного вида преступлений и их взаимосвязей, для последующего построения и проверки следственных версий. На сегодняшний день криминалистическая характеристика преступлений является неотъемлемым элементом заключительного раздела криминалистики — методики расследования преступлений, без учета которого формирование частных методик расследования определенных категорий (групп, видов) преступлений невозможно[4, 52].

Неоценимый вклад по внедрению криминалистической характеристики в состав методики расследования преступлений своими трудами внес Л. А. Сергеев[5, 438; 6, 4 – 5].

Вместе с тем, в научной среде до сих пор существуют большое количество различных взглядов на определение криминалистической характеристики преступлений.

Так, Е. П. Ищенко под данной категорией понимает «своеобразный обобщенный “портрет” преступления, научную абстракцию, аккумулирующую то общее, что объединяет множество конкретных преступлений»[7, 222].

Так, А.М. Шмонин отмечает: «Возникновение криминалистической характеристики преступлений как системного описания существенных сторон, свойств, признаков и внутренних связей отражаемого в ней объекта не стало случайным, а было связано, прежде всего, с углубленной разработкой методики расследования отдельных видов преступлений, а также с формированием теоретических основ криминалистики[8, 143].

А. Ф. Лубин в качестве криминалистической характеристики рассматривает «сущностное выводное знание о преступной деятельности», выступающее наряду с организационными и техническими средствами «в качестве информационного средства расследования». Указывая при этом, что «это опережающие, предпосылочные сведения о закономерностях функционирования объекта (предмета), которые обусловливают закономерности расследования»[9].

В свою очередь, В. А. Гуляев под криминалистической характеристикой предлагает понимать «систему устойчивых признаков определенного вида преступления, проявляющую себя вовне материальными и идеальными (или интеллектуальными) следами, образованными последовательными в пространстве и во времени действиями преступника в пределах причинно связанных с преступлением предшествующих ему событий, при совершении преступления и в течение причинно связанных с ним последующих событий»[10, 59 – 60].

Аналогичным образом к определению данной категории подходит и Н. П. Яблоков, рассматривая криминалистическую характеристику преступления как «систему научного описания криминалистически значимых признаков вида, разновидности, группы преступлений и отдельного преступления, проявляющихся в особенностях таких ее элементов, как способ, механизм и обстановка его совершения, личность его субъекта и иных особенностях определенного вида преступной деятельности, дополненную выявленной и статистически обработанной информацией о характере закономерных связей между ее элементами»[11, 28 – 29].

Анализируя вышепредставленные и иные определения криминалистической характеристики преступлений, нельзя не согласиться с высказываемым некоторыми учеными мнением о том, что попытка выделить изимеющихся или сформировать самостоятельно универсальное определение данной научной категории — бесперспективна[12, 91; 13, 20].

В то же время следует обратить внимание на то, что большинство исследователей рассматривают криминалистическую характеристику преступлений как систему сведений о типичных признаках определенной категории (вида, группы) преступлений, знание которых значительно повышает эффективность расследования и раскрытия данной категории преступлений.

Таким образом, под криминалистической характеристикой преступлений, связанных с умышленным причинением телесного повреждения, следует понимать систему криминалистически значимых сведений о наиболее типичных мотивах, способах, времени и местах совершения преступлений данной категории, а также об общих признаках, характеризующих особенности личности лиц, совершивших указанные преступные деяния или непосредственно пострадавших от их совершения.

Между тем, единообразного понимания структуры криминалистической характеристики преступлений в научной среде на сегодняшний день нет. Выработка единой структуры криминалистической характеристики преступлений, выступающей в качестве готовой модели для формирования видовых и межвидовых криминалистических характеристик, несмотря на неоднократные попытки, не увенчалась успехом. К настоящему моменту в юридической литературе устоялась точка зрения о том, что содержание криминалистической характеристики не является константой, и варьируется в зависимости от изучаемой категории (вида, состава) преступлений[14, 23–25; 15, 330; 16, 78 – 82].

В то же время мнения ученых рознятся в вопросе: что должно выступать в качестве первоосновы, базиса, отправной точки для построения криминалистической характеристики? Анализ специальной юридической литературы позволил выделить две наиболее распространенные точки зрения по данному вопросу. Так, одна группа ученых полагает, что основанием для построения криминалистической характеристики является состав преступления[17, 58 – 61; 18, 43].

В противовес данному суждению выступает плеяда исследователей, рассматривающих в качестве фундамента криминалистической характеристики предмет доказывания по уголовному делу[19, 165; 20, 326].

Наиболее рациональной нам представляется точка зрения, согласно которой основанием для создания криминалистической характеристики преступлений является функционально-деятельная структура общественно опасного деяния, состоящая из субъекта, его способа действий, предмета посягательства, преступного результата, времени, места и обстановки совершения преступления[21, 92].

В этой связи внимания заслуживает позиция А. В. Самойлова о том, что для построения эффективной криминалистической характеристики преступлений ее структурные элементы должны соответствовать следующим критериям:

1) быть теоретически доказанными;

2) быть значимыми для научного и практического решения задач по выявлению, раскрытию преступлений и осуществлению уголовного преследования виновных, раскрытию преступлений[22, 5 – 6].

С учетом изложенного нам представляется, что структуру криминалистической характеристики преступлений, связанных с умышленным причинением тяжкого вреда здоровью, образуют следующие элементы:

- мотивы и цели преступлений, связанных с умышленным причинением тяжкого вреда здоровью;
- обстановка совершения преступления (время, место и другие обстоятельства);
- основные способы совершения исследуемой категории преступлений;
- особенности личности субъекта противоправного деяния;
- особенности личности потерпевшего лица.

Аналогично, с незначительными дополнениями или изъятиями, структуру криминалистической характеристики преступлений, связанных с умышленным причинением вреда здоровью, рассматривают и другие исследователи[23, 36; 24, 14 – 16].

Анализ представленных элементов через познание механизма преступной деятельности позволит выстроить эффективный алгоритм расследования.

---

[1] Норбаев А. Н, Закутский А. С. Методика расследования преступлений: Учеб. пос. — Ташкент, 2006.

[2] Миразов Д. М. Криминалистика: Учебн. — Ташкент, 2017.

[3] Головин А. Ю. Роль криминалистической характеристики преступления в структуре частной криминалистической методики //Актуальные проблемы современной юридической науки и практики: Мат-лыМеждународ. науч.-практ. конф. – Ростов-н/Д, 2013.

[4] Головин А. Ю. Криминалистическая характеристика преступлений как категория современной криминалистики // Изв. ТулГУ. Экономические и юридические науки. 2012. Вып. 1. Ч. 1. Юридические науки.

[5] Сергеев Л. А. Сущность и значение криминалистической характеристики преступлений: Руководство для следователей. — М., 1971.

[6] Сергеев Л. А. Расследование и предупреждение хищений, совершаемых при производстве строительных работ: Дис. … канд. юрид. наук. — М., 1966.

[7] Ищенко Е. П., Топорков А. А. Криминалистика: Учебн. / Под ред. Е. П. Ищенко. — М., 2006.

[8] Шмонин А. В. Методология криминалистической методики: Монография. — М., 2010.

[9] Лубин А. Ф. в качестве криминалистической характеристики рассматривает «сущностное выводное знание о преступной деятельности», выступающее наряду с организационными и техническими средствами «в качестве информационного средства расследования». Указывая при этом, что «это опережающие, предпосылочные сведения о закономерностях функционирования объекта (предмета), которые обусловливают закономерности расследования».

[10] Гуляев В. А. Содержание и значение криминалистических характеристик преступлений // Криминалистическая характеристика преступлений. — М., 1984.

[11] Криминалистика: Учебн. для вузов / Н. П. Яблоков. — 2-е изд., перераб. и доп. — М., 2014.

[12] Латушкина С. Г. Об определении понятий предмета криминалистики и криминалистической характеристики преступлений // Законность и правопорядок в современном обществе. — 2014. — № 19.

[13] Вдовин А. Н. Особенности методики расследования и поддержания государственного обвинения по уголовным делам о преступлениях, связанных с незаконным оборотом оружия и боеприпасов: Дис. … канд. юрид. наук. — Новосибирск, 2015.

[14] Копыткин С. А. Криминалистическая характеристика преступлений, совершенных лицами, страдающими психическими расстройствами // Российский следователь. — 2010. — № 16.

[15] Криминалистика / Под ред. И. Ф. Герасимова, Л. Я. Драпкина. — М., 1994.

[16] Амрахов Н. И. К вопросу о криминалистической характеристике преступлений против конституционных прав человека // Науч. вед. Белгородск. гос. ун-та. Серия: философия, социология, право. 2012. № 22.

[17] Гуняев В. А., Басалаев А. Н. Криминалистическая характеристика преступлений // Криминалистическая характеристика преступлений. — М., 1984.

[18] Колесниченко А. Н., Суетнов В. П., Хотенец В. М. Проблемы развития методики расследования преступлений // Совершенствование расследования преступлений. — Иркутск, 1980.

[19] Гавло В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. — Томск, 1985.

[20] Топорков А. А. Криминалистика: Учебн. — М., 2013.

[21] Григорович В. Л., Федоров Г. Н. Теоретические взгляды на структуру криминалистической характеристики преступлений в сфере наркобизнеса // Вестн. Сибирск. юрид. ин-та ФСКН России. 2013. № 1.

[22] Самойлов А. В. Современное состояние учения о криминалистической характеристике преступлений // Российский следователь. — 2010. — № 22.

[23] Беспечный О. В. Теоретические и практические проблемы расследования преступлений, связанных с причинением тяжкого вреда здоровью: Дис. … канд. юрид. наук. — М., 2003.

[24] Карева А. А. Расследование преступлений по уголовным делам об умышленном причинении вреда здоровью: Дис. … канд. юрид. наук. — М., 2006.

Жабагин М. К.,
заведующий лабораторией генетики человека,
кандидат биологических наук, PhD, ассоциированный профессор
(Национальный центр биотехнологии,
Республика Казахстан, г. Нур-Султан)

Генетическое прогнозирование цвета глаз, волос и кожи для криминалистики

Генетическое прогнозирование внешних видимых характеристик индивида является одной из перспективных и быстро развивающихся областей в судебной биологии. К таким характеристикам относятся фенотипы цвет глаз, волос и кожи как наиболее заметные для использования в криминалистической практике, когда невозможно установить личность с помощью ДНК-дактилоскопии.

Генетическое прогнозирование внешних видимых характеристик индивида основано на ассоциации генотипа с фенотипом. Аллели генотипа выражаются в разнообразии фенотипа, обусловленные генетическим полиморфизмом в кодирующих и регуляторных областях ДНК, которые приводят к заменам аминокислот, изменяя функциональные свойства транслируемого белка. Различия между цветом глаз, волос и кожи в основном зависят от типа, количества и распределения меланина, продукта окислительных превращений аминокислоты тирозина в клетках меланоцитов[1; 2].

Существуют два типа меланина — эумеланин и феомеланин, имеющих соответственно коричнево-черную и желто-красную окраску. Возможность поглощать весь спектр цвета первым типом, и наоборот отражать широкий спектр цвета вторым типом, позволяет наблюдать цвет глаз от черного до зеленого. При отсутствии меланина можно наблюдать серый и голубой цвет глаз[3; 4].

В настоящее время ведется большое количество исследований по поиску генетического полиморфизма в виде однокулеотидных замен ДНК, отвечающих за цвет глаз, волос и кожи. Наиболее значимые из этих сайтов были включены в систему прогнозирования внешних видимых характеристик индивида IrisPlex для цвета глаз[5], затем в HIrisPlex для цвета глаз и волос[6], и расширенную версию системы генетического прогнозирования HIrisPlex-S для цвета глаз, волос и кожи[7]. Эти системы преимущественно разрабатывались европейских популяциях.

Прогнозирование цвета глаз основано на 6 однокулеотидных заменах ДНК в генах пигментации (HERC2, OCA2, SLC24A4, SLC45A2, TYR и IRF4), позволяя различать голубые и карие глаза с высокой точностью >90 % как в однородных, так и в смешанных популяциях. Однако валидация предсказательной силы этих однокулеотидных замен в выборках из азиатских популяций не показало такой же высокой точности[8], что требует проводить поиск дополнительных генетических маркеров специфичных для разных популяций.

Прогнозирование цвета волос основано на 18 однокулеотидных заменах ДНК в генах пигментации (MC1R, TUBB3, SLC45A2, KITLG, LOC105374875, IRF4, TYR, OCA2, SLC24A4, HERC2, PIGU, LOC105370627 и TYRP1) и 6 однокулеотидных замен ранее использовавшимся при прогнозировании цвета глаз. Система позволила различать с точностью 75 – 92 % четыре типа цвета волос — черный, коричневый, красный и светлый. Однако прогнозирование имеет ограничение по индивидам, у которых цвет волос менялся на протяжении всей жизни — обычно в детстве более светлый цвет и потемнее в возрасте от 6 до 13 лет. В этой связи актуально стоит вопрос связанный с поиском генетических маркеров возрастных фенотипов, которые могут объяснять частичное более низкое значение точности для светлых волос — только 69,5 % против 78,5 %, 80 % и 87,5 % для коричневого, красного и черного цвета соответственно. Недавнее исследование молодых людей выявило, что модель HIrisPlex неверно предсказывает фенотип волос для тех людей, которые в раннем детстве имели более светлые

волосы[9]. Это указывает на необходимость поиска новых маркеров, которые могли бы уменьшить коэффициент таких ошибок.

Прогнозирование цвета кожи основано на 36 однокулеотидных заменах ДНК в 17 генах пигментации (MC1R, HERC2, OCA2, SLC45A2, KITLG, EXOC2, TYR, SLC24A4, IRF4, ASIP и TYRP1 и другими). Результат прогнозирования цвета кожи определяет пять категорий: очень бледная, светлая, смуглая, темная, черная с получением точности от 72 – 97 %. Цвет кожи является одним из наиболее сложных изученных фенотипов пигментации, так как его формирование находится под сильным давлением естественного отбора и определяется балансом защиты от ультрафиолета и необходимого уровня синтеза витамина D. В связи с этим высокие корреляции фенотипа и генотипа можно ожидать только в разрезе определенных популяций, тогда как для однородных популяцийбывает весьма сложно различить цвета кожи между отдельными подгруппами популяций[10].

Модель генетического прогнозирования систем IrisPlex, HIrisPlex и HIrisPlex-S интегрирована в общедоступный интерактивный инструмент (https://hirisplex.erasmusmc.nl/), используемый для предсказания цвета глаз, волос и кожи по данным ДНК. На сайт вносятся данные генотипа по 41 однонуклеотидным полиморфизмам для получения вероятностей для трех категорий цвета глаз, четырех волос и пяти категорий цвета кожи.

Популяция казахов относиться к смешанному антропологическому типу — южносибирской расе. Это одна из переходных рас между монголоидами и европеоидами, сложившаяся в процессе их смешения на юге Сибири, в Казахстане и Средней Азии. Фенотипическое разнообразие внешности лица казахской популяции представлено от темного до светлого цвета глаз, волос и кожи. Сравнительные исследования генофондов популяций разных регионов указывают, что популяции из пограничных регионов между Азией и Европой генетически отличаются от европейских популяций, поэтому светлые фенотипы могут иметь отличительные генетические основы пигментации[11]. В связи с этим важно оценить точность предикции цвета глаз, волос и кожи по генетическим маркерам системы HIrisPlex-S в популяции казахов для принятия решения внедрения этой системы в отечественную практику судебно-медицинской экспертизы. При необходимости дополнить систему полиморфными сайтами специфичных для казахской популяции с целью повысить достоверность прогнозирования.

Национальный центр биотехнологии КН МОН РК совместно с Карагандинской академией МВД РК им. Б. Бейсенова запустили первую фазу исследования генетической вариабельности цвета глаз, волос и кожи в популяции казахов. В рамках исследования в 2021 г. сформирована выборка образцов ДНК добровольцев с более 1 000 фотографиями внешности лица, которая будет генотипирована по системе HIrisPlex-S. Значимость исследования кроме сферы криминалистики, также имеется для сферы медицины (патология пигментации), физической антропологии и археологии (реконструкция внешности по древней ДНК). Созданные предпосылки для изучения генетических основ разнообразия фенотипов внешности в популяции казахов будут задействованы в смежных науках.

---

[1] Wielgus A. R., Sarna T. Melanin in human irides of different color and age of donors. Pigment Cell Res. 2005 Dec; 18 (6): 454-64. doi: 10.1111/j.1600-0749.2005.00268.x. PMID: 16280011.

[2] Sturm R. A., Frudakis T. N. Eye colour: portals into pigmentation genes and ancestry. Trends Genet. 2004 Aug; 20 (8): 327-32. doi: 10.1016/j.tig.2004.06.010. PMID: 15262401.

[3] Larsson M., Duffy D. L., Zhu G, Liu J. Z., Macgregor S., McRae A. F., Wright M. J., Sturm R. A., Mackey D. A., Montgomery G. W., Martin N. G., Medland S. E. GWAS findings for human iris patterns: associations with variants in genes that influence normal neuronal pattern development. Am J Hum Genet. 2011 Aug 12; 89 (2): 334-43. doi: 10.1016/j.ajhg.2011.07.011. PMID: 21835309; PMCID: PMC3155193.

[4] Prota G., Hu D. N., Vincensi M. R., McCormick S. A., Napolitano A. Characterization of melanins in human irides and cultured uveal melanocytes from eyes of different colors. Exp Eye Res. 1998 Sep; 67 (3): 293-9. doi: 10.1006/exer.1998.0518. PMID: 9778410.

[5] Walsh S., Liu F., Ballantyne K. N., van Oven M., Lao O., Kayser M. IrisPlex: a sensitive DNA tool for accurate prediction of blue and brown eye colour in the absence of ancestry information. Forensic SciInt Genet. 2011 Jun; 5 (3): 170-80. doi: 10.1016/j.fsigen.2010.02.004. Epub 2010 Mar 27. PMID: 20457092.

[6] Walsh S., Liu F., Wollstein A., Kovatsi L., Ralf A., Kosiniak-Kamysz A., Branicki W., Kayser M. The HIrisPlex system for simultaneous prediction of hair and eye colour from DNA. Forensic SciInt Genet. 2013 Jan; 7 (1): 98-115. doi: 10.1016/j.fsigen.2012.07.005. Epub 2012 Aug 20. PMID: 22917817.

[7] Chaitanya L., Breslin K., Zuñiga S., Wirken L., Pośpiech E., Kukla-Bartoszek M., Sijen T., Knijff P., Liu F., Branicki W., Kayser M., Walsh S. The HIrisPlex-S system for eye, hair and skin colour prediction from DNA: Introduction and forensic developmental validation. Forensic SciInt Genet. 2018 Jul; 35: 123-135. doi: 10.1016/j.fsigen.2018.04.004. Epub 2018 Apr 12. PMID: 29753263.

[8] Yun L., Gu Y., Rajeevan H., Kidd K. K. Application of six IrisPlex SNPs and comparison of two eye color prediction systems in diverse Eurasia populations. Int J Legal Med. 2014 May; 128 (3): 447-53. doi: 10.1007/s00414-013-0953-1. Epub 2014 Jan 7. PMID: 24395150.

[9] Kukla-Bartoszek M., Pośpiech E., Spólnicka M., Karłowska-Pik J., Strapagiel D., Żądzińska E., Rosset I., Sobalska-Kwapis M., Słomka M., Walsh S., Kayser M., Sitek A., Branicki W. Investigating the impact of age-depended hair colour darkening during childhood on DNA-based hair colour prediction with the HIrisPlex system. Forensic SciInt Genet. 2018 Sep; 36: 26-33. doi: 10.1016/j.fsigen.2018.06.007. Epub 2018 Jun 6. PMID: 29913343.

[10] Liu F., Visser M., Duffy D. L., Hysi P. G., Jacobs L. C., Lao O., Zhong K., Walsh S., Chaitanya L., Wollstein A., Zhu G., Montgomery G. W., Henders A. K., Mangino M., Glass D., Bataille V., Sturm R. A., Rivadeneira F., Hofman A., van IJcken W. F., Uitterlinden A. G., Palstra R. J., Spector T. D., Martin N. G., Nijsten T. E., Kayser M. Genetics of skin color variation in Europeans: genome-wide association studies with functional follow-up. Hum Genet. 2015 Aug; 134 (8): 823-35. doi: 10.1007/s00439-015-1559-0. Epub 2015 May 12. PMID: 25963972; PMCID: PMC4495261.

[11] Balanovska E., Lukianova E., Kagazezheva J., Maurer A., Leybova N., Agdzhoyan A., Gorin I., Petrushenko V., Zhabagin M., Pylev V., Kostryukova E., Balanovsky O. Optimizing the genetic prediction of the eye and hair color for North Eurasian populations. BMC Genomics. 2020 Sep 10; 21 (Suppl 7): 527. doi: 10.1186/s12864-020-06923-1. PMID: 32912208; PMCID: PMC7488246.

Жаксылыков А. Ж.,
начальник отдела кадровой политики,
магистр юридических наук, майор полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова);
Молдыбаева Р. Б.,
старший преподаватель кафедры уголовного права,
уголовного процесса и криминалистики,
магистр юридических наук, майор полиции
(Актюбинский юридический институт
МВД Республики Казахстан им. М. Букенбаева)

Современные возможности внедрения в Республике Казахстан практики идентификации лица по видеозаписи по динамическим признакам внешности

Для повышения качества жизни населения и конкурентоспособности экономики Казахстана посредством прогрессивного развития цифровой экосистемы с 2017 г. действует Государственная программа «Цифровой Казахстан»[1].

В рамках цифровизации деятельности полиции предусмотрено создание Единой информационно-аналитической системы и модернизация Ситуационного центра МВД, интеграция различных каналов приема и обращений граждан, покрытие системой видеонаблюдения областных центров, городов и столицы, реализация проекта «Цифровой полицейский», создание комплексной системы безопасности учреждений уголовно-исполнительной системы.

Для обеспечения эффективности расследования и оперативности реагирования на инциденты все чаще применяются возможности искусственного интеллекта.

За последнее время в оперативно-криминалистических подразделениях органов внутренних дел значительное развитие получила криминалистическая идентификация человека по видеоизображениям. С развитием видеотехники в качестве объектов портретного криминалистического исследования все чаще стали выступать видеоизображения, полученные с уличных камер видеонаблюдения, камер видеонаблюдения из банкоматов, магазинов, подъездов жилых домов, аэропортов, вокзалов и т. д. Такие видеоизображения могут использоваться при раскрытии и расследования преступлений, а также при их предупреждении и профилактике[2, 27].

На первоначальном этапе расследования преступлений (особенно совершенных в условиях неочевидности) одной из наиболее сложных задач является установление личности преступника. Данные о признаках внешности лиц, совершивших преступление, полученные от потерпевших и свидетелей, как правило, малоинформативны, так как позволяют установить лишь групповую принадлежность и не содержат индивидуализирующую информацию. Традиционные криминалистические методики не

дают необходимой информации, позволяющей в кратчайшие сроки установить его личность и организовать розыск неизвестного преступника.

Значительное влияние на разработку способов фиксации признаков внешности человека было оказано работами выдающегося французского криминалиста Альфонса Бертильона[3]. Именно антропометрическая система идентификации личности и метод «словесного портрета», разработанные А. Бертильоном в 80 – 90-х годах XIX в., позволили создать основу для полноценного описания элементов и признаков внешности человека, в том числе и тех, которые проявляются в динамике, т. е. динамических признаков внешности.

Под динамическим признакам внешности человека понимается особенности походки, жестикуляции, мимики лица, артикуляция речевого аппарата, то есть те или иные признаки внешности, которые обладают свойством проявляться в двигательной активности человека, сопровождающей его жизнедеятельность, и быть доступными для визуального наблюдения или фиксирования с помощью технических средств[4, 28 – 30].

Процесс установления причастности того или иного человека к совершению преступления заключается в идентификационном исследовании его внешнего облика, отобразившегося на видеозаписи, в связи с чем возникает необходимость в получении сравнительных образцов тех или иных отображений внешности человека для проведения портретного исследования.

Специалисты в области производства портретных исследований сталкиваются с определенными проблемами. А. М. Зинин отмечает, что лицо человека на видеоматериалах редко отображается крупным планом, занимает незначительную часть кадра и зафиксировано в ракурсах, затрудняющих изучение признаков элементов лица[5, 19], а в некоторых случаях на видеоизображениях запечатлеваются только силуэты фигур, что в принципе исключает возможность проведения портретного исследования или приводит к вероятным выводам, так как применение традиционных методик исследования фотоизображений оказывается малопригодным для исследования видеоизображений.

При решении вопроса о достаточном количестве видеоизображений с отображением походки конкретного человека в качестве сравнительного материала необходимо обращать внимание на то, что особенности походки лучше всего проявляются спустя некоторое время после начала движения, т. е. когда человек пройдет несколько шагов. Для того, чтобы преодолеть состояние «скованности», особенно перед объективом видеокамеры, лицу, чьи образцы походки отбирают, необходимо создать благоприятные условия, при которых он не будет чувствовать напряжения, состояния психологического давления. Например, человеку, у которого отбираются образцы, предлагается свобода действий при передвижении, но, в то же время, следователю необходимо создавать ситуации, чтобы проявлялись те особенности походки, которые были отображены на исследуемой видеозаписи. Достаточное количество образцов походки для дальнейшего исследования определяется специалистом, которому будет поручено производство портретного исследования. Различные элементы походки и их отличительные признаки могут быть исследованы по тем отображениям, которые получаются как с фронтальной точки съемки относительно направления движения человека (например, угол разворота стопы и ширина шага), так и с боковой (например, длина, частота шага, время переноса ноги[6, 43] и др.).

Для исследования динамических признаков внешности человека по видеоизображениям должны применяться в комплексе с математическими методами также методы таких наук как: антропология, медицина, биомеханика, психофизиология и др. Анализ и исследование таких материалов не могут быть проведены без использования специальных знаний в области компьютерных и информационно-коммуникационных технологий.

Изучение научных статейроссийских ученых Булгакова В. Г., Сафонова А. А.,Барковской Е. Г., Зинина А. М. и др. показывает, что данный метод широко исследуется в Российской Федерации с 2010 г., тогда как в Республике Казахстан изучение вышеуказанного метода только набирает обороты. Так, 2020 г. на базе Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова прошел международный круглый стол на тему: «Современные возможности методов распознания человека по анатомическим и функциональным признакам внешности с использованием информационных систем», модераторами которого были сотрудники центрального аппарата МВД. В ходе его работы затрагивались такие вопросы, как современные возможности использования камер видеонаблюдения при идентификации внешнего облика человека, использование биометрических методов в криминалистической регистрации при идентификации личности человека по внешним элементам и признакам, а также методика проведения криминалистических портретных исследований.

Особенно остро ощущается неразработанность как в науке, так и на практике при расследовании преступлений в Республике Казахстан криминалистического метода идентификации лица по видеозаписи по динамическим признакам внешности. Однако при расследованиях преступлений террористического характера актуализировалось использование технологий профайлинга в целях выявления потенциально опасных граждан и предотвращения террористических угроз, где рассматриваются личностные и психологические параметры преступников, способных к совершению терактов[7].

Таким образом, мы приходим к выводу, что в Республике Казахстан идентификация лица по динамическим признакам внешности человека не нашла достаточного освещения в криминалистической литературе, в частности, отсутствует нормативно-правовая база в области отождествления личности по признакам внешнего облика, запечатленного на видеокадрах, отсутствует методика производства портретного исследования по видеоизображениям. Все эти обстоятельства в своей совокупности, на наш взгляд, не позволяют полноценно и объективно осуществлять криминалистическую идентификацию человека по динамическим признакам лица, отобразившимся на видеозаписи.

---

[1] Постановление Правительства Республики Казахстан «Об утверждении Государственной программы «Цифровой Казахстан» от 12 декабря 2017 г. № 827. [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P1700000827 (дата обращения: 03.11.2021).

[2] Ильин Н. Н. Криминалистическая идентификация человека по видеоизображениям: Дис. … канд. юрид. наук: — М., 2016.

[3] Ильин Н. Н. Комплексный подход при решении проблемы криминалистической идентификации человека по видеоизображениям // Вестн. Московск. ун-та МВД России. 2012. № 2.

[4] Крылов И. Ф. Очерки истории криминалистической экспертизы. — Л., 1975.

[5] Сафонов А. А. Криминалистическое исследование динамических признаков человека: история и современное состояние // Общество и право — 2010. — № 3 (30).

[6] Белкова Г. Г. Некоторые проблемы криминалистической экспертизы видеоизображения // Новый юридический вестник. — 2017. — № 2 (2). — С. 57 – 60.

[7] Юрицин А. Е., Куянова А. В., Зверев В. О., Половников О. Г. Психологическое портретирование и технология профайлинга в деятельности полиции как средство противодействия террористическим актам на транспорте // Психопедагогика в правоохранительных органах. — 2015. — № 3 (62).

Жакудаев Д. А.,
старший преподаватель кафедры криминалистики,
магистр юриспруденции, подполковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

К ВОПРОСУ О СУЩНОСТИ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ

Интенсивные экономические и социальные преобразования в стране обусловили появление новых способов совершения уголовных правонарушений в отношении граждан. Учитывая, что жизнь и общественные отношения протекают гораздо динамичнее, чем сопутствующая им ответная реакция законодателя, в последние годы ежегодно наблюдался стабильный прирост регистрации уголовных правонарушений, совершаемых с использованием сетей телекоммуникаций. Данное обстоятельство послужило пусть и не основной, но все-таки причиной введения в Уголовный кодекс Республики Казахстан новой к тому времени главы 7 «Уголовные правонарушения в сфере информатизации и связи», которая по истечении времени претерпела изменения в части использования некоторых словосочетаний. Вместе с тем, рост преступлений, наблюдаемый в сфере высоких технологий, явился и причиной возникновения потребности в новой услуге, которая была бы нацелена на выявление, предупреждение и предотвращение мошеннических действий.

Принимая во внимание, что форензика как наука о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих так называемую форму цифровых доказательств, представляет собой явление достаточно новое, в т. ч. в области экспертных учреждений, опыт и инструментарий которых, можно однозначно утверждать, пока не велик. Вместе с тем требования законодательства определенным образом заострены под особенности применяемых технологий по выявлению и фиксации следов уголовных правонарушений в киберпространстве. Форензика зародившись, оказалась почти не связанной с традиционными разделами криминалистики, ну разве что, по мнению некоторых авторов, прослеживается определенная

связь с технико-криминалистическим исследованием документов, а по мнению других авторов, является той же криминалистикой, обозреваемой только с другого ракурса.

В настоящее время структура форензики обусловлена наличием ряда узких знаний обладаемых специалистами в данной области. Это послужило появлению взаимозависящих, и в тоже время независимых друг от друга направлений: компьютерная криминалистика и сетевая криминалистика. Первая специализируется на исследовании информационного содержимого компьютеров, второе на исследованиях различного рода программ вредоносного характера.

Вопрос о сущности компьютерной криминалистики показал, что обзор отечественной, Российской и зарубежной литературы свидетельствует об отсутствии единого подхода в понимании сущности явления. Предметом описываемой науки является криминальная практика, способы, инструменты совершения киберпреступлений, оперативно-следственная и судебная практика, методы экспертного исследования цифровой информации, достижения науки в области сетей телекоммуникации.

Борьба с уголовными правонарушениями в сфере высоких технологий невозможна без анализа причин и условий, способствующих проявлению компьютерных и сетевых преступлений. Исходя из передовых достижений техники и технологии, можно с ответственностью заявить, что на развитие описываемых преступлений влияет ряд факторов: непрерывный технический прогресс, подпитываемый фактором качественного преобразования человека в целом дает возможность использовать все новые способы совершения прежних преступлений на примере мошенничества; новые общественные отношения, порождаемые информационными технологиями, окутавшими нас повсеместно, становятся предметом преступных посягательств на примере доменных имен; просматриваемые на научном горизонте новые субъекты общественных отношений в сфере таких информационных технологий, как искусственный интеллект способны порождать новые объекты авторского права, которые в недалеком будущем вызовут новые правоотношения и, соответственно новые преступления. Однако в реалиях нынешнего времени у форензики достаточно и настоящих проблем, несущих определенную угрозу обществу, а также возможно и аппарату управления. Заметна отчетливая тенденция возрастания доли информации, поступающей к потребителю через всевозможные сети, превращает интернет-пространство и вовлеченное в ее орбиту пространство в некое поле для «войн», которые могут быть частью войны обыкновенной без развязывания каких-либо действий. Постепенно наше общество, существовавшее в «аналоговом» времени, перешло в так называемый цифровой мир со всеми его позитивными и негативными обстоятельствами. Тем самым диктуя новый вектор отношений в борьбе с киберпреступностью. Шаги по противодействию возможным угрозам в зависимости обстоятельств выглядят в виде решения определенных задач, перечень которых нельзя назвать исчерпывающим: максимальное затруднение механизмов по обналичиванию, а также вводу денежных средств, с использованием электронных кошельков, регистрация всех сетей телекоммуникаций на территории страны, где они имеют место быть, подбор и расстановка специалистов требуемого формата на службу в правоохранительные органы.

В развитых странах форензика как прикладная наука существует полноценно: издан ряд научных трудов, имеются кафедры и учебные курсы, практические работники при раскрытии компьютерных преступлений обязаны следовать официальным рекомендациям, написанным соответствующими специалистами[1]. Нужно признать, что мы относимся к числу тех стран, где форензика находится в определенно зародышевом состоянии. В то же время, качественные характеристики отечественных компьютерных специалистов находятся на передовом уровне, не уступая соседним странам. Особенности нынешней системы высшего образования, в частности ее исследовательский уклон в подготовке кадров, привели к тому, что выпускаемые специалисты в описываемой области способны быстро осваивать новые знания, характеризуются критичностью мышления, а это то, что требуется для успешного совершения компьютерных преступлений и их раскрытия.

Вопросы привлечения на службу в правоохранительные органы специалистов весьма затруднительны. Во-первых, всем известная оплата труда, находящаяся на грани «ниже средней заработной платы» по сравнению с IT компаниями. Во-вторых, в какой-то мере естественная текучесть научных кругов и быстрая смена поколений в научной и ведомственной иерархии. Все это не позволяет новым специалистам влиться в криминалистическую науку, а уже существующие работники почти не в состоянии переквалифицироваться. Например, «некоторое время назад знакомый уволился из органов внутренних дел, где он служил оперуполномоченным в управлении «К». Он давно уже жаловался на службу, при этом основная претензия состояла в том, что все сотрудники управления, кроме него, раз-

бирались в компьютерной информации крайне слабо. В результате этот знакомый всю работу отдела исполнял сам и в награду выслушивал некомпетентные упреки руководства. Понятно, что рассчитывать на повышение единственному грамотному специалисту не стоило — не выслужил положенного срока. Прислали нового начальника. Это был старый и опытный кадр. Хорошо зарекомендовавший себя на предшествующей должности — командира батальона. Учитывая, что до пенсии ему оставалось еще долго, знакомый с сожалением покинул службу, после чего в этом «К» не осталось вообще ни одного сотрудника, знающего, что такое IP-адрес».

Изучение имеющихся трудов в данной области показало, что значимые книги по компьютерной криминалистике издавались только в США. В соседней стране на русском языке вышло несколько мелких работ[2; 3; 4], что весьма затруднительно говорить о литературе в нашей стране на государственном языке, которой и вовсе нет.

Одним из показателей развития форензики является всевозможные научные изыскания в данной области, а также серийный выпуск техники и программного обеспечения, специально предназначенных для сбора доказательств, для обеспечения целостности данных при обнаружении, изъятии и последующем исследовании. Однако специализированных магазинов по реализации подобной техники у нас, к сожалению, нет, так же, как не производится и закуп подобного оборудования.

Но как нам видится ситуация с IT в нашей стране и мире в целом, сейчас активно ведется работа в направлении деанонимизации интернета, и в сочетании с уже имеющейся законодательной базой возможно, в скором времени онадаст свои результаты.

---

[1] Good Practice Guide for computer based Electronic Evidence, (версия 3.0). AssociationofChiefPoliceOfficers (ACPO). Великобритания, 2006.

[2] Вехов В. Б., Илюшин Д. А., Попова В. В. Тактические особенности расследования преступлений в сфере компьютерной информации: Науч.-практ. пос. 2-е изд. — М., 2004.

[3] Завидов Б. Д. Обычное мошенничество и мошенничество в сфере высоких технологий. — М., 2002.

[4] Мещеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. — Воронеж, 2001.

Жакулин А. Б.,
начальник кафедры криминалистики,
кандидат юридических наук, доцент, полковник полиции;
Еленюк А. Г.,
заместитель начальника кафедры криминалистики,
кандидат юридических наук, полковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Инновационные направления развития криминалистической техники в современных условиях

Современные реалии XXI в. ознаменовались тем, что мировое сообщество столкнулось с одной из самых опасных угроз последнего времени — эпидемией коронавируса COVID – 19. В марте 2020 г. Всемирная организация здравоохранения объявила пандемию из-за вспышки коронавирусной инфекции, назвав распространение коронавируса «глобальной чрезвычайной ситуацией»[1]. В результате эпидемия коронавируса COVID – 19 и ее последствия значительно повлияли на мировую экономику, сознание и поведение людей, что, в свою очередь, изменило преступную и правоохранительную деятельность и обусловило появление новых задач и функций криминалистики в современных условиях. В условиях пандемии современная преступность несколько изменилась, она приобрела новые черты, тенденции и характеристики. Практика показывает, что в таких условиях уличная преступность значительно снизилась, в то время как резко возросло количество преступлений, связанных с использованием интернет-технологий. Мошенничество, характеризующееся преступной специализацией и четким разделением функций, а зачастую и международным уровнем связей, получило широкое распространение. Такие негативные тенденции в динамике и структуре преступности поставили перед криминалистикой новые задачи, которые связаны с заказом от практики на поиск адекватных средств, приемов и методов борьбы с современными вызовами преступности.

Традиционно в криминалистике выделяют три направления разработки и внедрения инноваций — технико-криминалистическое, тактико-криминалистическое и обеспечение методик расследования отдельных видов преступлений. На наш взгляд, технико-криминалистическое направление получило наиболее активное развитие в плане инноваций, но на данном направлении существует много дискуссионных и нерешенных вопросов.

Изучение и анализ криминалистических источников и эмпирики позволило выявить ряд проблем, связанных с использованием технико-криминалистических средств практическими работниками. В большинстве случаев данные проблемы являются следствием недостаточного криминалистического обеспечения такой деятельности, а также с низким уровнем подготовки соответствующих специалистов — отсутствие необходимых знаний, навыков и практических умений для работы с новейшими научно-техническими средствами, методами, инновационными технологиями в выявлении, расследовании и предотвращении современных противоправных деяний. В этой связи необходимо повысить роль прикладной функции криминалистики, создать соответствующее научно-методическое обеспечение использования средств и методов криминалистической техники, организовать их внедрение в практическую деятельность.

Сегодня криминалистическая техника, гармонично сочетающая достижения естественных, технических, гуманитарных наук, рассматривается большинством ученых-криминалистов (Т. В. Аверьянова, Р. С. Белкин, К. Е. Демин Е. П. Ищенко и др.) как раздел криминалистики, представляющий собой систему научных положений и разрабатываемых на их основе технических средств, приемов и методик, предназначенных для собирания, исследования и использования доказательств и иных мер раскрытия и предупреждения преступлений[2]. Возникновение криминалистической техники как системы криминалистических знаний и разнообразных практических мероприятий связано с внедрением достижений естественных и технических наук в практику борьбы с преступностью[3]. Наряду с этим разрабатывались и собственные криминалистические приемы и средства.

В современных реалиях в области криминалистической техники наблюдается тенденция активного поиска, разработки и внедрения инновационных криминалистических средств и методов, направленных на оптимизацию расследования преступлений. К таким инновационным продуктам относятся новые разработанные или адаптированные к потребностям следственной практики криминалистические средства, современные информационные технологии, электронные базы знаний, методы регистрации, анализа и оценки доказательств и другие. Примерами инноваций в правоохранительной деятельности являются идентификационные биометрические системы, основанные на статических и динамических характеристиках человека (электронные системы идентификации человека на основе биометрических характеристик: отпечатков пальцев, внешнего вида, внешнего вида радужной оболочки глаза, ДНК, походки, почерка и т. д.); автоматизированные рабочие места (например, АРМ «Криминалист» в «Электронном уголовном деле»), автоматизированные информационно-поисковые системы и базы данных (АДИС Папилон, АИПС Образ 3.0 и т. п.) и др.

Среди инновационных методов и инструментов важное значение придается биометрии— системам, позволяющим измерять физические и поведенческие характеристики человека с целью его идентификации или решения диагностических задач, в частности: идентификация человека по его внешним признакам с помощью видеосистем, с использованием тепловизионного оборудования, по голосу, по артикуляции при произношении отдельных звуков, слов. Возможности полиграфа также недостаточно используются при определении пригодности к следственной и разыскной деятельности и наличии профессиональной деформации; при диагностике достоверности доказательств; при выявлении причастности к преступлению и т. д. С 1985 г. в практику борьбы с преступностью внедряется геномный метод идентификации человека по его ДНК, который является одним из наиболее значительных достижений криминалистики XX в. и может полностью заменить дактилоскопию в будущей криминалистической регистрации и идентификации личности. Разработка инновационных методов и технологий, расширяющих возможности идентификации человека при генотипической экспертизе, представляют научный и практический интерес, позволяя установить личность субъекта по крошечному следу ДНК с вероятностью 99,6 %, например, при обнаружении на месте происшествия, скажем, скомканной салфетки или окурка с небольшим количеством слюны, что раньше было невозможно[4].

В области криминалистической техники продолжается поиск новых биометрических методов для использования в следственной и судебной деятельности, в частности, идентификации человека по рисунку дна или радужной оболочки глаза. Так, согласно исследованиям и данным американских

ученых, отпечатки пальцев человека обладают 40, а радужная оболочка 256 уникальными характеристиками. Именно поэтому сканирование сетчатки человеческого глаза довольно активно используется системой банковской безопасности для идентификации человека[5]. Для решения проблемы идентификации используется метод сканирования так называемой венозной карты, то есть инфракрасного считывания изображения вен руки. Широкое использование иных компьютерных технологий привело ко все большему их использованию для обнаружения преступников. В результате использования инновационных биометрических технологий удалось идентифицировать человека по его «почерку»[6].

Криминалистическая техника сегодня развивается в направлении внедрения инновационных информационных, цифровых и телекоммуникационных технологий. Это развитие также связано с совершенствованием и созданием криминалистических средств для исследования звука, электронных следов, ДНК человека; адаптацией новейшей техники для технико-криминалистического обеспечения тактики следственных и негласных следственных (розыскных) действий.

В этом контексте актуальными в области криминалистической техники будут поиск и исследование идеальных следов в человеческой памяти. На наш взгляд, заявления ученых и практиков о том, что исследования в области использования технических средств, таких как полиграф, для диагностики информационного состояния личности вполне актуально и целесообразно[7].

В последнее время, наряду с традиционными средствами обнаружения, фиксации, поиска, а также изучения материальных следов и обстановки в целом, инновационным и очень перспективным направлением является активное использование современных трехмерных цифровых технологий и искусственного интеллекта, целью которого является создание визуализации и реконструкции обстоятельств и картин преступления или его отдельных эпизодов (деталей) с использованием 3D-моделей. Практика показывает, что сотрудники правоохранительных органов все чаще сталкиваются с необходимостью изучения и учета материальных объектов, расположенных на больших территориях — последствий криминальных взрывов, пожаров, аварий и катастроф на различных видах транспорта, техногенных катастроф. Для реконструкции места происшествия все большее распространение получает метод лазерного сканирования определенных объектов и их воспроизведения в виде систем 3D-визуализации, что позволяет запечатлеть и реконструировать место происшествия и его отдельные объекты в трехмерном пространстве. Это позволяет исследовать и использовать важную криминалистически значимую информацию в ходе расследования уголовных правонарушений и впоследствии в ходе судебного разбирательства по уголовному делу. Использование лазерного сканирования местности и объектов, в результате которого создается 3D-модель, позволяет в несколько раз повысить информативность данных, собираемых на месте происшествия, обеспечивает четкую и удобную визуализацию в трех измерениях, что позволяет достичь высокого иллюстративного качества[8].

Среди перспективных направлений, имеющих важное криминалистическое значение при расследовании преступлений, можно выделить использование технологии «Больших данных». BigData — обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами[9]. На практике этот метод используется при проведении следственных и негласных следственных (розыскных) действий. В то же время технологии сетевого анализа, тактического профилирования, анализа шаблонов позволяют успешно выявлять и расследовать преступления[10].

Перспективными направлениями применения инновационных технологий в борьбе с распространением коронавирусной инфекции COVID – 19 являются следующие: 1) использование беспилотных летательных аппаратов и транспортных средств; 2) применение систем наблюдения и видеонаблюдения; 3) использование электронного контроля за перемещением людей в пространстве; 4) разработка и применение систем идентификации для распознавания лиц; 5) использование технологий «Больших данных»; 6) внедрение различных приложений, сервисов и платформ, используемых в борьбе с распространением коронавируса; 7) использование системы обнаружения людей с повышенной температурой, которая может быть установлена у входа в здание; 8) использование автоматизированных систем для выявления потенциальных пациентов и предотвращения распространения коронавируса и т. д. Таким образом, перспективы развития данной отрасли связаны с созданием инновационных технологий с учетом зарубежного опыта (Китай, Южная Корея, США и т. п.). Работа по использованию искусственного интеллекта для обеспечения решения практических задач в борьбе с преступностью, в том числе борьбы с распространением эпидемии коронавируса, должна быть значительно активизирована.

На наш взгляд, перспективным направлением в криминалистике является использование инновационных средств и технологий криминалистической техники в различных сферах правоохранительной деятельности, расширение применения криминалистических знаний в различных видах юридической практики, что в современных реалиях является достаточно актуальным и требует дальнейших исследований. На наш взгляд, это свидетельствует о проявлении еще одной важной тенденции в развитии современной криминалистики ─ расширении применения криминалистических знаний из сферы борьбы с преступностью в правоохранительную и иную деятельность.

Целью использования криминалистической техники является выявление и изучение отражений (следов) преступного события и извлечение из них доказательств. Поэтому успешное и умелое использование инновационных средств криминалистической техники обеспечивает полноту, точность, оперативность, объективность и результативность расследования, способствует оптимизации этих мероприятий и решению основных задач уголовного судопроизводства. Как показывает практика, перспективным направлением исследований в современной криминалистике является изучение нетрадиционных отраслей криминалистической техники (криминалистическая одорология, фоноскопия, полиграфология и др.). В значительной степени они определяют инновационные направления современных криминалистических исследований в области криминалистической техники. Особое значение имеют возможности использования криминалистической техники в современных глобальных угрозах и ситуации эпидемиологического кризиса, связанного с пандемией коронавируса.

---

[1] Глобальные чрезвычайные ситуации в области здравоохранения. [Электронный ресурс]. — Режим доступа: https://www.who.int/ru/emergencies/overview (дата обращения: 15.10.2021).

[2] Криминалистическая техника: Учебн. для вузов / К. Е. Демин [и др.]; отв. ред. К. Е. Демин. — М., 2020.

[3] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика: Учебн. для вузов. / Под ред. Заслуженного деятеля науки Российской Федерации профессора Р. С. Белкина. — М., 2000.

[4] Жижина М. В. Инновационное развитие криминалистики на современном этапе // LEX RUSSICA. — 2012. — № 1. — С. 117 – 125.

[5] 14 октября — Всемирный день зрения. [Электронный ресурс]. — Режим доступа: http://cgie.62.rospotrebnadzor.ru/info/zdorovii-obraz-jizni/146846/ (дата обращения: 15.10.2021).

[6] Михайлов М. А. Биометрия: новое слово в идентификации личности // Воронежские криминалистические чтения: Сб. науч. тр. 2009. № 11. С. 267 – 279.

[7] Сагынбекова Г. Полиграф как источник доказательств. [Электронный ресурс]. — Режим доступа: https://www.zakon.kz/221763-poligraf-kak-istochnik-dokazatelstv-g..html (дата обращения: 15.10.2021).

[8] 3D-сканирование и фотографирование сравнили на практике как методы криминалистической экспертизы. [Электронный ресурс]. — Режим доступа: https://www.artec3d.com/ru/cases/ 3d-scanning-tested-against-photography-in-autopsy (дата обращения: 16.10.2021).

[9] URL: https://ru.wikipedia.org/wiki/Большие_данные (дата обращения: 16.10.2021).

[10] Саморока В. А., Прохоров К. О. Перспективы использования «BIG DATA» в раскрытии и расследовании преступлений // Академическая мысль. — 2019. — № 3 (8). — С. 74 – 78.

Жижимов В. В.,
доцент;
Таукебаев А. Е.,
старший преподаватель
(Академия КНБ Республики Казахстан, г. Алматы)

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИЧЕСКИХ ИССЛЕДОВАНИЙ КОМПЬЮТЕРНЫХ СРЕДСТВ И СИСТЕМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Современные компьютерные и информационно-коммуникационные технологии находят применение во всех сферах деятельности общества. Высокие темпы цифровизации как процесса внедрения цифровых технологий в разные сферы деятельности свидетельствуют о поступательном движении общества к развитию и самосовершенствованию.

Цифровизация отраслей экономики, деятельности государственных органов, развитие цифровой инфраструктуры, повышение цифровой грамотности населения, а также обеспечение информационной безопасности являются актуальными задачами построения цифрового Казахстана[1].

Развитиецифровых технологий дает возможность предоставлять услуги более высокого качества, с другой стороны оно породило новые виды компьютерных преступлений,изменило механизмы их совершения и сокрытия. Появились новые виды криминалистических экспертиз для расследования пре-

ступлений, совершаемых с использованием компьютерных средств и систем и, соответственно, новые термины — «электронная криминалистика», «цифровая криминалистика», «компьютерное преступление», «цифровой след».

Цифровая криминалистика (digitalforensics — альтернативное название: электронная судебная экспертиза) — термин, который не является устоявшимся и не имеет единого общепризнанного определения. В своих работах Яковлев А. Н.[2], Вехов В. Б.[3]позиционируют «электронную криминалистику» или «цифровую криминалистику» как развивающуюся науку, в сферу которой относят разработку криминалистического обеспечения расследования преступлений, совершаемых с использованием компьютерных средств и систем. Новые знания в криминалистике должны базироваться на понимании особенностей функционирования современных информационно-коммуникационных технологий и использоваться для выявления уголовно-релевантных закономерностей преступной деятельности[2]. По мнению Е. Р. Россинской, А. И. Семикаленовой, криминалистика может быть обосновывающим знанием для новых родов и видов судебных экспертиз, поэтому нет никакой необходимости менять название науки. Развитие криминалистики идет за счет изучения новых закономерностей, новых механизмов следообразования, новых технологий собирания (выявления, фиксации, изъятия), исследования, оценки и использования криминалистически значимой информации, новаций в области криминалистической тактики и методики[4].

В тоже время, внедрение новых технологий собирания, исследования и использования криминалистически значимой информации, создание методических рекомендаций для производства компьютерно-технической экспертизы зачастуюне успевает за интенсивным развитиемтехнического прогресса в области информационно-коммуникационных технологий. Кроме того, А. И. Семикаленова, Н. А. Хатунцев отмечают, что во многих случаях у следователя, отсутствуют технические знания в области цифровых технологий, необходимые при расследовании компьютерных преступлений, знания терминологии, используемой в информационно-коммуникационных технологиях, поэтому он неверно употребляет ее при формулировании вопросов. Эксперты используют терминологию, которая непонятна для суда и лиц, участвующих в деле, при этом в своих заключениях они не приводят расшифровки тех или иных понятий, используемых в исследовании[5].

Наряду с проблемой терминологической неопределенности в вопросах цифровой криминалистики, авторы хотели бы акцентировать внимание на некоторых технических проблемах при расследовании преступлений. По мере совершенствования криминалистических методов и инструментов, преступники используют новые технологии для сокрытия или удаления следов своих преступлений. Применение антикриминалистической техники, отрицательно влияющей на существование, количество или качество доказательств, рассматривается специалистами как ключевая проблема криминалистических исследований.

Среди методов антикриминалистической техники выделим следующие: шифрование информации; сокрытие данные в пространстве хранения; использование скрытых каналов передачи информации; хранение информации в «облачном хранилище данных».

Под «облачным хранилищем данных» мы будем понимать технологическую платформу, использующую интернет или выделенную распределенную информационно-коммуникационную инфраструктурудляпередачи и храненияэлектронных информационных ресурсов, предоставляемую в пользование клиентам третьей стороной. При этом количество, внутренняя структура и географическое местоположение серверов такой технологической платформы клиенту не известно. Усиливающаяся тенденция к хранению информации пользователей в облачном хранилище данныхделает процесс расследования более сложным, потому что на электронных носителях информации остается меньше цифровых следов, что можетсделать известные методы цифровой криминалистики бесполезными. В век глобальной цифровизации криминалистам необходимы методы выявления цифровых следов и в виртуальном пространстве. Однако такая потребность, вступает в противоречие с возможностью и сложностью ее технической реализации в практике расследования преступлений правоохранительными и специальными органами.

Рассмотрим пример, иллюстрирующий подобную ситуацию. При расследовании уголовного дела, возбужденного по факту убийства, сожительница подозреваемого лица постфактум предъявила в качестве алиби совместную фотографию на своем мобильном телефоне, на которой данный подозреваемый был отображен вместе с ней в предполагаемое время убийства. При этом сам фото-файл фактически хранился в облачном хранилище данных «GoogleDisk».

Вместе с тем,в ходе следствия появилисьвеские основания полагать, что версия сожительницы имеет цель скрыть преступление, следовательно, фотография в ее мобильном телефонемогла быть сфальсифицирована.Таким образом, дополнительную информациюследствию могло датькриминалистическое исследование,иперед экспертом был поставлен вопрос: «Имеется ли на представленном мобильном телефоне искомый фото-файл и возможно ли установить, когда был создан указанный фотофайл?»

При проведении криминалистического исследования экспертом было определено, чтоискомый фото-файл был удален из памяти мобильного телефона, а его копия былаобнаруженав «корзине»для удаленных файлов облачного хранилища данных «GoogleDisk». Данный фото-файл был восстановлен из «корзины» облачного хранилища, так как автоматическое удаление без возможности восстановления информации, предусмотренное политикой конфиденциальностиGoogle (по умолчанию — 60 дней),еще не выполнялось.Отметим, что возможности автоматического доступа к информации, которая размещена в облачном хранилище данных обеспечивает аппаратно-программный комплекс UFED[6].

Дата и время создания обнаруженного фото-файла соответствовалипредоставленной информации, ноустановить реальную дату и время создания фото-файла не представлялось возможным. Во-первых, теоретически — атрибуты файла можно программно модифицировать. Во-вторых, экспериментально показано, что атрибуты файла (дата и время создания — «created»)формируются по локальному времени устройства, т. е. возможно настроить на мобильном телефоне другие дату и время и сделать копию фото-файла, в итоге дата и время создания могут быть любыми. Следовательно, гарантировать достоверность времени создания существующего фото-файла только по его атрибутам нельзя.Поэтому представляется логичным проверитьпротоколирование сетевой или серверной информации при межсетевом взаимодействии устройств. Однако в случае использования облачного хранилища данных получить такую детальную экспертную информацию от третьей стороны (Google) почтиневозможно.

Таким образом, можно констатировать, что в настоящее время не теряют своей актуальности вопросы совершенствования не только технического и методического обеспечения компьютерно-технической экспертизы, но и регулирования правовых процедур взаимодействия государства в лице правоохранительных и специальных государственных органов с владельцами сетевых интернет-сервисов, облачных хранилищ данных.

Считаем, что законодательное регулирование интернет-услуг, предоставляемых глобальными интернет-платформами в Республике Казахстан, включая облачные хранилища данных, было бы первым шагом на пути решения проблемы применения методов антикриминалистической техники. Комплексный подход по решению обозначенных в данной публикации проблембудет способствовать повышению качества криминалистических исследований компьютерных средств и систем в условиях цифровизации.

---

[1] Постановление Правительства Республики Казахстан «Об утверждении Государственной программы «Цифровой Казахстан» от 12 декабря 2017 г. № 827. [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P1700000827 (дата обращения: 03.11.2021).

[2] Яковлев А. Н. Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе. // Совершенствование следственной деятельности в условиях информатизации: Мат-лымеждународ. науч.-практ. конф. — Минск, 2018.

[3] Вехов В. Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: Мат-лымеждународ. науч.-практ. конф. — Ростов-н/Д, 2017. С. 40 – 46.

[4] Россинская Е. Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности» // Вестн. Санкт-Петербургск. ун-та. 2020. С. 745 – 759.

[5] Судебная экспертиза: типичные ошибки / Под ред. Е. Р. Россинской. — М., 2015. С. 469 – 492.

[6] Мухин И. Г. Современные технико-криминалистические средства исследования информации, размещенной в облачных хранилищах // Проблемы современной криминалистики и судебной экспертизы: Тезисы докл. респ. науч.-практ. конф. — Минск, 2016. С. 46 – 48.

Захарова Л. Ю.,
старший преподаватель
кафедры исследованиядокументов
учебно-научного комплекса судебной экспертизы,
подполковник полиции
(Московский университет МВД России им. В. Я. Кикотя)

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ БИОМЕТРИИ В ИДЕНТИФИКАЦИИ ЧЕЛОВЕКА ПО ПРИЗНАКАМ ВНЕШНОСТИ

Технические устройства все активнее внедряются в повседневную человеческую деятельность. Уже становится сложно представить привычный ритм жизни человека без участия в нем автоматизированных систем. Технический прогресс распространился повсеместно, в том числе внедрился и в экспертную деятельность. Говоря о портретной экспертизе, перспективным направлением развития в рамках данного рода экспертизы можно считать биометрию.

Сама биометрия представляет собой распознавание человека по определенному набору черт, причем механизм распознавания основывается на статистическом анализе. Геометрические формы и размерные характеристики лица человека в целом и отдельных его частей, форма ладоней, ступней, ушей, папиллярные узоры, колебания голосовых связок и другие признаки в своей совокупности делают его обладателя уникальным, что позволяет идентифицировать его, то есть выделить именно его из числа похожих. Также важно учитывать тот факт, что данные характеристики являются неизменными для человека на протяжении всей их жизни.

Биометрия как система, основанная на математических принципах, позволяет достоверно оценить взаимосвязи и взаимозависимости рассмотренных выше характеристик, а также получить численное выражение и определить надежность проведенного экспертного исследования. Такая математизация процесса позволяет обнаруживать закономерности, которые могут быть не такими очевидными при производстве исследования с применением традиционных методов и методик. Однако полностью доверить осуществление идентификации компьютеру нельзя. Окончательное формулирование выводов может производиться только экспертом, поскольку только он может дать реальную оценку достоверности выявленных совпадений и различий.

На данный момент существуют отдельные области непосредственного применения биометрии. К таковым можно отнести технологии сканирования отпечатка пальца TouchIDили распознавания лицаFaceID, применяемые в смартфонах и иных технических средствах для получения доступа к пользованию устройством. Также аналогичные технологии применяются в некоторых банковских системах, что позволяет пользователям удаленно получать доступ к своим банковским картам или личным счетам.

Говоря об использовании биометрии для распознания людей, например, в городах, следует сказать, что данная система находится на стадии внедрения и апробации. Однако на сегодняшний день имеется ряд трудностей, касающихся правового регулирования возможностей применения биометрии. Это обусловлено тем, что не всегда возможно для законодателя «успевать» за регулярно появляющимися новинками в данной сфере, поэтому необходимо в меру расширить перечень устройств, допустимых для производства съемки, а также создать единую базу данных биометрических данных с законодательным закреплением.

Теперь более подробно остановимся на тех методах биометрии, которые могут рассматриваться в рамках портретной экспертизы.

В первую очередь, это распознавание человека по признакам на его лице. Данный метод является наиболее надежным и эффективным. Автоматизированная система идентификации человека по лицу строится на методике антропологической реконструкции, т. е. на оцифрованном изображении лица человека автоматически выбираются параметры (к ним относятся: волосяной покров головы, лоб, брови, глаза, веки, щеки, нос и другие, которые в свою очередь имеют различные проявления, а именно: форму, размер, цвет, положение, симметрия/асимметрия, наличие/отсутствие), которые в своей совокупности будут составлять уникальный набор характеристик данных параметров. Следовательно, каждое лицо может быть описано уникальным набором значения параметров.

Использование данной системы уже несколько раз доказывало свою эффективность. Известны случаи, когда камеры, подключенные к системе идентификации лиц, позволяли найти лицо, совершившее преступление в одном городе и скрывшееся в другом. Также известен случай, когда благодаря камерам удалось установить личность преступника в момент, когда им совершалось преступление. Таким образом, несмотря на сравнительно небольшой период времени, в течение которого используется система фиксации биометрической информации, уже имеются положительные примеры, когда эксплуатация системы способствовала изобличению преступников. Что также доказывает перспективность развития данного направления.

Одним из разработчиков алгоритмов по распознаванию лиц является компания NtechLab, состоящая из группы экспертов в области искусственных нейронных сетей и машинного обучения. Одним из продуктов данной компании является программный продукт FindFaceSecurity, являющийся интеллектуальной видеоаналитикой на основе распознавания лиц, способный в режиме реального времени определять лица в потоке с последующей отправкой уведомления в случае установления совпадения со списками мониторинга. Данная программа способна взаимодействовать с неограниченным количеством камер видеонаблюдения, также рассматриваемый программный продукт быстро внедряется и имеет возможность быстрого поиска искомого лица и возможности отслеживания его перемещений[1]. Эти достоинства позволяют использовать FindFaceSecurity для обеспечения безопасности в крупных городах. Кроме того, алгоритмы NtechLab неоднократно признавались лучшими в мире по результатам независимых сторонних тестов, в числе которых IARPA и Wider.

Также существует еще одна компания, занимающаяся разработкой алгоритмов, занимающихся разработкой алгоритмов для распознавания лиц, это компания VisionLabs, на данный момент уже имеющая в числе своих клиентов ряд розничных банков, применяющих данные технологии, в том числе для противодействия мошенническим схемам. Эффективность использования программных продуктов, разрабатываемых данным предприятием, подтверждается результатами международного тестирования LabeledFacesintheWild, проводимого в США в Университете Массачусетса, по итогам оценки которого алгоритм, используемый VisionLabs, признается одним из лучших в мире. Специфика данного теста заключается в том, распознавание лиц происходит по изображениям, полученным в обычных условиях, то есть без соблюдения правил съемки[2]. Тот факт, что рассматриваемый продукт проявил себя с положительной стороны именно в условиях применения непрофессиональной съемки, могло бы позволить использовать данные алгоритмы при подключении их к системе городских видеокамер для идентификации лиц на улицах. Также в отдельных случаях может быть актуальным применение возможности данного алгоритма для подсчета количества людей на определенной территории.

Также важно отметить, что обе рассмотренные выше компании, занимающиеся разработкой алгоритмов по идентификации лиц, являются отечественным.

Помимо идентификации лица немаловажным методом биометрии является распознание внешности человека по динамическим (функциональным) признакам. В большей мере в разработке программного и технического обеспечения данного метода преуспела Китайская компания Huawei.

Таким образом, еще недавно сложно было представить, что с помощью определенных автоматизированных средств станет возможным из множества людей обнаружить одного конкретного. Однако уже сегодня человечество достигло того уровня технического развития, что это становится возможным, даже если интересующее нас лицо находится в месте большого скопления людей, съемка производилась с различных ракурсов и т. д. Также имеются российские компании, занимающиеся разработкой систем алгоритмов, позволяющих производить идентификацию по лицу, и достигшие немалых успехов в данном направлении. В том числе и на базе разрабатываемых ими технологий можно было бы в какой-то степени автоматизировать процесс идентификации человека по лицу. Системы биометрии позволяют работать с большим объемом информации различной степени информативности и достоверности. Это свидетельствует о том, что биометрия может эффективно и перспективно применяться в рамках экспертной деятельности в области портретной экспертизы. Использование данной системы позволит расширить рамки проводимых исследований, ускорит и в некоторой мере и оптимизирует процесс идентификации конкретного человека. Однако всегда надо помнить, что полностью автоматизировать процесс идентификации человека по признакам внешности нельзя, поэтому в любом случае данная система будет носить вспомогательный характер для эксперта, не заменяя его полностью.

[1] URL: www.ntechlab.ru (дата обращения: 03.11.2021).
[2] URL: https://intalent.pro/article/intervyu-s-osnovatelyami-visionlabs.html (дата обращения: 03.11.2021).

Иванов В. Ю.,
преподаватель кафедры криминалистики,
старший лейтенант полиции;
Соколова А. С.,
курсант факультета подготовки следователей,
младший сержант полиции
(Уральский юридический институт МВД России, г. Екатеринбург)

ФИШИНГ КАК РАЗНОВИДНОСТЬ КОМПЬЮТЕРНОГО МОШЕННИЧЕСТВА

2021 г. является продолжением эпохи информационных технологий. Безусловно, многие люди стали изучать компьютерные нововведения и осваивать их в лучшем виде, также следует заметить, что больший процент граждан скажет лишь о плюсах в информационном прогрессе, так как с его появлением множество функций человек может реализовать, сидя у себя дома в комфортной обстановке.

Современное время характеризует себя появлением коронавирусной инфекции — «COVID – 19» вызванной коронавирусом SARS-CoV-2 (2019-nCoV).

Ограничительные меры, вводимые большинством разных стран, стали предпосылкой еще более глубокого и качественного развития компьютерных технологий. Ведь режим самоизоляции обездвижил множество людей на планете, также, как и различные организации, предприятия. В стадии снижения возможности работать, учиться, реализовывать свои интересы оффлайн, человечество нашло более простой и наиболее верный выход из ситуации: воплощать это дистанционно, то есть с использованием компьютерных технологий. Сейчас вам кажется, что у данной идеи нет за собой никаких погрешностей и изъянов, но как говорится «медаль имеет две стороны», точно также следует и рассмотреть развитие компьютерных технологий. Бесспорно, людям стало намного проще выживать и реализовывать свои потребности, но всегда ли эта реализация воплощается с добрым умыслом? На этот вопрос разумнее ответить «нет», так как всегда найдется тот процент человечества, кто желает перейти за рамки законного воплощения своих интересов.

Более актуальной проблемой является так называемый «фишинг». Самое простое определение фишинга заключается в том, что это метод мошенничества, при котором преступники, выдавая себя за представителей доверенных учреждений, вымогают конфиденциальные данные, чаще всего — пароли для входа в сервисы электронных банковских услуг, внутренние сети компании, а также номера платежных карт и адреса электронной почты[1].

Для выполнения столь сложных действий нужно профессионально владеть не только ораторскими качествами в плане построения диалога с человеком или отправки ему вредоносных сайтов или ссылок, но и умением работать с компьютерными программами, а также знать их взаимодействие между собой для получения желаемого результата.

Также следует указать, что в период с 2020 г. человечество стало наиболее часто использовать сервисы банковских услуг, реализовывать покупки онлайн, большинство людей стало держать свои денежные средства на банковских картах, все это, как было сказано выше, произошло из-за пандемии, которая и стала наиболее важным толчком к развитию компьютерных технологий. В настоящее время, обращаясь к интернет-ресурсам для того, чтобы узнать статистику распространения фишинга, чаще всего приводят данные 2019 – 2020 гг.

В сентябре 2019 г. эксперты проекта ОНФ «За права заемщиков» назвали пять мошеннических схем, которые чаще всего применялись в 2019 г. На первом месте (34 % упоминаний) оказался фишинг, цель которого — получить доступ к логинам и паролям пользователя. Классический пример фишинга — вредоносные ссылки.

Сообщается, что всего авторы рейтинга проанализировали около 50 тыс. сообщений граждан и более 20 тыс. публикаций в СМИ и других открытых источниках.

В 2020 г. во время пандемии коронавируса количество краж с банковских карт пользователей выросло в шесть раз, сообщала компания Group-IB, которая специализируется на предотвращении кибератак. По словам экспертов, мошенники заманивают пользователей на фишинговые сайты, где поку-

патели вводят платежные данные. Злоумышленники используют эти данные для обращения к публичным p2p-сервисам банков и перевода денег на свои счета[2].

Один банк в среднем фиксирует 400 – 600 попыток такого способа мошенничества в месяц. Средний чек одного перевода — 7 тыс. рублей. Часто злоумышленники создавали поддельные страницы онлайн-магазинов с масками, перчатками и санитайзерами (данные Group-IB). Таким образом, можно заметить активность мошенников, использующих фишинг, как способ завладения чужим имуществом путем обмана граждан.

Несмотря на то, что фишинг стал популярным преступным деянием с использованием компьютерной техники, данное преступление преследует за собой соответствующее наказание в виде лишения свободы или денежного штрафа. Так, например, МВД России и ФСБ России при экспертно-аналитической помощи «Лаборатории Касперского» завершили дело о компьютерном фишинге. Братья Евгений и Дмитрий Попелыши и их соучастник Александр Сарбин были установлены и задержаны. В отношении их возбуждено уголовное дело. В результате представлениям о хакерской безнаказанности был положен конец в виде вынесения судебного приговора[3].

К сожалению, не так часто случается, что фишинговые преступники найдены и наказаны. Данный пробел связан с тем, что в правоохранительных органах недостаточно сотрудников, обладающих наиболее профессиональными навыками в компьютерных технологиях, в связи с чем доказательственной базы у следователя даже для возбуждения уголовного дела иной раз не хватает.

Несомненно, следует отметить прогресс развития преступлений с использованием компьютерных технологий, даже фишинг — раннее не популярно звучащее слово, сейчас является не нововведением и даже имеет свои виды. Приведем перечень видов фишинга, но в связи с его развитием назовем лишь наиболее часто встречаемые.

Первым является Smishing, который представляет собой фишинговую атаку с использованием обычных SMS-сообщений. Он направлен на то, чтобы получатель, получая данное SMS, перешел по указанной ссылке на вредоносный сайт. Как правило, такие SMS обычно отправляются от легитимных компаний. Проанализировав статистику Smishing, можно констатировать, что смишинговым атакам подвергаются люди, во-первых, плохо разбирающиеся в компьютерных технологиях, во-вторых, относящиеся преимущественно к старшей возрастной группе, т. е. от 35 лет и выше[4].

Вторым видом фишинга является Vishing. Его новшество заключается в том, что злоумышленники используют телефон как средство атаки, посредством использования голосового сопровождения. Чем данный вид намного эффективнееSmishing? Люди могут не отреагировать на SMS-сообщение ввиду занятости или не заметить данное сообщение. Обратная сторона выступает в вишинге, так как человеку поступает звонок из компаний(наиболее частыми являются банки) с обращениями в виде срочной их оплаты по кредиту либо с сообщением о том, что был взят кредит на их имя. Пример вишинга: в сентябре 2020 г. медицинская организация SpectrumHealthSystem сообщила о вишинг-атаке, в рамках которой пациенты получали телефонные звонки от лиц, маскирующихся под ее сотрудников. Злоумышленники намеревались извлечь персональные данные пациентов и членов SpectrumHealth, включая идентификационные номера членов и другие личные медицинские данные, связанные с их учетными записями. SpectrumHealth сообщила, что злоумышленники использовали такие меры, как лесть или даже угрозы, чтобы заставить жертв передать свои данные, деньги или доступ к их личным устройствам[5].

Несмотря на разнообразие форм фишинга, расследования данных преступлений является возможным. В данном случае, при поступлении сообщения о совершении преступления посредством компьютера, Интернета, следователю необходимо: получить объяснения с лица непосредственно пострадавшего от совершения преступления, а также лиц, присутствующих при совершении данного деяния, которые могут дать какую-либо информацию, полезную для проведения расследования. Во-вторых, следователь может истребовать выписку о движении денежных средств с банковского счета лица либо он вправе истребовать детализацию входящих и исходящих звонков лица, в отношении которого совершено преступление. В-третьих, следователь проводит следственное действие — осмотр места происшествия, если в данном случае преступление совершено посредством использования потерпевшим своего ПК. В данном случае он должен в протоколе осмотра полностью описать компьютер, его характеристики, а также посредством фото (видео) зафиксировать то сообщение, посредством которого было совершено фишинговое преступление. Вторым целесообразным действием было бы изъятие компьютера в ходе осмотра места происшествия и его детальный осмотр с привлечением

специалистов в сфере компьютерных технологий. Также следователь может отправлять запросы провайдерам о предоставлении информации об интернет-соединениях абонента или абонентского устройства, так как они имеют большое значение для расследования и позволяют установить, кто использовал соответствующий IP адрес в конкретное время. Следователь вправе провести следственное действие — судебная компьютерная экспертиза, где он получит полный объем информации о содержании компьютера. Помощь от органа дознания также будет иметь значение для расследования уголовного дела, ведь следователь может дать письменное поручение для проведения соответствующих оперативно-розыскных мероприятий, результаты которых орган дознания обязан предоставить следователю не позднее 10 суток. Таким образом, следователь при расследовании данной категории дел имеет широкий арсенал действий для получения доказательственной базы, в данном случае следователю необходимо пользоваться помощью специалистов в сфере компьютерных технологий для более полного и глубокого изучения совершенного преступного деяния.

Рассмотрев наиболее часто встречаемые виды фишинга и процесс расследования данных дел, на наш взгляд, следует указать на то, что человечеству следует быть бдительными и аккуратными при использовании компьютерных технологий, сотовых средств и т. п. Злоумышленники изучают предмет своего дохода очень глубоко и полно обхватывают функционал его действий. Людям следует оградить себя от посещений ненадежных сайтов, а также переходов на сомнительные ссылки, полученных из SMS-сообщений или же расположенных на легитимном сайте.

---

[1] Батюшкин М. В. «Фишинг» — компьютерное мошенничество? // Символ науки: международный научный журнал. — 2021. — № 1. — С. 90 – 93.

[2] Что такое фишинг и как от него защититься? [Электронный ресурс]. — Режим доступа: https://rb.ru/story/what-is-fishing/ (дата обращения: 12.10.2021).

[3] Стоянов Р. В. Компьютерный фишинг — судебный приговор // Право и кибербезопасность. — 2012. — № 1. — С. 27 – 29.

[4] Алексеев А. С. Фишинг: интернет-мошенничество с применением социальной инженерии // Вестник современных исследований. 2019. № 1.13 (28). С. 12 – 16.

[5] 11 типов фишинга и их примеры из реальной жизни. [Электронный ресурс]. — Режим доступа: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/ (дата обращения: 14.10.2021).

Ильдебаев Р. Е.,
докторант, магистр права, капитан полиции
(Академия правоохранительных органов
при Генеральной прокуратуре Республики Казахстан,
Акмолинская обл., г. Косшы)

К ПРОБЛЕМЕ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПОДДЕЛКОЙ ДОКУМЕНТОВ В СФЕРЕ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Расследование преступлений, совершаемых путем подделки образовательных документов, на первоначальном этапе характеризуется множеством специфичных черт, присущих исключительно исследуемой совокупности. В рамках данного этапа следователь, дознаватель, как правило, сталкивается с одной из следующих следственных ситуаций:

- в распоряжении следователя, дознавателя имеется образовательный документ с признаками подделки, однако отсутствует лицо, подозревающееся в совершении преступления;
- подозреваемое лицо в совершении преступлений в сфере подделки образовательных документов заявляет о своей непричастности и отказывается от дачи признательных показаний;
- подозреваемое лицо в совершении подделки образовательных документов полностью признает свою вину и дает признательные показания.

Первая из вышеперечисленных нами следственных ситуаций характеризуется дефицитом информации. Для решения проблем, связанных с установлением личности, Г. И. Поврезнюком справедливо выделяется четыре этапа: «подготовительный, аналитический, сравнительный и оценочный»[1, 23]. Поэтому в основу проведения работы, направленной на установления лиц, причастных к совершению подделки образовательных документов, должны входить и средства оперативной аналитики.

Исходя из этого, следственными версиями применительно к данной следственной ситуации является:

- поддельный образовательный документ введен в оборот под видом подлинного с целью получения прибыли;

- поддельный образовательный документ введен в оборот с целью дискредитации легально циркулирующих образовательных документов;

- поддельный образовательный документ введен в оборот с целью хищения подлинных аналогов;

- поддельный образовательный документ выступил средством совершения иных разновидностей преступлений.

Задачами расследования в указанной ситуации являются:

- установления лиц, причастных к совершению подделки образовательных документов;

- определения реальности масштаба происшествия;

- отыскание материальных следов, доказывающие причастность конкретных лиц к совершению подделки образовательных документов;

- установление круга лиц, причастных к преступлению (организаторы, подстрекатели, пособники, в том числе лица, ответственные за выдачу и хранение документов); наличие признака неоднократности; устойчивость и длительность существования преступной группы; получение вербальной и материально-отображаемой доказательственной информации, в том числе компьютерных программ, баз данных, информации в сети Интернет;

- установление причинно-следственной связи подлога с родственными составами преступлений (мошенничеством, незаконным присвоением собственности, компьютерными преступлениями, служебным подлогом, в том числе с иностранным элементом).

- поиск лиц, ставших свидетелями либо потерпевшими от действий злоумышленников.

Важным тактическим решениями в отмеченных условиях является изучения оперативной обстановки путем проведения анализа поступления сигналов от граждан в территориальные подразделения правоохранительных органов, а также осуществления мероприятий по привлечению лиц, сотрудничающих на конфиденциальной основе. Причем в основу формирования алгоритма расследования примирительной данной ситуации необходимо включить действия и мероприятия, способствующих идентификации лиц, причастных к совершению расследуемого преступления.

Среди первоначальных и неотложных следственных действий и оперативно-розыскных мероприятий в качестве наиболее эффективных следуют выделить:

- осмотр места происшествия;

- организация назначения и производства судебных экспертиз;

- проведения осмотра предмета и документов;

- начало досудебного расследования;

- проверки по специальным учетом лиц, ранее осужденных за совершения аналогичных преступлений;

- опрос граждан, должностных лиц, получения от них информации;

- проведения допросов свидетеля и потерпевших;

- проведения опознания предметов и документов;

- снятие информации с технических каналов связи, компьютерных систем и иных технических средств.

В случае установления лиц, причастных к совершению подделки образовательных документов;

- осуществления задержания;

- допрос в качестве подозреваемого;

- проведения личного обыска;

- проведения обыска по месту жительства и работы (учебы).

Во втором случае расследования преступлений, совершаемых путем подделки образовательных документов, протекает в условиях конфликтности и противодействия. В качестве общих задач противодействия Б. Б. Нургалиевым выделяются «1) сокрытие информации о событии преступлений; 2) сокрытие информации о виновности конкретного лица в совершении преступлений и его соучастниках; 3) сокрытие информации о носителях доказательственной информации; 4) создание неблагоприятных условий для деятельности правоохранительных органов в их стремлении самостоятельно добыть доказательственную базу; 5) дискредитации добытых доказательств; 6) оказание психологического, физического воздействия на свидетеля, потерпевшего … следователя»[2, 10 – 11].

В большинстве случаев представляет серьезную трудность вопрос соотношения подозреваемого лица и отдельного образовательный документ в силу количественного и качественного разнообразия последних. К примеру, если наркотическое средство, изъятое у лица, страдающего наркотической зависимостью, не предполагает особых затруднений при соотношении, то поддельный документ образовательный документ может выходить за рамки социальной или профессиональной принадлежности индивида, негативно сказывается на процессе доказывания.

Наиболее вероятные следственные версии применительно к рассматриваемой ситуации:

- подозреваемое лицо в совершении подделки образовательных документов преднамеренно пытается ввести в заблуждение орган досудебного расследования, дабы избежать наказания;

- подозреваемое лицо действительно не имеет никого отношения к совершению расследуемого преступления.

Первоначальной задачей расследования в указанной ситуации является установления следующих обстоятельств:

поиск доказательств, уличающих либо, наоборот, оправдывающих подозреваемого лицо;

проверка алиби лица, подозревающегося в совершении подделки образовательных документов;

определение возможности совершения процессуальных нарушений при задержании лица в работе со свидетелями (потерпевшими) и понятыми.

проверка достоверности показаний подозреваемого лица.

установить время и места совершения преступления;

выдвинуть и осуществить проверку следственных версий;

назначить технико-криминалистическую экспертизу документа, которая позволит установить способ совершения преступления;

выявить схему совершения преступления;

составить планы допросов ответственных лиц за выдачу и хранение документов, а также подозреваемых;

провести допросы;

провести обыски у подозреваемых, наложить арест на оборудование и иное имущество, с помощью которого, как предполагается, совершенно преступление.

Наиболее эффективным тактическим решением в указанной ситуации является применение следователем психологическим приемов воздействия на подозреваемое лицо при проведении комплекса первоначальных и неотложных действий с его участием. Уяснения реальных событий происшедшего события является для следователя важным обстоятельством, способствующим принятию важных процессуальных решений по отдельному уголовному делу. Грамотное использование психологических приемов может изменить направление расследования в целом, не применяя обвинительный уклон процессуальных процедур к необоснованно подозреваемого лицам.

В данном случае комплекс первоначальных и неотложных следственных действий и оперативно-розыскных мероприятий должен выглядеть следующим образом:

осмотр места происшествия;

организация назначения и производства судебных экспертиз;

начало досудебного расследования;

проведение задержание лица;

проверка по оперативным, криминалистическим учетом и системам уголовного регистрации;

В отличие от вышеуказанного положения вещей третий ситуация носит, как правило, бесконфликтный характер. Тем не менее, нередки случаи, когда в рамках досудебного расследования подсудимый отказывается от своих первоначальных показаний, данных ими в ходе предварительного расследования, обвиняя органы досудебного расследования в предвзятом отношении и применении недозволенных мер воздействия. «Механизм распознания вероятных реакций субъектов противодействия заключается в умении посмотреть на создавшуюся ситуацию или переданную информацию его глазами и оценить ее, исходя из информированности, эффективных переживаний и обычных реакций людей в подобных ситуация, подсказываемых им здравым смыслом»[3, 16 – 17].

Наиболее характерными следственными версиями в указанной ситуации:

- в результате совершения преступных действий, связанных с подделкой образовательных документов, подозреваемое лицо осознало свою вину и желает оказать содействие в расследовании данного преступления;

- принимая на себя вину в полном объеме, подозреваемое лицо покрывает своих соучастников, преследуя следующие цели — получение материальной помощи и протекции о неустановленных следствием членов ОПГ, получение минимального срока в результате ошибочной квалификации преступного деяния;

- подозреваемое в совершении расследуемого преступления лицо умышленно оговаривает себя в результате запугивания со стороны представителей криминальных структур либо в связи с возможностью получения материальной выгоды.

Основными задачи расследования с учетом вышеуказанных обстоятельств является;

- поиск доказательств, уличающих либо, наоборот, оправдывающих подозреваемое лицо;

- установления причастности иных лиц к совершению подделки образовательных документов;

- выявление причин и условий, способствовавших совершению подделки образовательных документов.

Наиболее адекватными тактическими решением применительно к расследуемой ситуации является проведения следователем проверочных действий в отношении подозреваемого лица. С учетом имеющихся специфик, присущих подделки образовательных документов, представляется необходимым выяснение наличие у подозреваемого лица определенных навыков, способствовавших совершению рассматриваемой разновидности преступлений. Помимо этого, возникает вопрос потребность выяснения у подозреваемого лица его отношения к произошедшим событиям. Для решения данной проблемы следственной практикой апробированы и внедрены карты комплексного изучения лиц, совершения различные виды преступлений, составление которых позволяет следственным органом получения дополнительную информацию о личности подозреваемого.

Применительно к данной следственной ситуации алгоритм следственных действий и оперативно-розыскных мероприятий выглядит следующим образом:

организация назначения и производство судебных экспертиз;

производство осмотра места происшествия;

- установление взаимодействия с сотрудниками оперативно-розыскных подразделений и экспертами-криминалистами;

- установление предмета подлога, места, времени, способа, технических средств и обстановки его совершения;

- установление личности преступника (или преступной группы) по социально-демографическим, нравственным, поведенческо-психологическим признакам, принадлежности к гражданству РК, мотива совершения преступления;

- установление круга лиц, причастных к преступлению (организаторы, подстрекатели, пособники, в том числе лица, ответственные за выдачу и хранение документов); наличие признака неоднократности; устойчивость и длительность существования преступной группы; получение вербальной и материально-отображаемой доказательственной информации, в том числе компьютерных программ, баз данных, информации в сети Интернет;

- установление размера причиненного ущерба интересам третьих лиц;

установление причинно-следственной связи подлога с родственными составами преступлений (мошенничеством, незаконным присвоением собственности, компьютерными преступлениями, служебным подлогом, в том числе с иностранным элементом).

Среди предполагаемых способов решения, поставленных задач на первоначальном этапе расследования мы бы выделили: преследование, задержание и допросы лиц, совершивших преступление; обыск по месту жительства и работы подозреваемого; обнаружение, фиксацию, изъятие и сохранение следов преступления; установление свидетелей, очевидцев; назначение судебных экспертиз.

Допрос подозреваемого осуществляется в соответствии с положениями Главы 26 УПК РК и в частности ст. 216 УПК[4]. Допрос целесообразно проводить после допросов ответственных лиц, коллег, друзей, родственников. При этом следует иметь в виду, что доказательствами являются собственно ответы подозреваемого, а не вопросы, поэтому формулировка вопросов не так важна, как информация, которая может быть получена в ходе допроса. Кроме того, допрос можно построить в виде интервью, что позволяет беседе протекать более естественно, чем жесткий сценарий. Места, время и продолжительность допроса регламентируется ст. 209 УПК РК.

По мнению Е. Н. Бегалиева, «следственная ситуация представляет собой совокупность данных о событии преступления и обстоятельствах, характеризующих условие (обстановку) его расследования на конкретном этапе, обуславливающих выбор средств и методов установления истины по делу»[5, 221].

Выбор способа подлога документов об образовании, наряду с предметом преступления, обусловлен условиями места и времени его совершения, личными качествами преступника (или преступной группы), его умениями и навыками. Чтобы очертить круг участников преступления, предусмотренного ст. 385 УК РК, необходимо:

1) установить личности преступников, их возраст, социальное положение, должности, места жительство, работы (учебы);

2) кто является организатором преступной группы;

3) какие действия выполнялись каждым из участников, в течение какого периода времени;

4) какую цель преследовал каждый из участников преступной группы;

5) каким образом осуществлялось сокрытие фактов подлога;

6) как распределялся преступный доход от реализации поддельных документов.

От решения этих вопросов непосредственно зависит квалификация действия каждого из привлекаемых к уголовной ответственности лиц. Данные о роли и цели участников преступной группы позволяют следователю выбрать тактику допроса и получить правдивые показания. Если участник исполнял роль похитителя бланков или печатей, изучаются конкретные операции, которые совершало лицо, каким способом, в какой время, из каких объемах, каким образом похищенные документы изымались из мест хранения, как осуществлялось сокрытие фактов хищения. При хищении бланков должностным лицом, этому могли способствовать такие факторы, как: не отлаженная надлежащим образом система документооборота в органах власти и вузе; коррупционные связи должностных лиц; несоблюдение правил хранения печатей, штампов, бланков; слабая защита документов; низкий контроль руководства или преступный сговор с руководителем, и другие.

---

[1] Повезюк Г. И. Концептуальные основы криминалистического установления личности: Автореф. дис. … канд. юрид. наук. — Алматы, 2003.

[2] Нургалиев Б. Б. Тактические основы изобличения лиц, противодействующих расследованию преступлений путем дачи ложных показаний: Автореф. дис. … канд. юрид. наук. — Алматы, 2006.

[3] Исханов К. Е. Проблемы преодоления противодействия расследованию путем использования тактических приемов: Автореф. дис. … канд. юрид. наук. — Алматы, 2004.

[4] Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК (ред. 02.01.2021) // Ведомости Парламента РК. — 2014. — № 13-II.

[5] Бегалиев Е. Н. Расследование преступлений, совершаемых путем подделки материальных объектов. — Алматы, 2008.

Исаев А. А.,
профессор НОД «Право»
Школы права и государственного управления,
доктор юридических наук, профессор
(Университет «Нархоз», Республика Казахстан, г. Алматы)

Содержание идентификации в судебной экспертологии и в криминалистике в контексте применения инновационных технологий

Вопросы внедрения инновационных технологий в сферу научных исследований, в частности, информационных систем в качестве методической составляющей для решения задач расследования преступлений и судебной экспертизы, требуют завершенности в определении содержания предмета того или иного научного направления, изменения содержания предмета на различных временных промежутках, и обусловлены проблемами становления данного научного направления как самостоятельной отрасли знания, с различным объемом эмпирического и теоретического материала на различных этапах его развития.

В основе формирования любой отрасли знания лежат процессы дифференциации на основе эмпирического накопления нового знания в том или ином виде деятельности, оформления его содержания и системы в целостную структуру. Появление нового знания обусловлено также процессами интеграции, связанными с привлечением данных других отраслей знаний, их переработкой соответственно

целям и задачам того или иного вида деятельности, что в конечном счете приводит к появлению нового знания. Как правило, на начальном этапе появления нового знания еще не полностью бывают сформированы содержание, система и структура новой отрасли, поэтому на данном этапе представляет определенную сложность точное определение предмета данного нового знания, хотя отличие его от предмета знания, в недрах которого последнее сформировалось, является бесспорным.

Вышеуказанные особенности нашли свое отражение также в развитии криминалистики, в определении предмета криминалистики на различных этапах ее развития. Различными авторами в различные временные этапы давались различные определения предмета криминалистики, отражающие, в конечном счете, уровень развития криминалистики как новой отрасли знания. И не случайно по мере накопления практического и теоретического материала в рамках криминалистики взгляды ученых на ее предмет менялись. Более того, можно утверждать, что каждое определение могло претендовать на истину соответственно своему времени.

Аналогичные процессы имели место и в рамках становления и развития судебной экспертологии как самостоятельной отрасли науки. Для судебной экспертологии таким видом деятельности являлась изначально криминалистическая наука. Такие криминалистические учения, как учение о признаках, учение о механизмах следообразования, теории криминалистической идентификации, диагностики, классификации и ситуации и др., составляют основу теории судебной экспертизы. Вместе с тем, дифференциационные процессы, неподкрепленные завершенным эмпирическим и теоретическим материалом, не только сдерживают развитие новой отрасли знания, но и создают определенные проблемы в практической области деятельности. В частности, это касается теории криминалистической идентификации, которая трактуется в судебной экспертизе с позиций криминалистической науки, в связи с чем не удается выделить непосредственно сами разработки судебной экспертологии применительно к теории идентификации, что приводит к тому, что они не всегда воспринимаются в криминалистике и в практике уголовного судопроизводства. Причиной такого положения является трактовка идентификации в судебной экспертизе как установления индивидуально-конкретного тождества.

В связи с изложенным рассмотрим некоторые аспекты криминалистической теории идентификации, которая на протяжении длительного времени была одной из самых разработанных частных криминалистических теорий. Несмотря на наличие множества научных статей и монографических исследований различных авторов, ряд положений данной теории понимается учеными по-разному. Некоторые из них сужают границы криминалистической идентификации, круг исследуемых объектов, другие, напротив, безмерно их расширяют. Ряд положений, которые вчера казались бесспорными, сегодня требуют своей переоценки. Практика выдвинула перед теорией ряд задач, связанных с необходимостью пересмотра некоторых форм идентификационных исследований, существующих в рамках старых представлений об идентификации, что обедняет их и не позволяет им раскрыться во всех проявлениях.

Подобный интерес к проблемам криминалистической идентификации также связан с тем, что теория криминалистической идентификации, будучи наиболее систематизированной формой научного знания на настоящий момент, выполняет важную методологическую функцию в криминалистике и смежных отраслях знания. Формирование на базе положений общей теории криминалистической идентификации объектовых теорий привело к тому, что преобладающим стало трасологическое направление, и именно с трасологических позиций и трасологического понимания признака в отражательном процессе стали трактоваться объекты исследования, природа тождества в целом, виды идентификации. Широкий круг объектов криминалистической идентификации стал рассматриваться в рамках и с позиций трасологических объектов, а требования к ним стали ограничивать рамками требований индивидуальной определенности. Необходимо было выйти за рамки данных требований и рассматривать систему знаний криминалистической идентификации в рамках процесса доказывания, следовало расширить сферу применения криминалистической идентификации не только в судебной экспертизе, но и при производстве следственных действий любым участником процесса доказывания. Идентификация как один из способов познания при применении в практике расследования и судебном процессе используется для исследования единичного конкретного события преступления в юридически значимых признаках, то есть результаты идентификации в процессе доказывания используются в качестве судебных доказательств.

Вышеуказанные аспекты обусловили необходимость рассмотрения объектов идентификации не только в рамках установления тождества, то есть их деления на идентифицируемый и идентифици-

рующий, но и в рамках установления их связи с событием преступления, то есть выделение объектов проверяемых и искомого объекта. Если классификация объектов на идентифицирующие и идентифицируемые предназначена для исследования отражательного процесса и разрешения вопроса о тождестве, то деление объектов на проверяемые и искомые — для исследования связи единичного объекта с событием преступления методами процессуального доказывания с использованием идентификации. При этом установление идентифицируемого объекта опирается на идентификационные признаки и осуществляется путем технического сравнительного исследования. Установление искомого объекта опирается на систему доказательств об искомом объекте и осуществляется путем доказывания. Задача доказывания с использованием идентификации состоит в установлении единичного материального объекта и его связи с расследуемым событием. При этом доказывание не равнозначно акту отождествления. Доказывание включает в себя идентификацию в качестве одного из элементов.

В процессе доказывания необходимо различать:

- задачу идентификации, состоящую в разрешении вопросов о тождестве материальных объектов по их следам;

- задачу установления материального объекта и раскрытия его связи с расследуемым событием преступления на основе проведенной идентификации.

Последний подход при рассмотрении проблем криминалистической идентификации обусловил смещение акцентов в сторону установления причинной связи того или иного объекта с событием преступления. Наряду с установлением тождества стал исследоваться процесс доказывания тождества. Данное понимание тождества позволяет по-новому рассматривать формы идентификации, позволяет провести различие между идентификацией в судебной экспертизе и в криминалистике.

Необходимость разработки теоретических аспектов идентификации в судебной экспертизе возникла с появлением так называемой нетрадиционной криминалистической идентификации. Последняя стала разрабатываться с момента становления криминалистической экспертизы материалов и веществ. Исследования данного рода экспертиз стали причиной интенсивного разработки проблемы соотношения признака и свойства, пересмотра проблемы индивидуализации применительно к объектам исследования данного рода экспертизы. Все теоретические разработки в криминалистической экспертизе материалов и веществ были направлены на признание их объектов исследования индивидуально определенными и на возможность установления их тождества в процессе экспертного исследования. При этом результаты исследования «подгонялись» под запросы практики уголовного судопроизводства, выводам экспертиз пытались придавать значение прямых доказательств через создание и теоретическое обоснование таких форм криминалистической идентификации, как установление групповой принадлежности, установление общего источника происхождения, установление общего объема и массы, установление факта контактного взаимодействия объектов, идентификация по встречным связям. Невозможность установления индивидуально-конкретного тождества подменяли решением задачи установления целого по части, теоретически обосновывая возможность формулирования подобных экспертных выводов посредством признания единообразного содержания признаков и свойств в противовес пониманию содержания признака как отражения свойства. Игнорирование требования индивидуальности объекта исследования в рамках криминалистической идентификации становилось причиной проблем использования заключений криминалистической экспертизы материалов и веществ для решения задач уголовного судопроизводства — установления обстоятельств уголовного правонарушения, установления элементов состава уголовного правонарушения, доказывания вины подозреваемых. Следователи и судьи не могут использовать данные заключения как однозначные утверждения в процессе доказывания и ограничиваются простой констатацией данных выводов без их анализа применительно к имеющимся в деле доказательствам. Причиной такого положения является отсутствие понимания специфики идентификации в судебной экспертизе и рассмотрение проблем криминалистической экспертизы материалов и веществ через призму положений теории криминалистической идентификации.

На основе вышеизложенного однозначно напрашивается вывод о том, что дальнейшие попытки рассматривать проблему идентификации в судебной экспертизе в контексте теоретических положений криминалистической идентификации сдерживают развитие судебной экспертизы как в теоретическом, так и в практическом плане. Последнее особенно важно с появлением современных возможностей идентификации личности на основе применения инновационных технологий: биометрии, видеоизображения, ДНК-методов и др. Учитывая наличие самостоятельного научного знания как судебная экс-

пертология, следует разрабатывать теоретические положения идентификации применительно к специфике объектов исследования в судебной экспертизе. Именно с позиций возможности и допустимости доказывания тождества в процессе расследования, необходимости установления связей между объектами идентификации и обстоятельствами уголовного правонарушения необходимо рассматривать и разрабатывать теоретические положения идентификации в судебной экспертологии, трансформируя и адаптируя для этих целей при необходимости положения криминалистической идентификации.

[1] Белкин Р. С. Курс криминалистики: Частные криминалистические теории. Т. 2. — М.,1997.
[2] Белкин Р. С., Винберг А. И. Криминалистика и доказывание. — М., 1969.
[3] Винберг А. И., Малаховская Н. Т. Судебная экспертология. — Волгоград, 1979.
[4] Колдин В. Я. Идентификация при расследовании преступлений. — М., 1978.
[5] Колмаков В. П. Идентификационные действия следователя. — М., 1977.
[6] Потапов С. М. Роль методов криминалистики в доказательственном праве (рукопись). — М., 1943.
[7] Седова Т. А. Проблемы методологии и практики нетрадиционной криминалистической идентификации. — М., 1986.
[8] Сегай М. Я. Методология судебной идентификации. — Киев, 1970.

Кадырова Р. Т.,
Заместитель начальника кафедры кибербезопасности
и информационных технологий, подполковник полиции
(Алматинская академия
МВД Республики Казахстан им. М. Есбулатова)

КРИПТОВАЛЮТЫ: ПОЛОЖИТЕЛЬНЫЕ СВОЙСТВА И НЕДОСТАТКИ

В настоящее время криптовалюты привлекают к себе большое внимание. За темпами их развития внимательно следят новостные агентства, а также просто интернет-пользователи. Криптовалюта не является реальной валютой, она существует только в цифровом виде и содержит зашифрованную информацию, защищенную от подделок. Сейчас такая валюта становится все более популярной. Это связано с увеличением количества денежных транзакций, которые подтверждаются в интернете с помощью третьей стороны в платежной системе. С появлением криптовалюты транзакции происходят без участия третьих лиц, то есть транзакции подтверждаются самой сетью[1]. Это является важной особенностью использования криптовалюты, поскольку она помогает сократить расходы на перевод средств. В отличие от платежных систем криптовалюты, она имеет децентрализованную структуру, а также решает многие проблемы, связанные с валютными рисками и конвертацией[2].

Криптовалюта появилась не так давно, хотя историю ее развития уже можно разделить на этапы:

1) этапы выхода – появление криптовалюты начинается с создания биткоина человеком по имени СатошиНакомото или группой людей. Несомненно, большинство технологий, заложивших основы биткоина, уже сформировались в конце XX – начале XXI века. Однако только этот биткоин, появившийся в 2009 г., стал первой криптовалютой. В конце 2010 г. с выходом Сатоши из этого проекта завершается первый этап развития;

2) этапы становления (в конце 2011 – 2013 гг.) — в этот период произошло укрепление криптовалюты, появление новых ее видов (таких как Ripple, Litecoin, Namecoin, Peercoin и др.), а также рост доверия к ней и увеличение операций;

3) период ввода в оборот (2014 – 2016 гг.) — на этом этапе криптовалюта стала активно использоваться компаниями и простыми людьми для совершения сделок, а также осуществлялся запуск площадок, где торговля шла исключительно биткоинами;

4) период признания криптовалют и начала регулирования центробанками (2017 г. – по настоящее время) — разные страны по-разному относятся к криптовалютам, но многие стремятся ее регулировать, т. е. издавать законы и действовать в соответствии с ними на одном и том же рынке. Некоторые государства не хотят признавать такой подход к обмену: и на это есть определенные причины, так как у этой валюты есть свои недостатки, о которых мы расскажем ниже[3].

Так, несмотря на короткий период развития цифровых денег, они стремительно занимают свое место в экономике. Более того, с каждым годом криптовалют становится все больше. Далее рассмотрим наиболее распространенные их виды.

Основными криптовалютами, которые доминируют в мировой экономике, являются: Биткоин (Bitcoin – BTC), Эфириум (Ethereum — ETH), Риппл (Ripple) и др.

Одним из критериев, позволяющих составить рейтинг криптовалют, является рыночная капитализация. По этому критерию приведенные выше криптовалюты составили собственную шкалу. В «тройку лидеров» входят Биткоин, «Эфир», который в народе называют Эфириум, Риппл и Биткоин Кэш. Их капитализация составляет 159 триллионов долларов, 69 триллионов долларов, 36 триллионов долларов и 25 триллионов долларов соответственно.

В качестве иного критерия можно назвать популярность криптовалюты. В соответствии с этим ранжированием, биткоин снова является лидером. За ним стоит Эфириум, перспективы которого достаточны для того, чтобы в скором времени выйти на лидерские позиции. И замыкает тройку уже действующий Риппл с банками.

Кроме того, в качестве одного из критериев можно получить величину курса криптовалюты по отношению к доллару США. И здесь первое место занимает Биткоин по курсу 3.654.480,53 тенге ($ 9363,33). Следом за ним идут Биткоин-Кэш 106.127, 03 тенге ($ 270,75) и Эфириум 71.882,82 тенге (эфир 184,16).

Исходя из приведенных данных, можно сказать, что Bitcoin по-прежнему пользуется популярностью среди других криптовалют, несмотря на то, что конец 2017 г. упал с начала 2018 г. Биткоин добивается этого успеха, несмотря на высокую скорость оборота, анонимность и другие факторы, влияющие на их покупку, в отличие от криптовалют.

В настоящее время все криптовалюты находятся в очень динамичном состоянии. Однако у них есть свои положительные качества и недостатки, которые не меняются с момента их появления.

Начнем с рассмотрения положительных сторон криптовалюты. Наиболее заметным их свойством, как мне кажется, является их динамичность. Быстрые и несложные денежные переводы и платежи без участия посредников сегодня очень востребованы. И это говорит о высоком спросе на криптовалюты, о котором мы говорили выше. Нельзя не упомянуть и о том, что цифровые деньги может получить любой, кто имеет доступ к интернету.

Неограниченные возможности транзакций — еще одно преимущество. Это будет способствовать привлечению крупных компаний и бизнесменов, которым необходимо будет перевести большие суммы денег.

Следующее преимущество — мировая Распространенность. Благодаря этой особенности сотрудник может выполнять свои обязанности в любой точке мира. Это также позволяет каждому в кратчайшие сроки получать доход, производя выплаты в любом государстве.

Еще одним преимуществом является прозрачность. Невозможно обмануть криптовалютную систему или сделать что-то таким, каким другие не знают. Более того, большинство процессов контролируется разработчиками и сообществом, в связи с чем все участники сети могут видеть проводимые операции. Вот почему количество взломов криптовалютных систем очень мало. Однако здесь сохраняется анонимность, то есть можно узнать, сколько денег находится на любом кошельке, но определить его владельца невозможно[4].

К числу преимуществ виртуальных валют можно отнести, также криптовалютный кошелек. Это своеобразный расчетный счет, особенность которого заключается в невозможности его закрытия или прекращения.

Тем не менее, криптовалюты обладают не только такими положительными свойствами, но и почти такими недостатками, которые в большинстве случаев негативно сказываются на экономической среде.

Например, такие недостатки криптовалют, как анонимность выхода и оборота, высокая волатильность и спекулятивные колебания, тревожат финансовых регуляторов. Ведь такая тенденция может перерасти в теневую экономику, а это противозаконно[5].

Во-вторых, транснациональность криптовалют. По этой причине государства не могут поставить свои границы, а это исключает их контроль, т. е. возникает проблема, связанная с децентрализованным и наднациональным характером валюты. Одно государство не может ограничивать его оборот и обмен с его применением. Следствием этого является развитие и упрощение деятельности преступных сообществ. Для урегулирования этой тенденции необходима консолидация государств и совместные действия в этом направлении.

В-третьих, отсутствие или несовершенство законодательства, регулирующего конкретную сферу. В настоящее время большинство государств ограничиваются банковскими предложениями по использованию криптовалют и точечными правовыми нормами, не имеющими возможности полностью регулировать оборот криптовалют.

И последнее полная неподготовленность правоохранительных органов к раскрытию и расследованию преступлений, совершаемых с использованием криптовалют. Особенно это касается сферы наркоторговли.

Глядя на вышеизложенные вопросы, можно прийти к выводу, что регулирование криптовалютной отрасли очень сложно и в некоторых сферах совершенно невозможно. Государство должно создать законодательство для регулирования этой сферы общественной жизни.

Существует несколько способов, как государство должно вести себя в отношении цифровых денег[6]:

1. Признание их незаконными. Но такое решение приведет к финансовой самоизоляции государства от другого мира, а также к отказу от актуального для всего мира направления развития.

2. Регулирование валюты на законодательном уровне, введение налогообложения на осуществление операций с ними. Это приоритетное направление, выбранное большинством наиболее развитых государств.

3. То, что сейчас происходит в Республике Казахстан – это отсутствие законодательства. Пока это является переходным периодом, хотя парламент страны должен в ближайшее время принять решение о том, какую политику в этом направлении проводить.

Итак, вывод, на мой взгляд, отрасль, в которой осуществляется деятельность с помощью криптовалюты в Республике Казахстан, следует рассматривать, как способ существования рыночной экономики. Потому что, государство в настоящий момент не оказывает существенного влияния на экономический оборот, происходящий с помощью цифровых денег. В связи с этим можно сказать, что криптовалюта пока не может вытеснить наши обычные, привычные фиат-деньги. Но они имеют полное право на жизнь и развитие как часть экономики, если, конечно, основные проблемы, перечисленные выше, будут решены.

---

[1] Дурдыева Д. А. Состояние криптовалютного рынка и перспективы развития биткоин / Д. А. Дурдыева, А. А. Трапизонян // Инновационная наука. — 2017. — № 1. — С. 43 – 47.

[2] Любшина Д. С. Криптовалюта как инновационный инструмент мировой торговли / Д. С. Любшина, А. В. Золотарюк // Интерактивная наука. — 2016. — № 10. — С. 145 – 146.

[3] Бабкин А. В. Криптовалюта и блокчейн-технология в цифровой экономике: генезис развития / А. В. Бабкин, Д. Д. Буркальцева, В. В. Пшеничников, А. С. Тюлин // Научно-технические ведомости СПбГУ. Экономические науки. Том 10. 2017. № 5. С. 9 – 21.

[4] Зеленюк А. Н. Новые криптовалюты в мировой экономике / А. Н. Зеленюк, Г. А. Орлова, Е. В. Тарановская // Российский внешнеэкономический вестник. — 2017. — № 8. — С. 65 – 79.

[5] Сидоренко Э. Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. — 2017. — № 6. — С. 147 – 154.

[6] Современные информационно-коммуникационные технологии для успешного ведения бизнеса / Под ред. Ю. Д. Романовой. — М., 2017.

Калиев А. А.,
руководитель криминалистического отдела
Департамента экономических расследований по г. Алматы
Агентства Республики Казахстан по финансовому мониторингу,
квалификационный класс 4-ой категории (капитан)

Использования научного подхода цифровой криминалистики в расследовании любых видов правонарушений

«*Форензика*» (*компьютерная криминалистика, расследование киберпреступлений*) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. В современном быстроразвивающемся цифровом мире сложно переоценить роль компьютерной техники в жизни людей, злоумышленники все чаще используют достижения научного прогресса для совершения преступлений. Использования электронных гаджетов в совершении преступлений не несет в себе явных

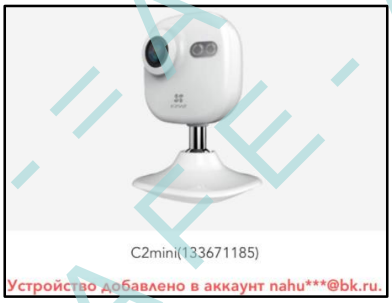
признаков правонарушения, однако, всегда остаются латентные следы. Использования научных методов цифровой криминалистики в расследовании преступлений делает возможным поиск цифровых улик, закрепления их как доказательную базу, а также правильную интерпретацию цифровых улик в суде.

В своей статья хотелось бы поделится положительным опытом использования основ «*Форензики*» в расследовании правонарушении любых видов.

В производства криминалистического отдела Департамента экономических расследований по городу Алматы поступило уголовное дело расследуемое центральным аппаратом Министерство внутренних дел РК по признакам правонарушения предусмотренного ст. 99 п. 2 ч. 6 «*Убийство, то есть противоправное умышленное причинение смерти другому человеку, совершенное опасным для жизни других способом*». **Фабула дела**: «*на гражданина А в период 2018 – 2019 совершено 5 покушений, в 6 раз преступники заминировали лестничный пролет коттеджа, в котором проживал подозреваемый, в качестве детонатора использовался мобильный телефон, на сотовый номер которого в нужный момент времени совершался звонок, тем самым приводя в действия взрывное устройство, как позже установлено тротил. Наблюдение за гражданином велось при помощи цифровой ip-камеры марки «EZVIZ»*»

После совершенного преступления оперативно следственная группа на месте преступления изъяла IP-камеру марки «*EZVIZ*», на которой не было обнаружено отпечатков пальцев. Опрос свидетелей не дал нужного результата.

С целью поиска и изобличения преступника, использовалось приложения для конфигурирования (*настройки*) и работы с IP-камера «*EZVIZ*». В результате первичного подключения ПО предлагает отсканировать «*QR-код*»[1], при выполнении соответствующих действий выдает уведомления о том, что объект отконфигурирован (*настроен*) и синхронизирован с аккаунтом (*логином*) «*nahuy2019@bk.ru*» (см. снимок с экрана № 1).



Снимок с экрана № 1. Проверка подключения к IP-камере

Согласно сведениям, предоставленным порталом «*mail.ru*», дата регистрации (*создания*) почтового ящика 07.12.2018 13:49 (*время сервера, расположенного в г. Москва*) IP-адрес создателя «*89.40.193.193*», привязан к абонентскому номеру «*+77778521753*». Обнаруженный IP-адрес является динамическим (*свободно выдающимся через определенный период времени*) IP-адресом, являющимся массивом адресов, принадлежащих ТОО «*КаР-Тел*» (см. снимок с экрана № 2).

Имя провайдера:	ТОО "КаР-Тел"
Сайт провайдера:	http://www.beeline.kz/
Проверяемый хост:	89.40.193.193 (whois)

Снимок с экрана № 2. Сервис проверки IP-адресов с сайта «https://2ip.ua»

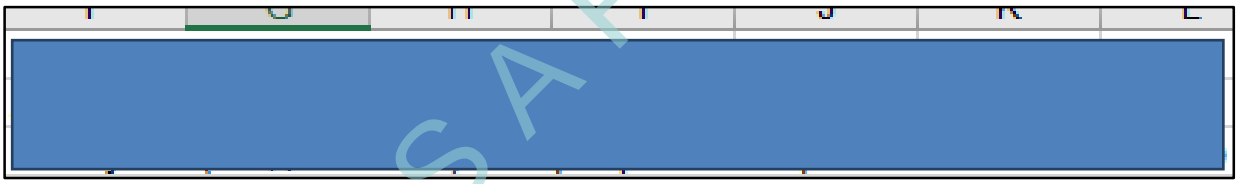
Согласно полученному ответу от интернет-провайдера ТОО «*КаР-Тел*» следует, что в интересующий период времени 07.12.2018 г. (*по времени г. Астана*) IP-адрес «*89.40.193.193*» присваивался 161 (*сто шестьдесят одному*) абоненту Билайн, в том числе и юридическим лицам (см. снимок с экрана № 3).

Снимок с экрана № 3. Данные ТОО «КаР-Тел»

Также согласно полученному ответу от интернет-провайдера ТОО «*КаР-Тел*» следует, что в интересующий период времени 16.12.2018 г. (*по времени г. Астана*) IP-адрес «*89.40.193.228*» присваивался 77 (*семидесяти семи*) абоненту Билайн, в том числе и юридическим лицам (см. снимок с экрана №4).

Снимок с экрана № 4. Данные ТОО «КаР-Тел»

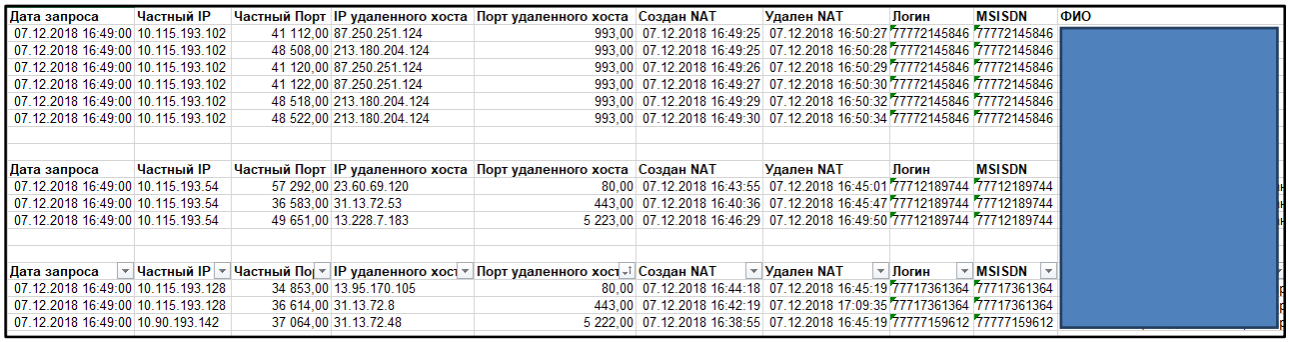
Для поиска создателя почтыпроводилось сравнения двух таблиц с историями посещения почтового ящика «*nahuy2019@bk.ru*» на предмет совпадения абонентов «*Билайн*». В результате выполненных действий установлено 3 (*три*) совпадения тесть обнаружены одинаковые абоненты провайдера ТОО «*КаР-Тел*» которым были присвоены IP-адреса 07.12 и 16.12.2018 г. (см. снимок с экрана № 5).



Снимок с экрана № 5. Данные ТОО «КаР-Тел»

Далее с целью установления фактов посещения почтовых сервисов специалист применял сортировку по фильтру с условием «*удаленный порт*». Порт приложения является целым числом, указывающим принадлежность к определённому приложению (*программе*), согласно международной маркировке «*IMAP — протокол прикладного уровня для доступа к электронной почте. Базируется на транспортном протоколе TCP и использует порт 143, а IMAPS (IMAP поверх SSL) — порт 993. IMAP работает только с сообщениями и не требует каких-либо пакетов со специальными заголовками*»

В результате применённого фильтра порт прикладного уровня для доступа к электронной почте 993 обнаружен только у абонента «*гражданин В*» (см. снимок с экрана № 6).



Дата запроса	Частный IP	Частный Порт	IP удаленного хоста	Порт удаленного хоста	Создан NAT	Удален NAT	Логин	MSISDN	ФИО
07.12.2018 16:49:00	10.115.193.102	41 112,00	87.250.251.124	993,00	07.12.2018 16:49:25	07.12.2018 16:50:27	77772145846	77772145846	
07.12.2018 16:49:00	10.115.193.102	48 508,00	213.180.204.124	993,00	07.12.2018 16:49:25	07.12.2018 16:50:28	77772145846	77772145846	
07.12.2018 16:49:00	10.115.193.102	41 120,00	87.250.251.124	993,00	07.12.2018 16:49:26	07.12.2018 16:50:29	77772145846	77772145846	
07.12.2018 16:49:00	10.115.193.102	41 122,00	87.250.251.124	993,00	07.12.2018 16:49:27	07.12.2018 16:50:30	77772145846	77772145846	
07.12.2018 16:49:00	10.115.193.102	48 518,00	213.180.204.124	993,00	07.12.2018 16:49:29	07.12.2018 16:50:32	77772145846	77772145846	
07.12.2018 16:49:00	10.115.193.102	48 522,00	213.180.204.124	993,00	07.12.2018 16:49:30	07.12.2018 16:50:34	77772145846	77772145846	

Дата запроса	Частный IP	Частный Порт	IP удаленного хоста	Порт удаленного хоста	Создан NAT	Удален NAT	Логин	MSISDN
07.12.2018 16:49:00	10.115.193.54	57 292,00	23.60.69.120	80,00	07.12.2018 16:43:55	07.12.2018 16:45:01	77712189744	77712189744
07.12.2018 16:49:00	10.115.193.54	36 583,00	31.13.72.53	443,00	07.12.2018 16:40:36	07.12.2018 16:45:47	77712189744	77712189744
07.12.2018 16:49:00	10.115.193.54	49 651,00	13.228.7.183	5 223,00	07.12.2018 16:46:29	07.12.2018 16:49:50	77712189744	77712189744

Дата запроса	Частный IP	Частный По	IP удаленного хост	Порт удаленного хост	Создан NAT	Удален NAT	Логин	MSISDN
07.12.2018 16:49:00	10.115.193.128	34 853,00	13.95.170.105	80,00	07.12.2018 16:44:18	07.12.2018 16:45:19	77717361364	77717361364
07.12.2018 16:49:00	10.115.193.128	36 614,00	31.13.72.8	443,00	07.12.2018 16:42:19	07.12.2018 17:09:35	77717361364	77717361364
07.12.2018 16:49:00	10.90.193.142	37 064,00	31.13.72.48	5 222,00	07.12.2018 16:38:55	07.12.2018 16:45:19	77777159612	77777159612

Снимок с экрана № 6. Фильтрация запросов к электронной почте

В результате проведенного криминалистического исследования установлен гражданин «В», который момент времени (*07.12.2018*) настраивал предоставленную камеру.

Фабула дела: *«ДЭР по городу Алматы проводилось досудебное расследования по факту хищения денежных средств АО «KCELL», выделенных на закуп услуг по рассылке СМС для клиентов АО «KaspiBank» и АО «Народный банк Казахстана» абонентов «Beeline, Altel, Tele2». Рассылка СМС осуществлялось через провайдера, которым в период 2017 – 2019 гг. являлось ТОО «MobileMultimediaServices», а с января 2019 г. ТОО «BS-Traffic».»*

В связи с тем, чтодля квалификации деяний по данной статье необходима точная сумма причиненного ущерба, а объектами исследования являются отправленные в адрес получателей «*СМС*» сообщения (*фактический «воздух»*) применения стандартных методов расследования не принесло желаемых результатов.

С целью установления, имеется ли, в базе данных сведения о количестве отправленных сообщений использовался структурированный SQL-запрос (*select*) к базе данных для получения требуемых сведений. **Фрагмент составленного запроса:**

```
select TO_CHAR(INIT_TIME, 'yyyy-mm') init_time,
user_id,
    sender,
rn_code,
message_status,
    sum(segment_count) total
from app_smsgw.v2_messages b
where init_time BETWEEN TO_DATE('2019-04-01 00:00:00',
    'YYYY-MM-DD HH24:MI:SS') AND TO_DATE('2019-05-01 00:00:00',
    'YYYY-MM-DD HH24:MI:SS')
    and user_id = '592'
group by TO_CHAR(INIT_TIME, 'yyyy-mm'), b.user_id, sender, rn_code, message_status
```

В результате составленного SQL-запроса[2] были получены следующие информационные сведения (см. снимок с экрана № 1):

```
select TO_CHAR(INIT_TIME, 'yyyy-mm') init_time,
       user_id,
       sender,
       rn_code,
       message_status,
       sum(segment_count) total
from app_smsgw.v2_messages b
where init_time BETWEEN TO_DATE('2019-04-01 00:00:00',
            'YYYY-MM-DD HH24:MI:SS') AND TO_DATE('2019-05-01 00:00:00',
            'YYYY-MM-DD HH24:MI:SS')
            and user_id = '592'
group by TO_CHAR(INIT_TIME, 'yyyy-mm'), b.user_id, sender, rn_code, message_status
```

ery Result

SQL | Fetched 50 rows in 75,612 seconds

INIT_TIME	USER_ID	SENDER	RN_CODE	MESSAGE_STATUS	TOTAL
2019-04	592	KaspiBonus	07	D	200641
2019-04	592	KaspiKredit	02	D	2129888
2019-04	592	KaspiBonus	02	D	1145691
2019-04	592	KaspiBonus	77	D	556268
2019-04	592	KaspiRED	77	E	26120
2019-04	592	kaspi bank	77	D	669638
2019-04	592	KaspiBank	01	D	901514
2019-04	592	kaspi bank	01	D	734546
2019-04	592	4215	02	D	230590
2019-04	592	Kaspi Shop	77	D	556303

(Снимок с экран № 1 «SQL-запрос»)

Далее с целью разделения полученных сведений по абонентам *«KCELL», «TELE2», «ALTEL», «BEELINE»* использовалась фильтрация по полю «*RN_CODE*» (*разделения на операторов связи*), в котором 01 — абоненты «*Beeline*», 02 — абоненты «*Kcell*», 07 — абоненты «*Altel*», 77 — абоненты «*Tele2*».

В результате разделения были получены следующие информационные сведения (см. снимок с экрана № 2).

3		Altel	Tele2	Beeline		Total
4	2017-01	438595	1710991	3218522		5368108
5	2017-02	464191	1840196	3365211		5669598
6	2017-03	525557	2053762	3587811		6167130
7	2017-04	1065470	1426724	3727901		6220095
8	2017-05	541295	2091563	3408022		6040880

Снимок с экрана № 2. Разделения по операторам связи

В результате криминалистического исследования в базе данных АО «KCELL» в период 2017 – 2019 гг. из ТОО «MobileMultimediaServices», а с января 2019 г. ТОО «BS-Traffic» в адрес АО «KCELL» отправлены данные о количестве СМС с завышением на **127 018 711** единиц, отправляемых клиентам АО «KaspiBank» и АО «Народный банк Казахстана», на сумму **693 000 611** тенге.

[1] QR-код (англ. QuickResponseCode — код быстрого реагирования; сокр. QR code) — тип матричных штрихкодов (или двумерных штрихкодов), изначально разработанных для автомобильной промышленности Японии. Сам термин является зарегистрированным товарным знаком японской компании «Denso».

[2] SQL («*язык структурированных запросов*») — декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных, управляемой соответствующей системой управления базами данных.

Каримова Д. Э.,
докторант факультета послевузовского образования,
доктор философии (PhD) по юридическим наукам, доцент
(Академия МВД Республики Узбекистан, г. Ташкент)

О ВЗАИМОДЕЙСТВИИ ОРГАНОВ ДОСУДЕБНОГО ПРОИЗВОДСТВА В РАССЛЕДОВАНИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

В современных условиях терроризм и экстремизм рассматриваются как одно из самых тяжких преступлений, совершаемых различными общеопасными способами, чем наносят непоправимый физический вред и огромный материальный ущерб. Согласно докладу Национального консорциума, ведущего наблюдения с 1970 г. по изучению терроризма и ответов на терроризм при Мэрилендском университете США, только в 2012 г. (рекордного года по числу терактов и количеству жертв) 8 500 терактов по всему миру унесли жизни почти 15,5 тыс. человек[1].

Президент Республики Узбекистан Шавкат Мирзиёев, выступая на 72-й Генассамблее ООН в Нью-Йорке, подняв в своем выступлении вопросы экологии, региональной безопасности и религиозной терпимости, заявил, что «Применение силовых методов в борьбе с терроризмом не всегда оправдывают себя. Нередко они направлены на борьбу с последствиями этого явлениями, а не на искоренение первопричины. Наряду с другими факторами, в основе международного терроризма, в первую очередь, лежат невежество и нетерпимость»[2].

Особая опасность терроризма заключается в том, что преступления данного вида совершаются в условиях неочевидности. Исполнители терроризма либо погибают, либо скрываются с мест совершения преступления, что естественно не позволяет своевременно устанавливать и привлекать к уголовной ответственности организаторов террористических актов. Эти обстоятельства доказывают, что использование в процессе раскрытия и расследования терроризма данных, полученных оперативным путем, является объективной необходимостью. Это исходит из того, что раскрыть такие преступления только традиционными методами трудно, а порой и невозможно, поскольку такого рода преступления совершаются с применением взрывных устройств и взрывчатых веществ, преступниками предпринимаются различные меры к сокрытию преступлений, что позволяет им зачастую совершать свои деяния в течение длительного периода времени. Поэтому вероятность раскрытия такого рода преступлений только следственными мероприятиями очень низкая. Допросы потерпевших, свидетелей, подозреваемых, в большинстве случаев оказываются недостаточными, поскольку, как показывает практика, в подобных случаях перед следователем особо стоит задача быстрейшего раскрытия этих преступлений. В процессе её решения приходится проводить большой объем следственных действий, для чего усилий одного следователя оказывается недостаточно. Кроме того, их проведение зачастую связано с большими затратами времени, а в подобных ситуациях вопрос стоит о максимально оперативном установлении преступников с целью недопущения возможности совершения ими новых преступлений. Вышеприведенное обусловливает, что оперативное и полное раскрытие преступлений, привлечение всех виновных к уголовной ответственности невозможны без слаженной работы органов досудебного производства, а именно следственных и оперативно-розыскных подразделений.

Следует отметить, что взаимодействие данных подразделений при расследовании терроризма и экстремизма является разновидностью скоординированной деятельности правоохранительных органов по борьбе с преступностью, которая не ограничена только расследованием преступлений, а имеет более широкие цели, задачи и формы.

Согласно ст. 19 Закона Республики Узбекистан «Об оперативно-розыскной деятельности» от 25 декабря 2012 г., по результатам проведенных оперативно-розыскных мероприятий следователь может получить сведения:

- об объектах и предметах, которые могут нести доказательственную информацию;
- о подозреваемых лицах;

- об обстоятельствах, определяющих тактические приемы собирания доказательств;
- сведения, содействующие правильной оценке доказательств;
- о способах, месте и времени совершения преступлений и др.

При раскрытии и расследовании рассматриваемых видов преступлений, взаимосвязанные совместными целями и задачами следователь и сотрудники оперативно-розыскных подразделений должны действовать на основе общей программы, относящейся ко всему процессу расследования либо к его относительно локализованному этапу. В процессе раскрытия и расследования между участниками согласованной групповой деятельности устанавливаются определенные правила и пределы их взаимодействия, их взаимозависимость и т. д. Специфика взаимодействия в данном случае по делам о терроризме заключается в том, что оно должно осуществляться непрерывно на протяжении всего этапа предварительного расследования. Исходя из этого, представляет практический интерес вопрос о наиболее эффективных формах такого взаимодействия. В криминалистической и уголовно-процессуальной литературе преобладает точка зрения, согласно которой все формы взаимодействия делятся на процессуальные и непроцессуальные[3, 122; 4, 21; 5]. Затрагивая общие аспекты взаимодействия следователя с оперативными работниками, Г. А. Абдумажидов указывает на продолжительность времени взаимодействия, подчеркивая, что оно может быть единоразовым, кратковременным и долговременным[6].

Следует отметить, что к числу процессуальных форм относятся действия, порядок которых регламентирован нормами уголовно-процессуального законодательства. Если же, кем-либо из субъектов взаимодействия выполняются действия, порядок выполнения которых не регламентирован УПК, то эти взаимоотношения относятся к непроцессуальным формам взаимодействия (например, совместное изучение и анализ результатов по делу, выработка розыскных версий, совместное планирование розыскных и оперативно-розыскных мероприятий, направленных на установление местонахождения разыскиваемого лица; работа в следственно-оперативной группе, систематический обмен информацией между следственными и оперативно-розыскными подразделениями в процессе работы по приостановленному уголовному делу, полученными в ходе оперативно-розыскной деятельности; внесение изменений в ранее разработанный план с учетом полученной новой информации; организация взаимодействия с другими правоохранительными органами и привлечение общественности и др.). Специфика расследования терроризма и экстремизма такова, что для достижения успеха в их раскрытии приходится использовать весь арсенал вышеприведенных форм взаимодействия.

Основная направленность взаимодействия на первоначальном этапе расследования терроризма и экстремизма всегда должна соответствовать по своему характеру главной задаче расследования любого преступления, совершенного без очевидцев — установлению подозреваемых, эффективность чего во многом предопределяется получением и правильным использованием информации оперативно-розыскного характера.

Основной непроцессуальной формой взаимодействия по делам о терроризме и экстремизме, безусловно, выступает следственно-оперативная группа, поскольку совместная деятельность органов следствия и оперативно-розыскных подразделений в подобных условиях, выступает в новом качестве, превышающем возможности каждой из взаимодействующих сторон. Стабильная, технически оснащенная следственно-оперативная группа, укомплектованная квалифицированными сотрудниками — первое непременное условие успешной работы по делу. При этом следователь, являясь организатором деятельности следственно-оперативной группы, регулирует межличностные отношения, определяет возможности отдельных членов группы с целью наиболее эффективного их использования.

Как справедливо, на наш взгляд, отмечает по этому поводу В. Юрин: «Не создавая опасности смешения уголовно-процессуальной и оперативно-розыскной функции, и, не умаляя полномочий каждого из входящих в нее органов, следственно-оперативная группа устраняет организационную разобщенность следователей и сотрудников органов дознания, позволяя организовать работу по единому плану, упростив оформление поручений о производстве следственных и розыскных действий, облегчить обмен информации между следователем и другими участниками расследования, а также более активно использовать в расследовании оперативно-розыскные мероприятия»[7]. Кроме того, на сегодняшний день оправдала себя практика создания СОГ по раскрытию тяжких, особо тяжких, многоэпизодных преступлений[8].

Совместными усилиями следователя и оперативных работников должно планироваться расследование, отдельные следственные действия. Необходимым условием должно являться строгое исполне-

ние оперативными работниками поручений следователя. Ибо, как отмечает В. В. Нечаев: «Взаимодействие данных субъектов, как связующий элемент системы органов предварительного расследования, может рассматриваться как основанное на сотрудничестве неподчиненных друг другу органов, действующих согласованно, целенаправленно и целесообразно, сочетая применяемые ими средства и способы в целях предупреждения, раскрытия и расследования преступлений. Оно может проявляться в различных формах от противодействия до содействия, которые периодически сменяют друг друга, обеспечивая связь между отдельными подсистемами, как по вертикали, так и по горизонтали»[9].

Стоит особо отметить, что немаловажным условием эффективности взаимодействия при раскрытии и расследовании преступлений является социально-психологическая совместимость его субъектов, игнорирование которой в процессе взаимодействия приводит к возникновению конфликтных ситуаций, что, в свою очередь, негативно отражается на результатах расследования.

Таким образом, следует отметить, что значение взаимодействия следственных и оперативно-розыскных подразделений при расследовании терроризма и экстремизма велико, аэффективная организация данного взаимодействия будет способствовать не только успешному расследованию преступлений, но также соответствовать научным требованиям системности подхода к организации комплексного управления процессом расследования.

---

[1] URL: https://ru.m.wikipedia.org (дата обращения: 03.11.2021).

[2] URL: http://uza.uz/ru/politics/prezident-uzbekistana-shavkat-mirziyeev-vystupil-na-72-y-ses-2 0-09-2017 (дата обращения: 03.11.2021).

[3] См., напр.: Аменицкая Н. А. Взаимодействие следователя и органов, осуществляющих оперативно-разыскную деятельность, в раскрытии и расследовании преступлений (в ОВД): Дис. … канд. юрид. наук. — Н. Новгород, 2006.

[4] См., напр.: Безруких Е. С. Особенности взаимодействия следователя с оперативного работника на первоначальном этапе расследования преступлений в сфере незаконного оборота наркотиков: Дис. … канд. юрид. наук. — Калиниград, 2003.

[5] См., напр.: Каримова Д. Э. Совершенствование взаимодействия следователя органов внутренних дел с подразделениями уголовного розыска: Автореф. дис. … д-ра филос. (PhD) по юрид. наук. — Ташкент, 2018.

[6] Криминалистика: Учебн. / Г. А. Абдумажидов и др.; под ред. И. Ф. Крылова, А. И. Бастрыкина. — М., 2001.

[7] Юрин В. Формы взаимодействия в расследовании // Законность. — 2003. — № 1. — С. 39 – 43.

[8] Эсанов М. Г., Ходжаев М. Р. Следствие. — Ташкент, 2009. С. 198 – 200.

[9] Нечаев В. В. Организационно-правовые основы взаимодействия органов предварительного следствия и органов дознания. — М., 2007. С. 157 – 161.

Карл Т. М.,
криминалистика кафедрасының оқытушысы,
полиция аға лейтенанты
(Қазақстан Республикасы ІІМ
Б. Бейсенов атындағы Қарағанды академиясы)

ЦИФРЛІ АҚПАРАТ КРИМИНАЛИСТИКАДА ЭЛЕКТРОНДЫҚ ДӘЛЕЛДЕРДІҢ НЕГІЗІ РЕТІНДЕ

Адамзат өркениеті өзінің дамуының жаңа кезеңіне тез енеді. Сондықтан цифрлық ақпараттық және телекоммуникациялық технологиялардың күнделікті біздің өмірімізге жаппай енуі бүгінде жаһандық құбылысқа айналды. Бұрынғы заманда адамдар компьютерлерсіз өмір сүрген, Интернет желісі болмаған, олар туралы ақпарат пен деректер басқаша сақталған және оларға кең қолжетімділік болмаған, бұл олардың үлкен қауіпсіздігін қамтамасыз етті. Қазіргі танда заманның дамуы мен ақпараттық XXI ғасырда компьютерлік техниканың көмегімен мемлекеттік құпия құжаттарды, мәліметтерді, құнды қағаздарды сақтаудың және өңдеудің басқа әдісі ойлап табылды. Қазіргі заманның адамдары іс жүзінде ақпараттық техникалық құралдарды жиі пайдаланады және ол оларды өзімен бірге алып жүреді (ұялы телефондар, смартфондар, компьютерлер және басқа да гаджеттер) немесе олардың ауқымына кіреді (бейнебақылау камералары, бейнетіркегіштер, мобильді базалық станциялар) немесе оларға тұрақты түрде жүгінеді (әлеуметтік желілер, интернет-ресурстары).

Бүгінгі таңда компьютерлік ақпарат саласында қылмыс жасау жиілеп кетті, өйткені мекемелер мен ұйымдардың ақпараттық жүйелерінде өздерінің бағдарламалық және ақпараттық салаларында кемшіліктер бар, бұл көбінесе компьютерлік вирустарды жұқтыру, жеке мәліметтер мен мемлекеттік құпиялық мүдделерін қорғайтын ақпаратты ұрлау мүмкіндігіне әкеледі. Компьютерлер мен интернеттің жаппай таралуы мен сандық медиада сақталған ақпарат компьютерлік техниканы пайдалану арқылы заңсыз иемдену үшін қолжетімді болды. Қаскүнемдер оны ұрлау және заңсыз пайдалану

тәсілдерін ойлап тапты. Осындай қылмыстық құқық бұзушылықтардың алдын алу және қылмысты тергеп-тексеру барысында криминалистикалық зерттеулермен, эксперименттердің алатын орыны ерекше. Цифрлі іздер, өз кезегінде, нақты типтегі электронды түрде қылмыстық іс жүргізу дәлелдеріне айналуы мүмкін. Ал өзінің жиынтығында цифрлық із ақпараты ол анықталған сәтте электрондық-цифрлық нысанда болуы мүмкін, мұндай түрде ол сотқа тиісті материалдық жеткізгіште ұсынылуға тиіс. Бұл цифрлі іздер немесе дәлелдемелер түп нұсқада немесе көшіріліп жазылған болып ұсынылуы мүмкін.

Барлығын цифрлау жаһандық өзгерістерге әкеледі, соның ішінде криминалистика ол жиі аталады онда «киберкриминалистика», содан кейін «компьютерлік форензика». Бұл ақпараттық және коммуникациялық технологиялар саласында жасалған қылмыстарды бақылау ерекшеліктерінің мазмұнын барынша толық көрсететін термин «цифрлі криминалистика»[1].

Цифрлі криминалистика — бұл компьютерлерде және сандық медиада кездесетін дәлелдерге қатысты компьютерлік ақпаратпен байланысты қылмыстарды ашу, сандық дәлелдемелерді зерттеу, осындай дәлелдемелерді іздеу, алу және бекіту әдістері туралы қолданбалы криминалистиканың бөлімі. Цифрлі криминалистиканың мақсаты — сандық ақпарат туралы фактілер мен пікірлерді анықтау, сақтау, қалпына келтіру, талдау және ұсыну мақсатында криминалистика тұрғысынан сандық медианы зерттеу. Компьютерлік құрылғылар мен цифрлық криминалистиканың ақпараттық-телекоммуникациялық желілерін криминалистикалық зерттеу, қылмыстарды ашу, тергеу және алдын алу мақсатында криминалистикалық маңызы бар компьютерлік ақпараттың материалдық тасымалдаушысы ретінде ғылыми ережелер жүйесі және олардың негізінде әзірленетін компьютерлік құрылғылар мен ақпараттық-телекоммуникациялық желілерде кездесетін қылмыстарды зерттеу әдістері мен тәсілдерін қолдану үшін маңызды болып табылады. Компьютерлік қылмыстарды орындау қиын, өйткені олар «бұзу», «компьютерлік вирусты жұқтыру» және басқа да көптеген жолдармен жасалады, оларды анықтау, оларды жасау үшін кінәлілерді есептеу және, тиісінше, қылмыстық жауапкершілікке тарту үшін криминалистикалық зерттеулер жасалуы тиіс. Цифрлі криминалистика компьютерлік дәлелдемелерді сақтау, сәйкестендіру, алу және құжаттау процесі ретінде анықталады. Бұл компьютер, ұялы телефон, сервер немесе желі сияқты сандық ақпарат құралдарынан дәлелдер табу туралы ғылым. Ол сарапшылар тобына сандық технологияларға қатысты күрделі істерді шешудің ең жақсы әдістері мен құралдарын ұсынады.

Цифрлі криминалистика тұрғысынан электронды ақпаратты тасымалдаушылардың бірнеше топтары ерекшеленеді, олар типтеріне және түрлеріне қарай қылмыстық, әкімшілік, азаматтық сот істерін де заттай дәлелдемелер ретінде қолданылады. Кәдімгі (дәстүрлі) құжаттардан айырмашылығы, компьютерлік ақпарат өзінің объективті көрінісінің кез келген түрінде арнайы материалдық тасымалдаушыларсыз бола алмайтындығына байланысты, олар көбінесе заттай дәлелдемелер ретінде әрекет етеді. Сонымен бірге, олардың жеке электронды модульдері жұмыс кезінде қоршаған кеңістікке қосымша криминалистикалық маңызы бар компьютерлік ақпаратты шығарады, оны тиісті электронды немесе басқа арнайы бағдарламалық-аппараттық кешендер арқылы қашықтықтан анықтауға және тіркеуге болады. Кейіннен ол компьютерлік бағдарламалар мен электронды-цифрлық құрылғылардың көмегімен таратып жазылуы немесе адам оқи алатын түрде ұсынылуы немесе қандай да бір ерекше белгілермен кодталуы мүмкін[2].

Ақпараттың электрондық тасымалдаушысы материалдық зат, оның ішінде кеңістікте және уақытта компьютерлік ақпаратты жазуға, тіркеуге, сақтауға, жинақтауға, түрлендіруге және беруге арналған техникалық құрылғы. Ақпаратты жазу, тіркеу — бұл кейінгі ақпаратты сақтау үшін ақпарат сигналдарын физикалық сипаттамалардың немесе жазба тасымалдаушысының пішінінің кеңістіктік өзгеруіне түрлендіру процесі. Бұл жағдайда: кез келген ақпаратты құрылымына немесе материалдық тасымалдаушының жадына жазуға болады, жазба контактілі және байланыссыз болуы мүмкін.

Цифрлі криминалистика процесі:

- компьютерлік және онымен байланысты материалдарды тергеу органдарына оларды сотта дәлел ретінде ұсынуға көмектесетін етіп қалпына келтіруге, талдауға және сақтауға көмектеседі;
- қылмыстың себептерін және басты кінәлінің жеке басын анықтауға көмектеседі;
- алынған сандық дәлелдердің бүлінбегеніне көз жеткізуге көмектесетін қылмыс жасалған жерде процедураларды әзірлеу;
- деректерді жинау және көшіру, дәлелдемелер алу және оларды тексеру үшін жойылған файлдар мен жойылған бөлімдерді сандық медиадан қалпына келтіруге мүмкіндік береді;

- дәлелдемелерді тез анықтауға көмектеседі, сонымен қатар зиянды әрекеттің жәбірленушіге тигізетін әсерін бағалауға мүмкіндік береді;

- тергеу процесі туралы толық есеп беретін компьютерлік сараптама есебін құруға ықпал етеді[3].

Әртүрлі ірі жеке компаниялардың немесе Мемлекеттік органдардың, мекемелердің ақпараттық қауіпсіздік орталықтарында жұмыс істейтін мамандар компьютерлік ақпараттың сенімді қорғалуын қамтамасыз ете алмайды, ал кейде өздері бұл ақпаратты қасақана немесе байқаусызда өзгерістерге ұшыратады, бұл «кибер-бұзу» немесе «компьютерлік вирустарды жұқтыру» түрінде бөгде адамдардың араласуына ықпал етті. Сол себепті цифрлі криминалистиканы қандай да бір құпия ақпараттар сақталатын электронды машинкалар немесе ұялы телефондармен жасалатын қылмыстық құқық бұзушылықтардын алдын алу мақсатында қолданған жөн. Тергеу барысында цифрлі криминалистиканың алатын орыны ерекше, сондықтан сандық ақпараттық іздерді әлдеқайда кеңірек қарастырған жөн. Мұндай іздерді біз әртүрлі критерийлер бойынша қарастырамыз. Практикада алынған сандық ақпарат басшылыққа алынады және тергеуші қылмыстық істі объективті тергеуде, қажетті сараптамаларды дұрыс тағайындауда, кінәлілерді анықтауда қолданады. Цифрлі ақпарат көмегімен анықтап оны қолдану арқылы криминалистикалық маңызды ақпаратты тасымалдаушыларды прогрестің арқасында зерттеу жүргізуге цифрлық технологияларды пайдаланамыз.

[1] Вехов В. Б., Зуев С. В. Цифрлі криминалистика. — М., 2021.

[2] Комаров И. М. Кибер кеңістікте жүргізілетін тергеу әрекеттерінің мәселелері // Криминалистикадағы мәселелер / Г. М. Меретуков, В. Д. Зеленский. — Краснодар, 2018.

[3] Фойгель Е. Н. Компьютерлік ақпарат саласындағы қылмыстарды ашу кезіндегі мәселелер. — Иркутск, 2016.

Климова Я. А.,
доцент кафедры криминалистики учебно-научного комплекса по предварительному следствию в органах внутренних дел, кандидат юридических наук
(Волгоградская академия МВД России)

Личность несовершеннолетнего преступника, осуществившего публичные призывы к террористической и экстремистской деятельности, совершенные с использованием сети «Интернет», и возможности «цифровой криминалистки»

В современном мире развитие цифровой экономики, увеличивающаяся популярность различных информационных систем, глобальная цифровизация в целом обусловили развитие тенденции увеличения количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Безусловно, стремительное развитие современных технологий, а также сложившиеся условия пандемии способствовали активной цифровизации всех сфер жизни, в том числе и сферы преступности. Это обуславливается стремительным расширением диапазона и разнообразия видов преступлений с использованием современных информационно-телекоммуникационных технологий и, как следствие, доступности их для несовершеннолетних, являющихся самыми активными пользователями IT-продуктов.

Основной проблемой, влияющей на снижение качества расследуемых уголовных дел данной категории, является отсутствие в настоящее время научно обоснованных разработок криминалистических характеристик и методик расследования новых видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Анализ уголовных дел свидетельствует о том, что значительно увеличилось количество несовершеннолетних, совершающих преступления с использованием современных информационно-телекоммуникационных технологий.

Особое внимание хотелось бы заострить на все большей распространенности среди несовершеннолетних преступников таких видов преступлений как возбуждение ненависти либо вражды, публичные призывы ктеррористической и экстремистской деятельности, совершенные с использованием сети «Интернет».

Анализ уголовных дел дает основание утверждать, что чаще всего рассматриваемые преступления совершают несовершеннолетние в возрасте 14 – 18 лет, как правило, нигде не работающими и не учащимися, реже — учащимися школ, студентами ССУЗов и ВУЗов. Их привлекают громкие лозунги, призывы, внешняя атрибутика, возможность почувствовать себя членом своеобразного «тайного общества», имеющего право безнаказанно творить расправу над «неугодными»[1].

В таких группировках несовершеннолетние участники попадают под влияние «сильного» авторитетного лидера и ими становится легко управлять. Они готовы пойти на совершение любого преступления. Различными неформальными группами несовершеннолетних совершаются многочисленные хулиганства, акты вандализма, а порой даже убийства и избиения граждан, в том числе и иностранных.

Так, резонансное жестокое убийство произошло в ночь на 13 июня 2020 г., после Дня России. Виталий Васильев нанес 20 ножевых ранений 17-летнему гражданину Азербайджана Тимуру Гаврилову, который скончался на месте происшествия. Было установлено, что на протяжении нескольких лет (в том числе являясь несовершеннолетним) Васильев состоял в неформальной организации, где воспитывалась ненависть к людям иной национальности. В результате этого Васильев принял целенаправленное решение убить «нерусского». В настоящее время дело рассматривается в суде[2].

Таким образом, полагаем, личность несовершеннолетнего преступника является важным элементом криминалистической характеристики рассматриваемой группы преступлений. Поскольку современной особенностью проявления экстремизма в молодежной среде, является развитие принципиально новой тенденции: объединению преступных групп несовершеннолетних по «сетевому» принципу, с использованием современных информационных технологий. Это способствует большей мобильности, самостоятельности, автономности, деструктивных групп несовершеннолетних.

Полагаем, что эффективность расследования рассматриваемых преступлений напрямую зависит от применения в процессе доказывания возможностей «цифровой криминалистики». Так, использование в ходе осмотра места происшествия, осмотра предметов и исследования современных криминалистических программных комплексов, таких, как, например, «Мобильный криминалист», «UFED», «BelkasoftEvidenceCenter», позволяет не только получить данные из установленных приложений, программ обмена сообщениями, электронной почты, а также извлечь сведения о геолокации и восстановить удаленную информацию.

В ходе исследования указанное программное обеспечение позволяет создать физический образ устройства, составить графы взаимодействия, провести анализ биллингов операторов сотовой связи. Это способствует установлению совокупности данных о времени публикации поста или отправки сообщения, о месте нахождения, скорости и траектории движения лица в этот момент. Тем самым способствует оперативному установлению личности и местонахождения несовершеннолетнего.

Таким образом, использование возможностей «цифровой криминалистики» видится нам перспективной для успешного установления личности несовершеннолетнего преступника, осуществлявшего публичные призывы к террористической и экстремистской деятельности, совершенные с использованием сети «Интернет».

---

[1] Анализ состояния преступности несовершеннолетних в г. Волгограде за 12 месяцев 2020 г., за первое полугодие 2021 г. (на основании материалов уголовных дел).

[2] ФСБ обвинила школьников в терроризме за планы «взорвать» здание ФСБ в Minecraft. [Электронный ресурс]. — Режим доступа: https://lenta.ru/news/2020/11/20/kansk/ (дата обращения: 10.10.2021).

Коломинов В. В.,
доцент кафедры криминалистики, судебных экспертиз и юридической психологии, кандидат юридических наук
(Байкальский государственный университет, г. Иркутск)

Безопасность биометрических данных

В настоящее время растет потребность в повышении безопасности не только людей, объектов и данных, но и надежности идентификация лиц[1; 2; 3]. Традиционные технологии идентификации (проверка документов, удостоверяющих личность, стандартный доступ системы, основанные на аутентификации по предмету или паролю) теперь на пределе своих возможностей[4; 5; 6, 11]. Повысить надежность идентификации человека способствует биометрическая идентификация. Биометрическая иден-

тификация понимается как наука, которая заинтересована в описании и измерении анатомо-физиологических особенностей и поведенческих черт человека.

Обычно используемые методы биометрических систем включают идентификацию отпечатка пальца, ладони, лица, радужной оболочки глаза, голоса.

Обычными областями использования биометрической идентификации являются: криминология, туризм, таможенное оформление и паспортный контроль, контроль передвижения людей, контртеррористические меры, мониторинг толпы, системы посещаемости и доступа, защита данных, персональные компьютеры и гаджеты и другие источники данных, электронный банкинг, транзакции онлайн-платежей и многое другое[7, 24; 8; 9].

Базовым компонентом системы биометрической идентификации является сенсорный модуль, обеспечивающий сканирование биометрических данных. Основная часть — это модуль принятия решений, который сравнивает биометрические характеристики, определенные в базе данных. Выходом системы биометрической идентификации является интерфейс связи или замок, разрешающий доступ в предоставленное пространство.

Снятие отпечатков пальцев — один из самых известных методов биометрической идентификации. Обычно отпечатки пальцев используются в криминологии. Сейчас они широко используются в коммерческой безопасности. Этот метод основан на идентификации гребня трения пальцев (сосочковые линии). Существует три основных схемы классификации сосочковых линий:

1. Сосочковые линии имеют форму петли. Петля составляет примерно 65 % всех отпечатков пальцев.

2. Сосочковые линии имеют форму круга, овала, спирали с сердцевиной. Формы вихря примерно 25 % всех отпечатков пальцев.

3. Сосочковые линии имеют форму простых дуг. Минимальное количество вхождений — примерно 5 – 10 % от вхождений.

Помимо основных форм сосочковых линий, прерывание или окончание сосочковых линий используется в дактилоскопическом подходе. Эти отметки называются мелкими деталями. Они могут быть в такой форме: начальная / конечная линия, точка, глаз, крюк, мостовые переходы, вилы, ломаные линии, боковая подвеска, прекращение и т. д.

Оптические датчики отпечатков пальцев основаны на отражении или пропускании света. Эти датчики используют разные формы отражения света от линий гребня и пространства между этими линиями. Отраженный свет оценивается с помощью ПЗС-матрицыили датчика CMOS.

Оптический датчик, использующий светопропускание, основан на подсветке пальца от верхней части (от ногтя) и записи датчиком изображения на противоположной стороне.

Принцип этого датчика основан на измерении разницы в емкости между сенсорной пластиной и пальцем.

Зона чувствительности оснащена большим количеством сенсорных микроэлектродов для оценки разницы в емкости между козырьком и углублением в пальце.

Для этого датчика ультразвуковой сигнал передается от передатчика к отпечатку пальца. Захватываются отраженные и деформированные волны вращающимся передатчиком или приемником, которые оцениваются дальше для распознавания линий.

В тепловизионных сканерах отпечатков пальцев в качестве термочувствительного элемента используется небольшой пиродетектор. Принцип этой технологии основан на измерении разницы температур между пиком и впадиной в сосочковых линиях пальца.

Для проверки надежности датчиков отпечатков пальцев используются две основные функции. *Первая* функция, называемая *falseacceptedreads (FAR),* — это коэффициент ложно принятых чтений.

Эта функция может быть определена следующим образом:

$$FAR = N_{FR/} N_{EIA} * 100\ [\%], \quad \textbf{(1)}$$

где:

N_{FR}— количество ложно принятых чтений

N_{IIA}— количество попыток неуполномоченных лиц идентифицировать.

*Вторая*функция*falserejectedreads (FRR)* — это коэффициент ложно отклоненных чтений. Эта функция может быть определена следующим образом:

$$FAR = N_{FR} / N_{IIA} * 100\ [\%], \quad \textbf{(2)}$$

где:

N_{FR}— количество ложно отклоненных чтений

N_{IIA}— количество попыток неуполномоченных лиц идентифицировать.

*Соотношение*между FRR и FAR показано на рисунке 1.

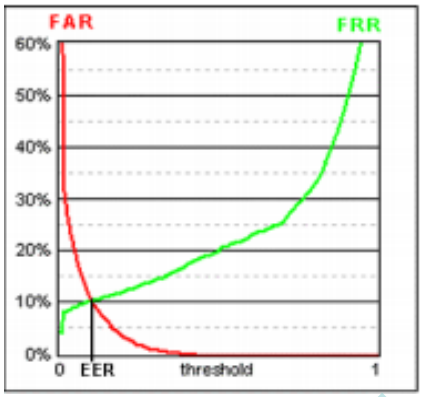


Рис. 1. Связь между FRR и FAR

Точка EER— равная частота ошибок представляет собой точку, в которой FAR и FRR имеют одинаковое значение. Этот переход является*хорошим*показателем общей производительности биометрических устройств. Меньше означает лучшую эффективность EER биометрического устройства.

Существует несколько возможных атак на системы идентификации. Атаки систем идентификации можно разделить на три группы:

- атака системного ввода;
- атака системы оценки;
- атака сложных решений — выходные части.

Для изготовления фальшивых отпечатков пальцев можно использовать два подхода:

1. Для создания поддельного отпечатка пальца можно использоватьнесколько материалов по сохранению папиллярных линий, включая их характер. Для производства можно использовать пластик, этот материал податлив после нагревания. Аналогичными свойствами обладает пластичный материал. Оригинальный отпечаток пальца вдавливается в пластик, таким образом можно сделать шаблон поддельного отпечатка пальца. Шаблон поддельного отпечатка пальца заполнен такими материалами, как желатин, силикон или пластик.

2. Отпечаток пальца можно выделить и сфотографировать или сканировать. Полученное изображение обрабатывается: обрезается, создаются различные оттенки черного и белого, улучшенный материал используется для создания формы. Можно использовать трафаретную печать на пластике или резине.

Обе процедуры могут создавать относительно качественные отпечатки пальцев, но они не имеют длительного срока хранения. Они не могут использоваться сканерами, которые используют контроль яркости. Например, желатин или силикон нельзя наносить на все сенсорные датчики, поскольку некоторые методы не соответствуют свойствам этих материалов, и не являются близкими по свойствам к человеческой коже.

По ложным отпечаткам пальцев измерялась невосприимчивость дактилоскопических датчиков для проверки ложного срабатывания.

На рис. 2 показаны результаты исследований. По отпечаткам пальцев был использован емкостной дактилоскопический датчик. Поддельные отпечатки пальцев изготавливались из штампованной резины (на рисунках обозначены ромбом) и пластика (на рисунках обозначены квадратом). По оси показано число испытаний.

Целью статьи было показать, что системы доступа, использующие отпечатки пальцев, могут быть относительно простым способом взломаны. В этом документе описаны методы, которые можно использовать для создания «поддельного» отпечатка пальца. Чтобы создать эти подделки для отпечатков пальцев можно использовать пластик или резину. Для повышения безопасности необходимо изменить

доступ к системе. Для повышения уровня надежности вместе с отпечатками пальцев необходимо использовать другие биометрические показатели: черты лица, сетчатку глаза, голос.

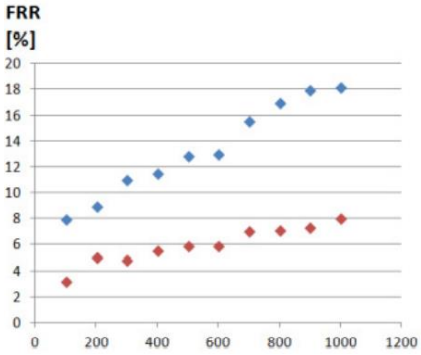


Рис. 2. FRR емкостного дактилоскопического датчика

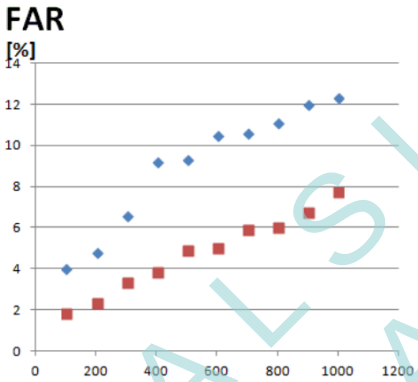


Рис. 3. FAR емкостного дактилоскопического датчика

---

[1] Жмуров Д. В., Поклад В. И. Новые термины в криминологии // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 3. С. 460 – 465.

[2] Кокорева Л. А., Шайтура С. В. Безопасность платежных систем России // Славянский форум. — 2015. — № 1 (7). — С. 92 – 100.

[3] Романова Ю. Д., Шайтура С. В. Безопасность банковских технологий // Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства: Сб. науч. тр. и результатов совместных научно-исследовательских проектов. — М., 2016. С. 527 – 531.

[4] Шайтура С. В. Безопасность банка при работе с электронными деньгами // Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства: Сб. науч. тр. и результатов совместных научно-исследовательских проектов. — М., 2016. С. 556 – 558.

[5] Голкина Г. Е., Шайтура С. В. Безопасность бухгалтерских информационных систем: Учеб. пос. — Бургас, 2016.

[6] Shaitura S. V., Nedkova A. S., Tyger L. M., Goryacheva E. D., Morozova N. O., Berketova L. V. Food security and catering // RevistaTurismoEstudos&Práticas. — 2020. — № S3.

[7] Shaitura S. V., Ordov K. V., Lesnichaya I. G., Romanova Yu. D., Khachaturova S. S. Services and mechanisms of competitive intelligence on the internet // Espacios. — 2018. — T. 39. — № 45.

[8] Shaytura S. V., Minitaeva A. M., Feoktistova V. M., Ordov K. V. Blockchains in spatial data security // CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). — 2019. — P. 70 – 74.

[9] Шайтура С. В., Белю Л. П., Минитаева А. М., Неделькин А. А. Продовольственная безопасность и кейтеринг // Вестн. Курск. гос. сельскохоз. акад. 2020. № 9. С. 103 – 112.

Костенко К. А.,
заведующий кафедрой уголовного права,
криминологии и уголовного процесса, полковник юстиции
(Хабаровский филиал Московской академии
Следственного комитета Российской Федерации);
Костенко И. К.,
магистрант
(Санкт-Петербургский филиал
Всероссийского государственного университета юстиции
(РПА Минюста России)

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НА СТАДИИ ОЗНАКОМЛЕНИЯ ОБВИНЯЕМОГО С МАТЕРИАЛАМИ УГОЛОВНОГО ДЕЛА

Современному следователю невозможно представить свою служебную деятельность без использования современных информационно-коммуникационных технологий, которые призваны решать задачи по эффективной организации информационного и коммуникационных процессов в досудебной стадии уголовного судопроизводства.

Рассматриваемые процессы включают в себя, как методы поиска, сбора, хранения, обработки, предоставления, распространения информации, так и способы осуществления таких процессов и методов[1]. В их числе, как элементарные, связанные с изготовлением печатных текстов документов, снятие с них копий и их сканирование для перевода в различные электронно-цифровые формы, так и имеющие определенный уровень сложности, связанные с использованием специальных программ, например, распознавания текста, голоса или передачи данных по специальным каналам связи и др.

В условиях активно происходящей цифровизации главной целью в следственной деятельности является снижение времени, а также затрат труда, энергии и материальных ресурсов, как для государства, так и для сторон уголовного судопроизводства. В связи с чем на первый план выходят задачи ускорения процесса расследования, сокращения сроков производства по уголовному делу путем использования современной электронной техники.

В рассматриваемом аспекте и в разрезе правоприменения уголовно-процессуального законодательства Российской Федерации (далее также УПК РФ) наиболее значимым, на наш взгляд, является использование современных цифровых и компьютерных технологий при реализации права обвиняемого на ознакомление с материалами уголовного дела (в т. ч. получение его копий).

Право на ознакомление с материалами уголовного дела и получение его копий в России имеет глубокие исторические корни. Еще со времен Императора Александра II в Российской империи по Уставу уголовного судопроизводства 1864 г. (далее также Устав) у обвиняемого существовало право на ознакомление с материалами уголовного дела и получение копий протоколов и постановлений судебного следователя совершенно бесплатно (ст. ст. 475 – 477). Указанная норма в то время имела очень важное значение и авторами Устава рассматривалась как «одно из первых условий правосудия: предоставление подсудимому возможных средств оправдания»[2, 22]. Кроме этого, авторы Устава считали, что открытие доказательств обвиняемому при ознакомлении с материалами уголовного дела позволит окончательно убедить его в бесполезности непризнания им своей вины.

Современная интерпретация данной нормы в уголовно-процессуальном законе 2001 г. более сдержана по своему содержанию (п. 1, 2, ч. 4 ст. 47 УПК РФ), так как, предоставляя обвиняемому право получить копии ряда документов уголовного дела (постановления о возбуждении уголовного дела, о привлечении в качестве обвиняемого и ряда других), фразу «бесплатно» не содержит. Более того, п. 13 ч. 4 ст. 47 УПК РФ о праве обвиняемого с помощью технических средств снимать копии с материалов уголовного дела, возлагает расходы за их получение на самого обвиняемого.

Представляется, что разработчики УПК РФ в большей степени преследовали цели — сэкономить бюджетные денежные средства государства за счет возложения изготовления копий материалов уголовного дела на сторону защиты и в какой-то степени облегчить труд следователя[3]. А выходило ино-

гда все наоборот, защитник с подзащитным затягивали ознакомление с материалами уголовного дела и этим шантажировали следователя, предлагая ему сделать для них его копии. А так как сроки предварительного следствия истекали, то следователю ничего не оставалось, как самостоятельного подготовить копии материалов уголовного дела для обвиняемого и его защитника.

О том, что цели законодателя в полной мере не достигнуты, свидетельствуют и результаты опросов следователей Следственного комитета, прошедших дистанционное обучение на курсах повышения квалификации в Хабаровском филиале Московской академии Следственного комитета в 1 полугодии 2021 г.

Всего было опрошено 35 следователей территориальных следственных органов из различных регионов Дальневосточного федерального округа, в том числе военных и специализированных следственных органов СК России. Ответы на поставленные вопросы оказались достаточно интересны с точки зрения понимания происходящих процессов развития современного предварительного следствия.

Так, по-прежнему наиболее распространенной формой ознакомления с материалами дела остается личное изучение обвиняемым и его адвокатом материалов уголовного дела, об этом сообщили 100 % опрошенных. При этом 34 опрошенных (97,1 %) указали о том, что сторона защиты все чаще использует фотооборудование, в основном встроенное в современные мобильные телефоны — смартфоны (англ. smartphone — умный телефон). При этом, доступ к быстрому получению фотографий, предоставляет возможность стороне защиты без особых затрат получить качественные снимки материалов уголовного дела.

Одиннадцать следователей или 31,4 %, хотя и в единичных случаях, но сталкивались в своей практике с фактами шантажа со стороны защитников обвиняемых, которые, не желая (исключительно за свой счет) снимать копии с материалов дела, готовы были подписать протокол об ознакомлении с делом только в случае если следователь предоставит им полную (или частичную) копию уголовного дела с описью. Такие факты, как правило, имели место, когда срок предварительного следствия или избранной меры пресечения обвиняемому истекали, а дальнейшее продление сроков для следователя было нежелательно. Это понимала и сторона защиты.

По сообщению 27-ми следователей (77,1 % от числа опрошенных) в их практике были случаи, когда в целях ускорения процесса ознакомления с материалами дела и экономии времени, как следователя, так и других участников уголовного процесса электронные сканы отдельных листов материалов уголовного дела направлялись обвиняемому или его адвокатам посредством электронных средств связи, в том числе через электронную почту, различные мессенджеры (WhatsApp, Viber и др.) или записывались на карту памяти (флеш-накопитель), диск, предоставленные стороной защиты.

Таким образом, по итогам проведенного опроса следует признать, что в условиях активно происходящей цифровизации социального пространства, на первый план, безусловно, выходят задачи ускорения процесса расследования и сокращения сроков производства по уголовному делу путем использования современной электронной техники.

В этой связи, на наш взгляд, в ст. 217 УПК РФ законодателю необходимо внести соответствующие изменения, которые бы установили порядок и условия предоставления электронных материалов уголовного дела стороне защиты и ознакомления с ними. Это, открыло бы новые возможности, например: ознакомление с электронными материалами без присутствия следователя в удобное для обвиняемого и его адвоката время, сокращение сроков ознакомления с материалами дела и др. Кроме этого, законодателю также следует определить сокращенные сроки ознакомления с материалами уголовного дела, в случаях, когда обвиняемый и его защитник по электронным каналам связи получили материалы уголовного дела в необходимом для них объеме, позволяющем выстроить свою линию, защиты.

Высказанные подходы исключили бы использование стороной защиты различных «схем» противодействия расследованию путем затягивания ознакомления с материалами дела. Не секрет, что эти «схемы» используются для достижения стороной защиты конкретных целей: «дотянуть до истечения сроков давности уголовной ответственности или до предельного срока содержания обвиняемого под стражей;… и др.»[4, 31]

С учетом этого требуют проработки и дополнительного изучения вопросы предоставления электронной копии в случаях, когда у обвиняемого два и более защитника (ч. 1 ст. 50 УПК РФ разрешает обвиняемому пригласить несколько защитников, а ст. 52 УПК предоставляет ему возможность в лю-

бой момент расследования уголовного дела (или даже рассмотрения его в суде) отказаться от защитника и ходатайствовать о допуске другого).

Необходимо отметить, что Россия всегда была и остается одним из немногих государств мира, где уже не одно столетие право на ознакомление с уголовным делом и снятие с него копий, реализуется в полном объеме, за исключением предоставления копий материалов, составляющих государственную тайну (ч. 2 ст. 217 УПК).

В качестве сравнения, особенно интересны для нас исследования А. Н. Петрухиной, которая, сопоставляя законодательство некоторых европейских стран, констатировала, что например, уголовно-процессуальное законодательство Франции и ФРГ не представляют обвиняемому право знакомиться с уголовным делом на досудебной стадии. Это право предоставлено лишь защитникам. При этом во Франции бесплатно обвиняемый может получить, только достаточно ограниченный перечень документов. Да и в целом в Евросоюзе ограничение в ознакомлении с материалами расследования на досудебной стадии, не считается нарушением принципа равенства сил (заложенного в п. 3 ст. 6 Европейской конвенции по правам человека), что также было признано Европейским судом по делам: «Кремцов против Австрии», Джеперс против Бельгии», «Куруп против Дании». В частности, Европейский суд признает возможность государства ограничить доступ к материалам дела для стороны защиты, даже если они представляют для них особую важность[5, 14 – 15].

На наш взгляд, для России это неприемлемо в принципе. Для нас, как и более 155 лет назад по Уставу уголовного судопроизводства, наиболее важным является предоставление обвиняемому всех возможных средств защиты от выдвинутого в его адрес обвинения. При этом будущее института ознакомления с материями уголовного дела неизбежно связано с расширением способов и средств использования современных инновационных информационно-коммуникационных технологий, что подразумевает в первую очередь полный доступ стороны защиты к электронным материалам уголовного дела, а это позволит существенно сократить время прохождения данной стадии.

---

[1] См.: Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, ст. 2. (с изм. и доп. на 09.03.2021 г.) // Собр. законодательства РФ. — 2006. — 31 июля. — № 31 (часть I). — Ст. 3448.

[2] Устав уголовного судопроизводства. Систематический комментарий. Вып. III. — М., 1914. С. 844. Цит. по: Ворошилова С. В. Правовой статус обвиняемого по судебным уставам 1864 года // Вестник Саратовской государственной юридической академии. 2015. № 2 (103).

[3] Прим. автора.

[4] Костенко К. А. Проблемы теории и практики противодействия затягиванию ознакомления с материалами уголовного дела путем приглашения обвиняемым нового защитника // Российский судья. — 2016. — № 9.

[5] Петрухина А. Н. Проблема реализации права обвиняемого на ознакомление с материалами уголовного дела // Государство и право: теория и практика. — 2017. — № 4 (9).

Күнғожинов Қ. Ә.,
начальник Управления специальных прокуроров
прокуратуры г. Алматы, магистр национальной безопасности
и военного дела, советник юстиции
(Республика Казахстан)

Состояние и перспективы расследования и доказывания транснациональных киберпреступлений

Использование Интернета растет по экспоненте: более 3,8 млрд пользователей по всему миру, что составляет почти 47 % от всего населения планеты. Согласно расчетам, пользователи проводят пять лет жизни в социальных сетях.

Технические методы киберпреступности коренным образом преобразовывают традиционные способы хищений денежных средств и совершения других преступлений.

80 процентов жертв киберпреступности, в правоохранительные органы о преступлении не сообщают. Редкое обращение в правоохранительные органы, объясняются не знанием о виктимизации, испытывают стыд или неловкость, не хотят быть втянутыми в уголовный процесс, так как им не причинен, по их мнению, существенный вред, а корпорации опасаются возможного репутационного риска и т. д.

По данным Комитета по правовой статистике и специальным учетам ГП РК, за период с 2015 г. по 2020 г. в Республике зарегистрировано 23 747 уголовных правонарушений в сфере информатизации и связи, в том числе иных преступлений, совершенных с использованием информационных технологий. В 2015 г. зарегистрировано — 663 преступлений, в 2016 г. — 1 705, в 2017 г. — 2 818, в 2018 г. — 5 101, в 2019 г. — 9 164, в 2020 г. — 4 296.

АО «Государственная техническая служба» в 2015 г. в Республике зарегистрировано 17 621 инцидентов информационной безопасности, в 2016 г. — 19 118, в 2017 г. — 24 584, в 2018 г. — 19 335, в 2019 г. — 20 458, в 2020 г. — 24 053.

За 2020 г. из 24 053 инцидентов ИБ: 4 885 в отношении государственных органов страны, 2 365 — местных исполнительных органов, 950 — критически важных объектов информационно-коммуникационной инфраструктуры, 1 038 — квазигосударственного сектора, 489 — финансового сектора, 14 326 — частного сектора.

В 2015 г. зарегистрировано 663 уголовных дела, а в АО «Государственная техническая служба» зарегистрировано 17 621 инцидентов ИБ. 2015 г. лишь по 3,8 %, от всех инцидентов ИБ, проводились досудебные расследования. В 2016 г. — 8,9 %, в 2017 г. — 11,5 %, в 2018 г. — 26,4 %, в 2019 г. — 44,8 %, в 2020 г. — 17,9 %, что свидетельствует о низкой регистрации киберпреступлений в соотношении с зарегистрированными инцидентами ИБ.

Низкая регистрация киберпреступлений, это лишь одна сторона проблемы в нашей стране. Вторая сторона, которая показывает реальную картину работы правоохранительных органов в раскрытии указанных преступлений, это количество дел, по которым виновные лица привлечены к уголовной ответственности.

Анализ соотношений уголовных дел, по которым виновные лица привлечены к уголовной ответственности из зафиксированных инцидентов информационной безопасности, показывает: в 2015 г. по 152 преступлениям лица привлечены к уголовной ответственности, из них в суд направлено 132, прекращено по нереабилитирующим основаниям 20 уголовных дел, что эквивалентно 0,8 % от всех зарегистрированных инцидентов ИБ за указанный период. По годам картина выглядит следующим образом, а именно в 2016 г. — 78 дел (в суд — 38; прекращено — 40) эквивалентно — 0,4 %, в 2017 г. — 207 (113/94) — 1 %, в 2018 г. — 979 (379/600) — 5 %, в 2019 г. — 1 488 (567/921) — 7,3 %, в 2020 г. — 525 (234/291) — 1 %.

Правоохранительными органами не проводятся достаточные мероприятия, направленные на раскрытие киберпреступлений.

В настоящее время невозможно контролировать киберпреступления, однако необходимо повысить качество расследования указанных преступлений.

АО «Государственная техническая служба» зафиксирована активность хакеров, занимающихся атаками и попытками несанкционированных доступов к компьютерным данным или системам (возможно промышленным шпионажем), в том числе в отношении государственных органов страны. Указанные хакеры после кибератак оставляют свои псевдонимы или «почерк», согласно указанным сведениям можем предположить, что некоторые хакеры являются гражданами нашей страны.

Неожиданным открытием 2019 г. явилось деятельность группы GoldenFalcon (или APT-C-34), которая проводила хакерские операции против частных компаний и государственных организаций Казахстана, вплоть до шпионажа. По предположению специалистов Group-IB за группой стоят спецслужбы Казахстана или лица, заинтересованные в мониторинге обстановки внутри государства.

Быстрый и стремительный рост использования Интернет-ресурсов порождает такой же рост киберпреступлений, что требует увеличения потенциала правоохранительных и специальных органов страны по работе с иностранными и отечественными поставщиками услуг в целях выявления и раскрытия киберпреступлений совершаемых на территории нашей страны и за ее пределами нашими гражданами.

Согласно оценкам Организации Объединенных Наций, свыше 80 % киберпреступлений совершаются в рамках той или иной формы организованной деятельности, включая формирование черного рынка киберпреступности, основанного на цикле разработки вредоносного программного обеспечения, заражения компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи данных и получения денег за финансовую информацию. В развитых странах доля киберпреступлений с транснациональным компонентом, выявляемых правоохранительными органами, как правило, велика, в то время как в развивающихся странах их доля значительно ниже и в некоторых

случаях составляет менее 10 %. С одной стороны, это может указывать на то, что в развивающихся странах киберпреступления ориентированы больше на жертв внутри страны и, возможно, на отдельные национальные компьютерные системы. С другой стороны, вполне возможно, что в связи с недостаточным развитием потенциала правоохранительных органов развивающихся стран менее часто выявляют или работают с иностранными поставщиками услуг или иностранными жертвами преступлений, расследуемых внутри страны.

Повсеместное распространение Интернета и персональных компьютерных устройств означает, что компьютерные системы или компьютерные данные могут использоваться для совершения практически любого уголовного правонарушения. Поэтому сфера цифровых доказательств неразрывно связана с киберпреступностью, хотя и отличается от нее в концептуальном плане. Сбор и представление электронных доказательств являются неотъемлемой частью расследования и судебного преследования киберпреступлений. Кроме того, это все чаще касается традиционных преступлений, таких как грабеж, кража или кража свзломом, а также различных форм организованной преступности. Компьютерные записи телефонных разговоров, электронная почта, журналы IP-соединений, SMS-сообщения, адресные книги мобильных телефонов и компьютерные файлы могут содержать доказательства местонахождения, мотива, нахождения на месте преступления или вовлеченности подозреваемого в преступление в случае практически любого вида преступлений.

Для расследования киберпреступлений правоохранительным органам необходимо использоватькак традиционные, так и новые методы следственно-оперативных мер. В то время как некоторые следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежитпространственный, ориентированный на предметы подход, трудно применять в ситуациях, связанных с хранением электронных данных и потоками данных в режиме реального времени.

В этой связи, в ходе досудебного расследования киберпреступлений необходимо применять новые методы следственно-оперативных мерс принятием компьютерно-ориентированных подходов. В их число могут входить просмотр, изъятие или копирование компьютерных данных, находящихся на принадлежащих подозреваемым лицам устройствах, получение компьютерных данных от третьих сторон, таких как поставщики услуг Интернета, и при необходимости перехват электронных сообщений.

Кроме того, необходимо учитывать такие проблемные аспекты, как неустойчивый характер электронных доказательств и применение злоумышленниками методов запутывания, включая шифрование, использование прокси-серверов, услуг облачного вычисления, «добросовестных» компьютерных систем, зараженных вредоносными программами, и многоадресную (или «луковую») маршрутизацию интернет-соединений. Эти аспекты, в частности, представляют особые трудности в отношении традиционных полномочий.

1. Согласно стандарту, введенному 1 апреля 2020 г. приказом Председателя Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан № 465-од от 13 декабря 2019 г. «Информационные технологии Методы обеспечения безопасности принципы и процессы расследования инцидентов «СТРКISO/IES27043-2019» дано определение: «Цифровое доказательство — информация или данные, хранящиеся или передаваемые в двоичной форме, на которые можно положиться в качестве доказательств». Указанное понятие согласно стандарту «СТРКISO/IES27043-2019» обозначает информацию, снятую с любого электронного носителя.

Поскольку понятие «цифровое доказательство» является более обширным, чем понятие «материалы, содержащие компьютерную информацию», понятие «цифровое доказательство» не ограничивает место только компьютером, а расширяет до любого электронно-цифрового устройства (сетевого оборудования, электронного датчика, смартфона и т. д.).

В этой связи, предлагается применить понятия «цифровое доказательство» в уголовно-процессуальном праве Республики Казахстан. В частности, предлагается внести изменения в Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК.

2. Для удостоверения целостности и неизменности данных электронных носителей информации с момента изъятия рекомендуется (по примеру Соединенных Штатов Америки) определить «стандарт безопасного хеширования», который может использоваться для определения, были ли сообщения изменены с момента их обнаружения и изъятия.

3. Для получения электронных доказательств у заграничных провайдеров услуг органам уголовного преследования, прокурорам и судам предлагается использовать в работе «Практическое Руководство по порядку запроса электронных доказательств из других стран», выпущенное ООН в январе 2019 г. (прилагается к докладу).

Матчанов А. А.,
начальник кафедры организационно-штабной деятельности,
доктор юридических наук, профессор, полковник
(АкадемияМВД Республики Узбекистан, г. Ташкент)

ОБ ОСОБЕННОСТЯХ ПРИМЕНЕНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В ТАКТИКЕ ПОЛУЧЕНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В КРИМИНАЛИСТИЧЕСКОЙ МЕТОДИКЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Быстрое и качественное раскрытие и расследование преступлений зависит от многих факторов, среди которых особое место занимает криминалистическая методика расследования отдельных видов преступлений и тактика проведения следственных действий направленных на получение доказательств. Эти две необходимые составляющие криминалистики в современных условиях претерпевают значительные изменения, связанные с бурным развитием современных информационно-коммуникационных (ИКТ) и иных технологий. Последние оказывают положительное влияние на эффективность тактики собирания доказательств и соответственно на результаты раскрытия и расследования общественно-опасных деяний, среди которых особое место занимают киберпреступления. Криминалистическая методика их расследования и криминалистическая тактика проведения следственных действий и оперативно-розыскных мероприятий имеет актуальный характер в современных условиях.

Термин «киберпреступления» можно воспринимать как общественно-опасные деяния, связанные с совершением преступлений, в сфере информационно-коммуникационных технологий, где сама электронная информация, техника или ресурсы, с помощью которой совершаются преступления, составляют признаки этих противоправных деяний.

Неотвратимость уголовной ответственности за совершения киберпреступлений, по мнению А. У. Расулева, зависит от повышения эффективности борьбы с преступлениями в сфере информационных технологий. При этом он выделяет такое приоритетное направление как обеспечение принципа неотвратимости ответственности за киберпреступления в сфере экономики путем раскрытия их юридической природы[1, 37].

Органы, осуществляющие доследственную проверку, дознаватели, следователи раскрывают и расследуют киберпреступления посредством процессуальных, следственных и оперативно-розыскных действий, которые могут оформляться в процессуальной и не процессуальной формах. При этом они применяют инновационные информационно-коммуникационные технологии, позволяющие значительно расширить диапазон возможностей криминалистической методики и тактики проведения следственных и оперативно-розыскных действий.

Процесс развития и совершенствования ИКТ и распространения в глобальном, международном пространстве посредством информационной интеграции, создал благоприятные условия для совершения киберпреступлений. Это потребовало от органов внутренних дел и других правоохранительных структур создать и оптимизировать методику расследования этих преступлений и тактику проведения следственных действий и оперативно-розыскных мероприятий направленных на получение доказательств, которые имеют несколько специфическую, электронную форму. Так, Н. А. Нугманов среди проблем, связанных с применением информационных технологий, выделят создание правовых условий для электронного документа в качестве доказательств[2, 42].

В методике расследования киберпреступлений особое место уделяется тактическим приемам получения доказательств посредством информационных технологий, которые создали предпосылки для возникновения таких специфических форм как цифровые или электронные доказательства.

Относительно этого Е. С. Ермакова отмечает, что «электронные доказательства легко подвергаются изменениям и мгновенному уничтожению. При этом он выделяет следующие особенности фиксации электронных доказательств: 1) Оперативность; 2) Участие специалиста; 3) Наличие специальных устройств для их записи, сохранения и воспроизведения»[3].

На наш взгляд эти особенности в методике расследования киберпреступлений наиболее полно отражают криминалистическую тактику их получения. При этом следует помнить, об особенностях присущих только этому источнику доказательств, а именно факт формирования цифровых сигналов в виртуальном пространстве.

Опыт методики расследования киберпреступлений в такой развитой информационно-коммуникационной сфере как США показывает, чтодля получения цифровых доказательств были созданы специальные технические группы по их исследованию — TechnicalWorkingGrouponDigitalEvidence (TWGDE), которые впоследствии были преобразованы в единую ScientificWorkingGrouponDigitalEvidence (SWGDE)[4].

В международно-правовом отношении криминалистическая тактика получения и фиксации доказательств в цифровой форме при расследовании киберпреступлений может иметь объективные препятствия, связанные с правовой реализацией их допустимости на территории того государства, где осуществляется расследование. Уголовно-процессуальный порядок обнаружения, изъятия, проверки и признания рассматриваемого вида цифровых доказательств может различаться или не быть урегулирован в нормативно-правовом порядке. Данные обстоятельства должны быть оговорены на уровне двухсторонних или многосторонних договоров при сотрудничестве в методике транснационального расследования киберпреступлений.

По мнению Н. А. Иванова, под цифровыми доказательствами понимаются фактические сведения, полученные с помощью информационно-коммуникационных технологий дискретных сигналов, содержащихся или зафиксированных на компьютерных или иных машинных носителях, изъятую, переданную участниками процесса или полученную иным способом в соответствии с действующим уголовно-процессуальным законодательством[5, 77 – 78].

Одним из основных приемов криминалистической тактики обнаружения и фиксирования цифровых доказательств является изъятие электронных носителей при проведении следственного осмотра, как следственного действия. В этом отношении В. А. Мещеряков, В. В. Трухачев установили особую важность данной криминалистической тактики, отметив, что «арсенал имеющихся процессуальных действий достаточно велик, он все же, с одной стороны, ограничен, исчерпывающим списком, а с другой — в рассматриваемых нами целях фактически сводится к одному единственному следственному действию — осмотру»[6]. Это связано с тем, что осмотр является универсальным следственным действием, в котором восприятие цифровой информации предусматривает наличие определенных технических средств и необходимого программного обеспечения, позволяющего понять сущность информации, выраженной в цифровой форме.

Органы, ответственные за расследование преступлений, не всегда имеют дело непосредственно с физическим электронным носителем информации. Особенность информационных, телекоммуникационных систем выражается в том, чтобы получить соответствующие цифровые доказательства, имеющие значение в методике расследования, не имея физического доступа к месту нахождения информационного носителя. При этом цифровая информация фиксируется в составляемом протоколе осмотра с использованием доступных для пользователей открытых источников, но только в том случае, когда данные размещены на общедоступных машинных, компьютерных или иных информационных носителях[7].

В отличие от осмотра, тактика обыска и выемки являются средством, направленным на возможность активного поиска и принудительного изъятия необходимой доказательственной цифровой информации.

Тактические приемы проведения данных следственных действий выражаются в непосредственном проникновении в помещение, где находятся их машинные, электронные и иные информационные носители. При этом, вышеуказанный вид доказательств может быть зафиксирован на любом материальном носителе, в том числе, полученном в результате применения и использования информационно-телекоммуникационных технологий. В сущности, они материализуются как вещественные доказательства или электронный документ посредством ИКТ, как сведения, представленные в форме цифровых сигналов материальным, машинным (электронным) носителем, независимо от средств их хранения, обработки и передачи. Это могут быть аппаратные и программные средства микропроцессорной техники. При этом доказательственную базу составляет информация, зафиксированная на машинных носителях или на CD-дисках, DVD-дисках, флеш-накопителях (переносимые носители), а также встроенных в средства микропроцессорной, компьютерной или иной инновационной техники.

Таким образом, на основании вышеизложенного, можно сделать вывод, что тактические приемы получения и фиксации цифровых доказательств в расследовании киберпреступлений представляют собой процедуру, сочетающую комплекс мероприятий, связанных с криминалистической методикой и тактикой обнаружения, получения и оценки этих доказательств. Знание и умение на практике применить оптимальную криминалистическую тактику работы с цифровыми доказательствами позволит создать наиболее эффективную и оптимальную методику расследования киберпреступлений.

[1] Расулев А. У. Совершенствование уголовно-правовых и криминалистических мер борьбы с преступлениями в сфере информационных технологий и безопасности: Автореф. дис. … д-ра юрид. наук (DSc). — Ташкент, 2018.

[2] Нугманов Н. А. Теоретико-практические особенности формирования международного информационного права: Автореф. дис. … д-ра юрид. наук (DSc). — Ташкент, 2018.

[3] Ермакова Е. С. Электронные доказательства как новое направление в практике расследования преступлений / Е. С. Ермакова, Д. М. Джумангалиева // Молодой ученый. — 2018. — № 23 (209). — С. 85 – 87. [Электронный ресурс]. — Режим доступа: https://moluch.ru/archive/ 209/51196/ (дата обращения: 05.10.2021).

[4] URL: http://ncfs.org/swgde/ (дата обращения: 05.10.2021).

[5] Иванов Н. А. О понятии «цифровые доказательства» // Вестн. Омск. юрид. ин-та. 2006. № 2 (5).

[6] Мещеряков В. А., Трухачев В. В. Формирование доказательств на основе электронной цифровой информации // Вестн. Воронежск. ин-та МВД России. 2012. № 2. С. 108 – 110.

[7] Карташов И. И. Нетрадиционные источники оперативной информации // Актуальные проблемы деятельности подразделений УИС: Сб. мат-лов открытой науч.-практ. конф. / ФГОУ ВПО Воронежский институт ФСИН России. – Воронеж, 2010. С. 169 – 174.

Махмудов А. М.,
начальник кафедры «Криминалистика»,
доктор философии по праву, доцент, полковник полиции
(Академия полиции МВД Азербайджанской Республики, г. Баку)

НЕКОТОРЫЕ ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

В современное время для проведения правовых реформ,усовершенствования и развития институтов национальной безопасности, атакже усиления информационного обеспечения борьбы с терроризмом, нелегальной миграцией, торговлей людьми и другими видами преступлений и угрозами разрабатываются и применяются новые методы и средства. Формируются биометрические информационные ресурсы с применением новых технологий для идентификации на основании фотографий, отпечатков пальцев, голосов и других персональных биометрических особенностей лиц.

Биометрия является широкой областью исследований, включающей в себя многие аспекты, в том числе правовые, социальные проблемы, а также вопросы экономики, безопасности, поддержания целостности данных и применения крупномасштабных систем[1, 15].

Биометрические данные — это индивидуальные сведения, характеризующие физиологические особенности идентифицированного или идентифицируемого физического лица, дающие возможность однозначно, либо согласованно с другими сведениями идентифицировать его, к которым применяются соответствующие стандарты и которые отражаются на материальных носителях.Биометрические данные собираются по следующим сферам деятельности: оформление удостоверяющих личность документов; миграционный и пограничный контроль; обеспечение информационной безопасности и регистрация средств электронной подписи; разведывательная, контрразведывательная и оперативно-розыскная деятельность; спасательные работы, связанные с чрезвычайными ситуациями; формирование национального банка ДНК; охрана общественного порядка и охрана объектов специального режима;уголовное преследование. Биометрические технологии также используются в области безопасности банковской деятельности, инвестирования и других финансовых перемещений, а также розничной торговле, охране правопорядка, вопросах охраны здоровья, а также в сфере социальных услуг[2].

Согласно Закону Азербайджанской Республики «О биометрической информации» от 13 июня 2008 г.[3] биометрические технологии применяются при осуществлении ряда мероприятий. Среди них можно указатьна некоторые: из них снятие, сбор и регистрация в электронном формате изображений лица, сетчатки глаз, создание, идентификация и верификация изображений с помощью фоторобота;

распознавание лица в толпе путем видеонаблюдения; снятие, сбор и регистрация в электронном формате отпечатков пальцев рук и ладоней, их идентификация и верификация; снятие, сбор и регистрация в электронном формате фрагментов голоса, их идентификация и верификация; анализ фрагментов голоса и его акустических параметров; конвертация информации из звукового формата в формат электронного текста, озвучивание текста; снятие, сбор и регистрация в электронном формате копий почерка и подписи на бумаге, их идентификация и верификация; анализ почерка; анализ ДНК, сбор и регистрация результатов анализа в электронном формате, идентификация лица.

Как известно, биометрия — это вся информация, которая характеризует физиологические и биологические особенности человека, на основании которых можно установить его личность, что может способствовать идентификации личности[4].

На современном этапе развития науки распознавания людейпо одной или более физическим или поведенческим чертам имеетважноезначение в деятельности правоохранительных органов.Идентификация личности человека в основном изучается наукой криминалистики. А также ускорением темпов разработки и совершенствования новых технологий, криминалистика по-прежнему нуждается в расширении спектра технологий, методов и методик, позволяющих автоматизировать процесс идентификации человека. В основе биометрии лежит идентификация конкретного человека, только ему присущим характеристикам, которые могут ориентироваться как на неизменные, так ина динамические, то есть меняющиеся свозрастом или приобретенные параметры. Биометрическая идентификация — это процесс сравнения между данными человека и его биометрическим параметром.

Привлечение новейших достижений биометрии в сферу правоприменительной деятельности при расследовании преступлений позволяет решать ряд идентификационных, но и неидентификационных задач. Из них более распространенным является использование дактилоскопической информации в борьбе с преступностью. Основной наиболее предпочтительной и приоритетной автоматизированной дактилоскопической информационной системой является АДИС, которой ведется Главном Управлением Оперативной и Статистической Информации, Управлением Криминалистических Исследований МВД Азербайджанской Республики. Система АДИС предоставляет следующие возможности:ввод и хранение в базе данных электронных дактилоскопических карт, включающих в себя: текстовую информацию, отпечатки пальцев и ладоней, контрольные оттиски;ввод и хранение в базе данных следов пальцев рук и ладоней, изъятых с мест по нераскрытым преступлениям;автоматические поиски для всех вводимых в базу данных дактилоскопической карты или следа; ведение автоматизированногодактилоскопического учета: получение выборок из базы данных, сортировка списков базы данных, удаление и редактирование записей;просмотр и печать текстовой и графической информации (отпечатки, следы, фотоизображения);взаимодействие с другими видами автоматизированных учетов[5, 39].

Согласно ст. 5 Закона АзербайджанскойРеспублики «О государственной дактилоскопическойи геномной регистрации в Азербайджанской Республике»государственной дактилоскопической регистрации, используются для следующих целей: поиска пропавших без вести лиц, установления личности человека на основании неопознанного трупа,установления личности лиц, которые не способны по состоянию здоровья и в связи с возрастом сообщить информацию о себе и установить личность которых другими способами не представляетсявозможным,предотвращения, раскрытия преступлений и административных проступков и проведения расследования.

Дактилоскопический принцип — самый популярный среди всех биометрических технологий. Дактилоскопия, в отличие от других биометрических технологий, характеризуется наибольшей стандартизацией. Одной из важнейших характеристик любых биометрических систем является их точность. Необходимо отметить, что применения биометрических характеристик отличаются высоким качеством изображения отпечатка. В этих условиях необходима разработка более совершенных методов, обеспечивающих надежность и точность биометрического идентификационного процесса. Идентификация по особенностям папиллярных узоров пальцев рук человека в настоящее время осуществляется в автоматическом режиме. Для этого, наряду с традиционным получением окрашенных отпечатков пальцев на бумаге, используется оптическое сканирование узора пальца руки, который прикладывается к поверхности сканера.Контроль за полнотой и достоверностью информации, направляемой в целяхгосударственной дактилоскопической регистрации и (организации) или соответствующего структурного подразделения, регистрации генома, осуществляет руководитель государственного органа направившего информацию[6].

Недостаток такой технологии в том, что качество получаемого изображения зависит от состояния кожи человека. Если она влажная или сухая, то отпечаток может быть расплывчатым или бледным и, соответственно, непригодным. В перспективе могут использоваться ультразвуковые сканеры, с помощью которых изображение получается бесконтактно[7].

Закон Азербайджанской Республики «О государственной дактилоскопической и геномной регистрации в Азербайджанской Республике» устанавливает правовые основы превентивного получения, хранения и использования для идентификации личности человека геномной информации отдельных категорий гражданреспублики, иностранных граждан и лиц без гражданства в целях повышения эффективности борьбы с преступностью. Обязательную государственную геномную регистрацию проходят следующие лица: лица, подозреваемые, обвиняемые в совершении тяжкого или особо тяжкого преступления, а также преступления против половой неприкосновенности лица и половой свободы или осужденные за совершение подобного преступления; лица, которые не способны по состоянию здоровья и в связи с возрастом сообщить информацию о себе и установить личность которых другими способами не представляется возможным; биологические родственники без вести пропавших лиц; неопознанные трупы и ихбиологический материал.

Таким образом, указанный закон значительно ограничивает количество лиц, подлежащих обязательной государственной геномной регистрации. Однако практика показывает, что в ходе раскрытия и расследования преступлений значительная часть поступающего для исследования биологического материала принадлежит лицам, не подлежащим обязательной государственной геномной регистрации.

Изложенное выше в совокупности свидетельствует о том, что положения ст. 14 Закона Азербайджанской Республики «О государственной дактилоскопической и геномной регистрации в Азербайджанской Республике»регулирующей вопросы обязательной государственной геномной регистрации, не соответствуют реальным потребностям правоохранительных органов в борьбе с преступностью и обеспечении общественной безопасности. По нашему мнению, ст. 14 указанного закона целесообразно изложить следующей редакции: Лица, подозреваемые в совершении преступления, обвиняемые в совершении преступления, осужденные за совершение преступлений, подвергнутые административному аресту, а также совершившие административное правонарушение, если их генетический профиль установлен при проведении оперативно-розыскных мероприятий и следственных действий. Это позволит эффективно использовать полученную в ходе производства экспертиз и исследований геномную информацию в раскрытии и расследовании преступлений.

Исследование материалов биологического происхождения при проведении ДНК имеют большое значение в сборе биометрических данных. Поскольку преступления против личности и собственности обычно хорошо планируется и организуется, и потому на месте происшествия редко можно найти традиционные следы (пальцы рук и ног). В связи с этим еще более важно выявить на месте происшествия материалы биологического происхождения и идентифицировать их с помощью биологических исследований. Это метод исследования ДНК, который отличается своей точностью при исследовании биологических материалов и играет важную роль в идентификации.Помимо идентификации людей по их индивидуальным характеристикам, это исследование позволяет определить кровное родство, сексуальную ориентацию, принадлежность к одному и тому же человеку, наличие или отсутствие наследственных заболеваний и т. д. Материал биологического происхождения, использованный в исследовании, включает кровь, сперму, слюну, пот и другие выделения тела, волосы, ногти, кости, микроскопический зуд внешних слоев тела и т. д.

ДНК-исследования могут проводиться по следующим направлениям: идентификация;опознание неизвестных трупов;исследование различных биологических следов, снятых с места происшествия;идентификация отдельных частей тела и идентификация неопознанных трупов; другие исследования (определение родственных отношений и др.).

Поскольку метод тестирования ДНК отличается от других методов своей чувствительностью, любое загрязнение (контаминация) может существенно повлиять на результаты. Во избежание таких случаев: лицо, осматривающее место происшествия, должно быть в специальной одежде (шляпа, маска, перчатки и халат);использовать чистую одноразовую прнадлежностей; использованные инструменты следует заменить или простерилизовать 70 %-ным медицинским спиртом при удалении другого биологического материала; образцы биологического происхождения в процессе сбора и упаковки должны быть упакованы отдельно после сушки при комнатной температуре, защищены от сол-

нечного света бумажными конвертами или бумажными коробками, а также не должна нарушаться целостность упаковки при разрезании и прокалывании предметов; со слизистой оболочки полости рта в качестве биологического образца от лиц, причастных к происшествию следует обязательно изъять образцы, а в случае выявления инфекционных заболеваний провести надлежащий учет; кровь для сравнительного исследования следует сдавать только в уполномоченном медицинском учреждении; все полученные биологические материалы необходимо хранить при +4°С (в холодильном контейнере) и доставить в лабораторию ДНК не позднее, чем через 24 часа[8, 339].

Необходимо отметить, что в областибиометрических технологий в данный моментимеются определенные проблемыкоторые постепенно разрешаются: это — дороговизна, неуниверсальность, чувствительность к обману, совершенствование нормативной базы.

К изложенному добавим: для того, чтобы в полной мере использовать возможности биометрии в деятельности правоохранительных органов необходимо совершенствовать поиск и разработка носителей информации о биометрических данных человека и возможностей их последующей фиксации и использования правоохранительными органами.

По мнению некоторых авторов, можно с уверенностью говорить о том, что создание всеобщей геномной регистрации, очевидно, успешно обеспечит борьбу с международной преступностью,хотяэто очень затратное мероприятие с финансовой точки зрения.

Инновационное применение новейших средств раскрытия преступлений требует специальных знаний целого комплекса различных наук (юридических, медицинских, биологических, технических и пр.), что вызывает определенные сложности в ментальном восприятии этих юридико-технических новаций.

---

[1] Безмалый В. Парольная защита: прошлое, настоящее, будущее // Компьютер пресс. — 2008. — № 9.

[2] Закон Азербайджанской Республики «О государственной дактилоскопической регистрации в Азербайджанской Республике» от 22 февраля 2000 г. № 816-IQ. // Азербайджан. 2000. 24 марта («LegalActs» LLC). С поправками согласно Законам от 27 октября 2009 г. № 900-IIIQD; 6 октября 2015 г. № 1346-IVQD («LegalActs» LLC).

[3] Закон Азербайджанской Республики «О биометрической информации» от 13 июня 2008 г.

[4] URL: https://ru.wikipedia.org/wiki.

[5] URL: https://fond-ai.ru/art1/art228.html.

[6] Правила проведения государственной дактилоскопической и геномной регистрации в Азербайджанской Республике» от 16 января 2019 г. Q 12-001-19.

[7] Байрбекова Г. С., Нугманова С. А., Мазаков Т. Ж. Анализ динамики научных публикаций по биометрическим методам в компьютерных технологиях в базе данных WebofScienceCoreCollections. Федеральное агенство научных организаций. Всероссийский институт научной и технической информации Российской Академии Наук (ВИНИТИ РАН). Серия 1. Организация и методика информфционной работы: Ежемесячный научно-технический сборник. № 4. С. 29 – 33.

[8] Махмудов А. М., Алиев Б. А. и др. Криминалистическая техника: Учеб. пос. — Баку, 2016.

Мельников Е. Б.,
начальник кафедры криминалистики,
кандидат химических наук, доцент
(Сибирский юридический институт МВД России, г. Красноярск)

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ В СИСТЕМЕ КРИМИНАЛИСТИЧЕСКОЙ ТЕХНИКИ

Развитие криминалистической техники как раздела науки криминалистики неразрывно связано как с появлением новых ее отраслей, так и развитием уже существующих. Глобальный процесс интеграции и дифференциации криминалистических знаний затрагивает и отрасль криминалистической техники, которую стали включать в ее систему относительно недавно, хотя исследования подобного рода проводились в ходе раскрытия и расследования преступлений еще на этапе становления криминалистики как науки. Речь идет об исследовании материалов, веществ, изделий, представленном широким кругом видов криминалистического исследования, реализуемых на основе методов изучения субстанциональных признаков. Среди более чем десятка видов таких исследований особое место занимает криминалистическое исследование наркотических средств (далее — НС) и психотропных веществ (далее — ПВ). Выделение отдельных направлений в самостоятельные отрасли (подотрасли) криминалистической техники обычно происходит в соответствии с несколькими критериями, одним из кото-

рых является уровень сформированности частного криминалистического учения, составляющего теоретическую основу той или иной отрасли криминалистической техники. В настоящее время криминалистические знания в области исследования НС и ПВ интегрированы в отрасль криминалистической техники «Криминалистическое исследование материалов, веществ изделий» (далее — КИМВИ). В связи с этим вопрос о возможном выделении криминалистического исследования НС и ПВ в самостоятельную подотрасль КИМВИ представляется актуальным, в первую очередь в аспектах формирования частного криминалистического учения в данной области и практической значимости соответствующего вида исследований в правоохранительной деятельности.

Несмотря на то, что экспертные исследования НС и ПВ проводятся уже достаточно долгое время, эту область криминалистических знаний нельзя назвать достаточно разработанной. В литературе имеются лишь единичные публикации, свидетельствующие о зарождении в системе криминалистики нового частного криминалистического учения — «Криминалистическое нарковедение»[1]. С другой стороны, криминалистическое исследование НС и ПВ стало фигурировать как подотрасль криминалистической техники в некоторых учебных курсах криминалистики[2, 356]. Попытка обобщить и систематизировать накопленные знания в области криминалистического исследования НС и ПВ была предпринята П. А. Ивановым и др.[3, 120] Наличие данного вида исследований в структуре криминалистического исследования материалов, веществ и изделий показано в работах М. Б. Вандера[4, 67], Ю. Г. Корухова[5, 96], В. С. Митричева и В. Н. Хрусталева[6, 591]. Это свидетельствует о начале формирования новой области криминалистических знаний, связанных с исследованием специфической группы объектов — наркотических средств, психотропных и сильнодействующих веществ, их прекурсоров и аналогов. Необходимость выделения этой области в отдельную отрасль криминалистических знаний обусловлена следующими основными факторами:

1) широким распространением исследования НС и ПС в практической деятельности экспертно-криминалистических подразделений правоохранительных органов;

2) многообразием контролируемых веществ, обладающих психоактивным действием, и их прекурсоров, характеризующихся широким спектром свойств, значимых для определения их природы;

3) большим количеством способов изготовления НС, ПВ и их аналогов.

Однако активный процесс формирования отрасли, имевший место в начале 2000-х годов, ощутимо замедлился в последнее десятилетие. Это связано с несколькими обстоятельствами. Во-первых, с качественным изменением структуры незаконного оборота наркотических средств, характеризующимся резким увеличением доли синтетических наркотиков. Во-вторых, с лавинообразным увеличением количества контролируемых веществ в 2010 – 2015 годы, сопровождавшимся отставанием в своевременной разработке методик их экспертного исследования, а также методик по исследованию аналогов наркотических средств; эта проблема не решена до настоящего времени. В-третьих, с необходимостью разработки новых способов обнаружения, фиксации и изъятия объектов криминалистического исследования при расследовании преступлений, связанных с бесконтактным сбытом наркотических средств. Таким образом, процесс формирования отрасли — в аспекте создания базового криминалистического учения — с этапа теоретического осмысления вернулся на этап накопления эмпирического материала, что потребует в ближайшем будущем активных научных исследований в этой области.

Современный процесс расследования преступлений в сфере оборота наркотических средств без использования достижений науки криминалистики абсолютно невозможен. Достижения криминалистической техники, развитие современных методик вкупе с эффективным использованием законодательства правоприменителем способны на более высоком качественном уровне обеспечивать борьбу с преступлениями в сфере незаконного оборота наркотиков. В последние десятилетия наука криминалистика поступательно развивается как в фиксации, так и в исследованиях наркотических и психотропных веществ. Последние проводятся в рамках экспертизы, которая в соответствии с приказом МВД России[7] называется исследованием наркотических средств, психотропных веществ и их прекурсоров, сильнодействующих и ядовитых веществ и входит в родовую группу экспертиз материалов, веществ и изделий. Вместе с тем исследования основных видов объектов, перечисленных в названии экспертизы, достаточно сходны как в методическом плане, так и применяемыми инструментальными методами и техническими средствами. Следует отметить, что практическое использование столь длинного наименования для обозначения конкретного вида криминалистического исследования в сфере профессионального общения крайне неудобно, и в среде специалистов оно чаще всего фигурирует как «экспертиза НС и ПВ» и подразумевает исследование всех категорий объектов.

Таким образом, на современном этапе развития говорить о завершении процесса формирования новой отрасли криминалистической техники — криминалистического исследования наркотических средств и психотропных веществ — было бы преждевременно. Несмотря на широкое распространение исследований НС и ПС в практической деятельности экспертно-криминалистических подразделений правоохранительных органов, в настоящее время формирование соответствующего частного криминалистического учения скорее находится на этапе накопления эмпирического материала, чем на этапе его теоретического осмысления.

---

[1] Кузьминых К. С. Криминалистическое нарковедение // Вестник криминалистики / Отв. ред. А. Г. Филиппов. Вып.1. — М., 2000. С. 52 – 62.

[2] Криминалистика: Учебн. для вузов / Под ред. А. А. Закатова, Б. П. Смагоринского. — М., 2003.

[3] Криминалистическое исследование наркотических средств, психотропных и сильнодействующих веществ: Учеб. пос. / П. А. Иванов [и др.]. — М., 2004.

[4] Вандер М. Б. Криминалистическая экспертиза материалов, веществ и изделий. — СПб, 2001.

[5] Современные возможности судебных экспертиз / Под ред. Ю. Г. Корухова [и др.]. — М., 2000.

[6] Митричев В. С. Основы криминалистического исследования материалов, веществ и изделий из них. — СПб., 2003.

[7] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»): приказ МВД России от 29 июня 2005 г. № 511.

Мещеряков В. А.,
профессор кафедры криминалистики,
доктор юридических наук, профессор
(Воронежский государственный университет);
Цурлуй О. Ю.,
доцент кафедры судебной экспертизы
и криминалистики, кандидат юридических наук, доцент;
Фурсов В. В.,
старший преподаватель
кафедры судебной экспертизыи криминалистики
(Центральный филиалРоссийского государственного
университета правосудия, г. Воронеж)

ОСОБЕННОСТИ ИДЕНТИФИКАЦИИ УЧАСТНИКОВ СУДЕБНОГО РАЗБИРАТЕЛЬСТВА УГОЛОВНЫХ ДЕЛ В ФОРМАТЕ ОНЛАЙН

Активное внедрение цифровых технологий в уголовное судопроизводство в большей степени осуществляется посредством рассмотрения уголовных дел в формате онлайн. Судебное разбирательство с использованием веб-конференции проводится с соблюдением регламентированных уголовно-процессуальным законом общих правил, но вместе с тем имеет ряд особенностей, требующих на наш взгляд законодательного закрепления.

Использование в судебном процессе видеоконференцсвязи упрощает участие в судебном заседании эксперта (специалиста), в случае необходимости его допроса в судебном заседании, проводимом в ином населенном пункте или регионе, чем местонахождение эксперта (специалиста). Соответственно для участия в судебном заседании эксперта (специалиста) в очном формате необходимо решить вопрос об оформлении командировочных документов, компенсации расходов на транспорт, питание и, возможно, проживание, изменении графика работы. Помимо этого, например, эксперт государственного экспертного учреждения, относящегося к силовому ведомству (МВД РФ, СК РФ, ФСБ РФ) может на момент рассмотрения дела в суде находится в длительной служебной командировке. Таким образом, онлайн формат позволяет избежать перечисленных для эксперта, экспертного учреждения, работодателя затруднения и неудобства.

В настоящее время в соответствии с требованиями ГПК РФ и УПК РФ идентификация личности, участвующей в судебном заседании в онлайн формате, осуществляется судом по месту нахождения участника процесса (свидетеля, эксперта, специалиста, переводчика и т. д.). Авторами данной статьи

рассматриваются иные варианты идентификации личности, исходя из современных технических возможностей.

Несомненно, наиболее значимой проблемой, с которой сталкивается суд при допуске к участию в судебном заседании лица посредством веб-конференции, на наш взгляд, является именно идентификация участника процесса.

С момента внедрения возможности рассмотрения дел онлайн, суды применяли следующие способы идентификации:

1. Сопоставление лица с демонстрируемым им паспортом. К такому способу прибегли судьи Верховного суда РФ при первом рассмотрении вышеупомянутого гражданского дела № 60-КГ20-2 в онлайн формате. Председательствующий попросил стороны назвать полные фамилию имя отчество и показать в камеру документ, удостоверяющий личность.

2. Использование программного обеспечения, позволяющего производить распознавание лиц по элементам и признакам внешности, например, на основе нейросетей. Данный опыт имел место в Московском городском суде 2 июня 2020 г., когда впервые состоялось онлайн заседание по рассмотрению апелляционной жалобы по делу об административном правонарушении, с использованием биометрической системы распознавания лиц на основе нейросетей, совместного пилотного проекта с компанией «Крок». Обученные нейросети могут распознать человека по фотоснимку, загруженному в базу данных. При этом достаточно 30 % видимости лица, т. е. распознавание возможно при смене прически, наличииимедицинской маски и т. д. Видеопоток постоянно анализируется во время заседания. «Если освещение хорошее, а человек сидит лицом к камере, корректность распознавания лиц равна 98 %», — отметил А. Болотов, руководитель по работе с корпоративными клиентами компании «Крок»[1]. Подключение участников к сервису видеоконференцсвязи суда осуществилось после авторизации на портале судов общей юрисдикции столицы.

3. Идентификация участников судебного разбирательства возможна на сегодняшний день через портал Госуслуг, в котором зафиксированы персональные данные граждан.

В апреле 2021 г. Правительством Российской Федерации внесен в Государственную думу и в июне текущего года принят в первом чтении проект № 1144921-7 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования дистанционного участия в судебном процессе» (далее — Законопроект). Положения данного законопроекта предлагают внесение изменений в процессуальное законодательство России, регламентирующее гражданское, арбитражное и административное судопроизводство. Анализ Законопроекта позволяет высказать мнение о возможности использования ряда содержащихся в нем положений о порядке рассмотрения судами гражданских, арбитражных и административных дел, в рамках уголовного судопроизводства.

В частности из текста Законопроектаследует, что законодатель предлагает для арбитражного, гражданского и административного судопроизводства производить «установление личности субъекта судопроизводства при его участии в судебном заседании путем использования системы веб-конференции с использованием информационно-технологических средств, обеспечивающих идентификацию лица без его личного присутствия (единой системы идентификации и аутентификации, единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации)». В Концепции информатизации Верховного суда Российской Федерации, утвержденной приказом Председателя Верховного Суда Российской Федерации от 15 февраля 2021 г. № 9-П справедливо отмечено, что технологии дистанционной биометрической аутентификации позволяют организовать проведение судебных заседаний с дистанционным участием в них одного или всех участников судебного процесса без привлечения второго суда, оказывающего содействие в проведении судебного заседания с дистанционным участием, с использованием технологии веб-конференции. Внедрение в судебную деятельность технологии биометрической аутентификации участника судебного заседания по лицу и голосу находит определенную поддержку в среде специалистов[2, 105].

Приведенное выше положение Законопроекта предлагается внести в качестве дополнений в ст. 56 АПК РФ, в ст. 177 ГПК РФ, в ст. 160 КАС РФ, дополнить им отдельную ст. 153.2 АПК РФ, ст. 155.2 ГПК РФ, ст. 142.1 КАС РФ.

На наш взгляд аналогичное положение может найти свое отражение в нормах глав 35, 37 УПК РФ, регламентирующих общие условия судебного разбирательства и порядок проведения судебного следствия.

Нормы Законопроекта уполномочивающие суд, рассматривающий дело, отбирать подписку у свидетелей, экспертов, переводчиков, участвующих в судебном заседании путем использования системы веб-конференции, о разъяснении им их прав, обязанностей и ответственности, в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, по аналогии с положениями ст. 474.1 УПК РФ могут быть внесены в соответствующую норму главы 36 УПК РФ.

Следует отметить, что арбитражные суды достаточный период времени активно рассматривают дела онлайн. К участию в судебном онлайн-заседании допускаются только пользователи, имеющие учетные записи, подтвержденные в единой системе идентификации и аутентификации. Получение соответствующих учетных записей осуществляется в порядке, предусмотренном Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утвержденными постановлением Правительства РФ от 10 июля 2013 г. № 584. Лицо, участвующее в деле в формате онлайн, равно как и его представитель, подает в арбитражный суд ходатайство, заполняя соответствующуюэлектронную форму в информационной системе «Мой Арбитр», прикладывая к ходатайству копию паспорта. Представителю лица необходимо приложить к ходатайству помимокопий паспорта и диплома, копию доверенности или иного документа, подтверждающего полномочия о представлении интересов участника. Для подключения к онлайн-заседанию необходимо использовать интернет-браузер GoogleChrome. Иной специальной программы не требуется.

Изложенное подтверждает отлаженную процедуру проведения онлайн судебных заседаний по рассмотрению арбитражных дел.

Корректная идентификация участников судопроизводства возможно при создании учетной записи, привязанной к порталу Госуслуг, на сайте суда, а также установке в судах программного обеспечения по распознаванию лиц по элементам и признакам внешности на основе нейросетей. Данная процедура вполне реальна, однако требует материальных затрат и времени.

В заключении отметим, что современное судопроизводство имеет техническое обеспечение, практический опыт и перспективу законодательной регламентации надежной и качественной системы идентификации участников процесса при рассмотрении дел с использованием веб-конференции. Очевидно, что уголовный процесс представляет собой особенную и весьма специфическую форму судопроизводства, но при этом он все же не исключает возможности активного использования современных информационных технологий как в целях криминалистического обеспечения судебной деятельности по рассмотрению и разрешению уголовных дел, так и для рациональной организации таковой.

[1] URL: https://zasudili.ru/news/mosgorsud-vpervye-provel-onlayn_zasedanie-s-raspoznavaniem-lits/ (дата обращения: 04.11.2021).

[2] Шереметьев И. И. Использование современных цифровых технологий при судебном разбирательстве уголовных дел в дистанционном режиме // Вестн. Ун-та им. О. Е. Кутафина (МГЮА). 2020. № 10.

Овсянников В. В.,
старший преподаватель кафедры криминалистики
(Барнаульский юридический институт МВД России)

НЕКОТОРЫЕ АСПЕКТЫ УСТАНОВЛЕНИЯ И РОЗЫСКА ЛИЦ, ПРИЧАСТНЫХ К СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЯ, В УСЛОВИЯХ СОВРЕМЕННОСТИ

Согласно статистическим данным за 12 месяцев 2020 г. из 2 044,2 тыс. зарегистрированных преступлений, не раскрыто 963,8 тыс. преступлений. Остались нераскрытыми 316 убийств и покушений на убийство, 698 фактов умышленного причинения тяжкого вреда здоровью, 9,1 тыс. грабежей, 637 разбойных нападений. По итогам 2020 г. остались нераскрытыми 941,4 тыс. преступлений в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого[1].

В настоящее время, в условиях еще пока продолжающейся пандемии коронавируса COVID – 19, в ряде регионов, отмечается увеличение количества совершенных контактных преступлений с использованием медицинских масок, используемых преступниками с целью сокрытия своего внешнего облика.

Отметим, что личностная информация, характеризующая человека, в том числе, сведения об особых его приметах, еще в глубокой древности использовались для розыска лиц, совершивших преступление[2, 18; 3, 34]. В последующем, некоторые аспекты криминалистического учения о внешнем облике нашли свое отражение в трудах ученых, стоящих у истоков развития криминалистики: А. Бертильона, И. И. Ганна, Г. Гросса, К. Г. Прохорова, Н. В. Терзиева и др.

В настоящее время криминалистическое учение о внешнем облике человека заняло надлежащее место в числе частных криминалистических теорий (учений). Содержащиеся в нем выводы и рекомендации служат своеобразной методологической основой для разработки тактических и методических положений производства ряда следственных действий поисково-познавательного характера. Кроме того, они представляют практический интерес для сотрудников правоохранительных органов, задействованных в установлении лиц, причастных к совершению преступления, а также в розыскной деятельности субъекта, осуществляющего предварительное расследование.

О востребованности положений рассматриваемого частного учения, в том числе, свидетельствует возрастание числа специальных работ, посвященных формированию либо совершенствованию методик расследования преступлений, в которых задействуются некоторые положения габитоскопии.

В тоже время существующая на данный момент практика составления субъективных портретов свидетельствует о том, что потерпевшие, свидетели и, в том числе, очевидцы не всегда могут описать внешний облик преступника, а возможности используемых технических средств не позволяют использовать их для изготовления субъективного портрета в таких случаях (когда очевидец, свидетель преступления, не может воспроизвести в своей памяти внешний облик преступника из-за используемых им маскирующих элементов). Так, использование обычной медицинской маски (стандартный размер которой составляет 17,5 на 9,5 см) позволяет скрыть большую часть лица (закрывая собой область от переносицы до подбородка), и практически, приводит к невозможности составления субъективного портрета.

Соответственно, возможно говорить о назревшей потребности правоохранительных органов в разработке современных подходов, методов и средств, позволяющих осуществлять установление и розыск лиц, причастных к совершению преступления.

Так, в Следственном комитете Российской Федерации, уже сейчас, осуществляется разработка программного обеспечения позволяющего создавать 3D-модель лица, даже в том случае, если преступник использовал маску (медицинскую маску). Технология использует наложение полученной 3D-модели лица на размытые фотоснимки (кадры) подозреваемого, запечатленного на видеозаписи.

Следует отметить и относительно новое направление — изучение вопросов взаимосвязи цепи ДНК с фенотипической природой человека.

В настоящее время в области молекулярно-генетических методов наряду с уже привычными для их использования вопросами идентификации личности все большее внимание уделяется решению диагностических задач, связанных с криминалистическим ДНК-фенотипированием.

Криминалистическое ДНК-фенотипирование предполагает прогнозирование некоторых признаков внешности[4], при производстве соответствующих диагностических исследований:

- исследование признаков, связанных с пигментацией[5];
- прогнозирование особенностей морфологии лица[6];
- прогнозирование морфологии ушной раковины;
- прогнозирование роста;
- прогнозирование возраста;
- прогнозирование географического происхождения[7].

В этой связи повышается значение качественного выявления, фиксации, изъятия и сохранения биологических следов, изымаемых в ходе проведения осмотра места происшествия.

Так, в 2020 г. в рамках проводимой межведомственной Стратегической сессии были рассмотрены вопросы внедрения на территории Российской Федерации системы прогнозирования признаков внешнего облика лиц, причастных к совершению преступления, путем изготовления их субъективных

портретов в ходе анализа ДНК (РНК), выделенных с биологических объектов, изъятых с мест нераскрытых преступлений.

Таким образом, использование возможностей диагностических исследований ДНК (РНК) — анализа, в области прогнозирования признаков внешнего облика, безусловно, представляется значимым и перспективным с точки зрения, возможности повышения эффективности раскрытия и расследования различных категорий преступлений.

Отметим, что особая криминалистическая информативность внешнего облика заставляет асоциальное лицо, как в предкриминальной, так и в посткриминальной ситуациях, принимать различные меры затрудняющие распознавание его как индивидуального объекта.

Учитывая, что реконструктивная и пластическая хирургия получили свое широкое распространение только в конце XX — начале XXI вв., в настоящее время, пластическая хирургия и косметические операции имеют массовое распространение, при этом их количество ежегодно увеличивается. Современный период их развития непосредственно связан с микрохирургической техникой замещения дефектов тканей различными аутотрансплантатами[8, 9].

В связи с этим, особого внимания на наш взгляд, заслуживают вопросы рассмотрения закономерностей изменения внешнего облика человека посредством пластической и реконструктивной хирургии, а также косметических (эстетических) операций, требующие от сотрудников правоохранительных органов знания современных методов и средств, используемых в пластической хирургии и косметологии.

Так, современные возможности реконструктивной и пластической хирургии позволяют изменить внешний облик человека практически до неузнаваемости:

- удаляются последствия ряда генетических и приобретенных заболеваний;
- восстанавливаются поврежденные участки мягких тканей, образующиеся при травматическом воздействии (укусы животных, ножевые и огнестрельные ранения, последствия автомобильных травм и т. п.);
- восстанавливаются поврежденные участки костной структуры при переломах;
- выполняется замещение волос;
- удаляются складки и морщины кожи;
- изменяют форму и положение век; размеры, форму и степень раскрытия глазной щели; позволяют удалить (скорректировать) эпикантус;
- липосакция и ритидэктомия лица и шеи;
- липосакция, брахиопластика рук, абдоминопластика живота;
- исправляется форма и степень оттопыренности ушных раковин;
- изменяется длина ротовой щели;
- корректируется ширина и контур каймы губ;
- изменяется форма скул, подбородка.

Приведенный перечень, безусловно, не является исчерпывающим, однако, позволяет составить общее представление о современных возможностях пластической и реконструктивной хирургии, в том числе, о возможностях изменения не только мягких тканей, но и костно-хрящевых элементов. В заключение рассмотрения данного аспекта отметим, что развитие технологий в области пластической хирургии и реконструктивной хирургии, уже в настоящее время, позволяет успешно проводить операции по полной трансплантации лица[9]. А методы рассматриваемых разделов хирургии все чаще используется в преступных целях[10].

Косметические операции, в свою очередь, позволяют выполнять ряд уже указанных выше изменений внешнего облика, при этом, практически не оставляя видимых следов такого оперативного вмешательства.

Особо следует отметить, метод лазерного удаления татуировок. Данный метод появился сравнительно недавно, однако главной особенностью его применения, является удаление татуировки без повреждения эпителиального слоя кожи, т. е. рассматриваемая процедура является не только практически безболезненной, но также не оставляет шрамов и рубцов на коже. Так, татуировка представляет собой частицы красящего вещества, введенного под кожу татуировочной иглой. Использование лазера, при этом, позволяет осуществлять дробление частиц красящего пигмента, обеспечивая его последующее естественное выведение организмом человека через кровеносную и мочевыделительную системы.

Рассматривая дельнейшие перспективы развития учения о внешнем облике человека, отметим, что многие авторы предлагают комплексный подход[11], заключающийся в задействовании различных областей знаний[12], проведения» комплексных консультаций», в том числе, при условии необходимости, и со специалистами в области реконструктивной либо пластической хирургии[13].

В качестве вывода по рассматриваемой тематике следует согласиться с мнением вышеуказанных авторов, отмечающих необходимость комплексного междисциплинарного подхода к вопросам установления и розыска лиц, причастных к совершению преступления, а также к процессу отождествления лиц, внешний облик которых был предположительно изменен посредством реконструктивной либо пластической хирургии. В таких случаях, по нашему мнению, целесообразно привлечение соответствующих специалистов в области реконструктивной либо пластической хирургии как для дачи консультации, так и в случаях проведения медицинского освидетельствования лиц, причастных к совершению преступления, внешность которых предположительно могла быть изменена.

---

[1] Статистика и аналитика // Официальный сайт МВД России. [Электронный ресурс]. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 29.09.2021).

[2] Гейндль Р. Уголовная техника. Из мастерской уголовного розыска / Пер. с нем., под ред. П. И. Люблинского. — М., 1925.

[3] Якимов И. Н. Опознание преступника. — М., 1928.

[4] Перепечина И. О. Некоторые новые возможности ДНК (РНК)-диагностики. / Вестн. экономич. безопасности. 2019. № (2). С. 214 – 219.

[5] Walsh S., et al. Global skin colour prediction from DNA // Hum. Genet., 2017. V. 136. №. 7.

[6] Shaffer J. R., et al. Genome-Wide Association Study Reveals Multiple Loci Influencing Normal Human Facial Morphology. PLOS Genetics, 2016. V. 12. № 8.

[7] Evett I. W., et al. An investigation of the feasibility of inferring ethnic origin from DNA profiles // J. of Forensic Science Society, 1992. V. 32.

[8] Решетов И. В. Реконструктивная и пластическая хирургия опухолей головы и шеи // Практическая онкология. — 2003. — Т. 4. — № 1.

[9] Все о пластике. Человек с тремя лицами: француз перенес 2 лицевых трансплантации. [Электронный ресурс]. — Режим доступа: //http://vseoplastike.ru/articles/detail/373364 (дата обращения: 25.03.2021).

[10] Это не я: как преступники меняют внешность, чтобы остаться непойманными. [Электронный ресурс]. — Режим доступа: //http://ren.tv/news/kriminal/421806-eto-ne-ia-kak-prestupniki-meniaiut-vneshnost-chtoby-ostatsia-nepoimannymi (дата обращения: 29.09.2021).

[11] Смирнова С. А., Эджубов Л. Г., Карпухина Е. С. О некоторых новых возможностях использования комплексного подхода в судебной экспертизе // Теория и практика судебной экспертизы. — 2012. — № 2 (26). — С. 188 – 195.

[12] Пичугин С. А. Концепция комплексного криминалистического исследования признаков внешности человека: Монография. — М., 2014.

[13] Зинин А. М. Некоторые проблемы судебно-портретной идентификации // Теория и практика судебной экспертизы. — 2015. — № 2 (38). — С. 10 – 12.

Ополонина К. Ю.,
старший преподаватель кафедры криминалистики,
магистр юридических наук, подполковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Значение компьютерной криминалистики в раскрытии и расследовании преступлений, совершенных в сфере информатизации и связи

В век информатизации, цифровые технологии проникли практически в каждую сферу деятельности человека. На сегодняшний день становится сложным представить развитие общества и государства без возможностей различных цифровых систем и устройств. Весь мир поглощен информационными технологиями, а человек уже испытывает некие трудности и неудобства в случаях отсутствия в его повседневной жизни интернета, компьютера, смартфона, а также социальных сетей. Нельзя скрыт тот факт, что и преступная деятельность неизбежно развивается в данном направлении — в сфере компьютерных технологий.

На сегодняшний день, настоящей проблемой для правоохранительных органов выступают правонарушители, действующие в киберпространстве — в области взаимодействия информационных систем различного уровня, включающих компьютерные системы, сети, программы и т. п.

При этом достижение успешных результатов в деятельности по раскрытию и расследованию таких преступлений связано с правильным использованием достижений современных научно-технических средств.

С целью повышения эффективности борьбы с киберпреступностью, которая выходит на новый уровень, правоохранительным органам приходится искать новые средства и пути получения и использования доказательственной и ориентирующей информации, в том числе, при помощи цифровых технологий.

Решение этой задачи в теории криминалистики непосредственно связывают с необходимостью использования смежных с криминалистикой областей знаний[1], в частности знаний в сфере компьютерной криминалистики — форензики, которая является достаточно молодой и не в полной мере, постигнутой для казахстанской криминалистической науки.

Форензика занимается сбором, исследованием, оценкой следов преступлений в компьютерной области, а также разрабатывает систему специальных приемов, методов и средств, применяемых в ходе предварительного следствия для предупреждения, раскрытия и расследования преступлений[2]. Форензика была создана исключительно с целью раскрытия и расследования компьютерных преступлений и на сегодняшний день включает в себя: компьютерную криминалистику (Computerforensics / Digitalforensics), сетевую криминалистику (Networkforensics), криминалистический анализ данных (Forensicdataanalysis), форензику аппаратного обеспечения и технических устройств (Hardwareforensic). Именно такая классификация представлена в странах, где наука форензика достаточно развита.

Постижение компьютерной криминалистики имеет большое значение как для казахстанской криминалистической науки, так и для практической деятельности органов, осуществляющих раскрытие и расследование преступлений.

Во-первых, преступность, являясь основным дестабилизатором спокойствия в обществе, всецело использует все последние достижения науки и техники, совершенствуясь изо дня в день, приводя процентные показатели раскрываемости отдельных видов преступлений к значительно низкому уровню. В частности, речь идет о преступлениях, совершенных в сфере информатизации и связи (интернет преступления, киберпреступления).

Так, в 2020 г. против 110 уголовных правонарушений, совершенных в сфере информатизации и связи 42 остались не раскрытыми (38 %). В 2019 г. из 147 уголовных правонарушений, не раскрытых 51 (34 %). В 2018 г. из 168 уголовных дел, не раскрыто — 42 (25 %). В 2017 г., против 160 досудебных расследований, 27 числятся нераскрытыми (16 %). В 2016 г. из 182 уголовных дел не раскрыто 29 (15 %). В 2015 г. из 176 досудебных расследований не раскрыто 39 (22 %) (Рис. 1).

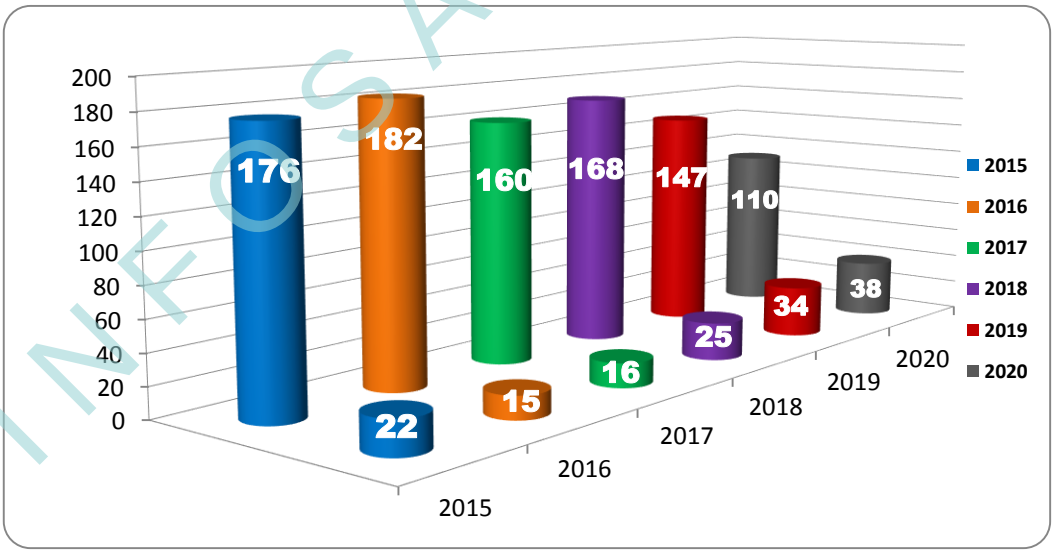


Рисунок 1. Соотношение количества преступлений, совершенных в сфере информатизации и связи, с процентом нераскрытых уголовных дел

Во-вторых, преступления, совершаемые с использованием цифровых технологий, влекут обнаружение как традиционных следов, с которыми, обычно, работают криминалисты, так и цифровых следов. К слову, бывают и случаи, когда при совершении преступлений в сфере информатизации и связи,

бывает достаточно сложно, а порой — невозможно отыскать следы пальцев рук, следы орудий, инструментов и т. п. Вместо них существует множество других — цифровых или же «виртуальных» следов.

Ученые сходятся во мнении, что «виртуальные» следы компьютерных преступлений — это любое изменения состояния компьютерной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Не представляется возможным характеризовать данные следы преступлений как материальные или же идеальные, так как виртуальные следы не выражены физически, например, в виде какого-либо предмета. Являясь содержимым различных устройств, они остаются нетронутыми при производстве обычного осмотра, к примеру осмотра предмета преступления (мобильный телефон или компьютер). Следует сказать, что в теории криминалистики ведутся дискуссии не только в отношении методов сбора и исследования таких следов, но также и в отношении самого понятия» цифровые следы»[3 15; 4; 5].

В каждом случае фиксации цифровых следов, органу, ведущему расследование, необходимо привлечь специалиста-криминалиста, имеющего не только соответствующие опыт и знания, но и материально-техническое оснащение[6, 49]. В целом, в этом и заключается необходимость постижения форензики как науки, поскольку следы киберпреступления, как правило, нематериальны, а значит их изучение не сможет провести обычный криминалист, не обладающий познаниями в сфере IT-технологий. К сожалению, как показывает казахстанская практика, таких специалистов насчитываются единицы.

В-третьих, в последние годы становится все более актуальным опыт применения современных компьютерных средств и технологий цифровой фиксации доказательственной информации при производстве различных следственных действий[7].

В целом, следует сказать, что цифровизация производства следственных и иных процессуальных действий является актуальной на протяжении значительного промежутка времени[8]. Несмотря на то, что использование цифровых видеокамер и приборов аудиозаписи все чаще используются при производстве таких следственных действий как осмотр, допрос, очная ставка, уточнение показаний на месте, следственный эксперимент и др., существует недостаточно методических рекомендаций по правильному использованию цифровых приборов и дальнейшему исследованию собранных доказательств.

Наряду с тем, что материалы цифровой видеозаписи следственного действия в большинстве случаев уже стали достойной заменой архаичного института понятых, а соответствии с уголовно-процессуальным законом (ч. 5 ст. 220 УПК РК)[9], существует проблема достоверности зафиксированного цифрового видеоизображения. Многие ученые-правоведы подходят критически к вопросу использования цифровых технологий в следственных действиях, и поэтому считают недопустимым внедрения методов цифровой видеосъемки в следственную практику в силу возможности внесения изменений в зафиксированные цифровые данные посредством компьютерных программ редакторов видеоизображений[10].

Таким образом, углубленное изучение положений и методик компьютерной криминалистики — форензики, должно стать неотъемлемой частью учебного процесса в высших учебных заведениях МВД Республики Казахстан, в том числе — в Карагандинской академии им. Б. Бейсенова. Постижение основ форензики положительно скажется не только на приобретении слушателями навыков, необходимых для успешного раскрытия и расследования преступлений в сфере информатизации и связи, но и поспособствует постижению практического мастерства работы с инструментами по сбору, обработке и исследованию цифровых доказательств.

---

[1] Кемали Е. С., Журсимбаев С. К. Некоторые проблемы криминалистики в свете сегодняшнего дня // Вестн. Ин-та законодательства Республики Казахстан. 2020. № 1 (59).

[2] Медведев И. В. Компьютерная криминалистика «Форензика» и киберпреступность в России // Пролог: журнал о праве. — 2013. — № 3. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kompyuternaya-kriminalistika-forenzika-i-kiberprestupnost-v-rossii (дата обращения: 06.10.2021).

[3] Кирсанова С. О., Калинина А. А. Виртуальные следы: понятие, сущность, проблемы // Скиф. — 2018. — № 3 (19). [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/virtualnye-sledy-ponyatie-suschnost-problemy (дата обращения: 05.10.2021).

[4] Петров С. В. Цифровые (виртуальные) следы как новое направление исследований в криминалистике // Современные научные исследования и разработки. — 2018. — № 12 (29). — С. 685 – 687.

[5] Перов В. А. Компьютерная криминалистика: электронный след понятие и виды // Уголовное судопроизводство: проблемы теории и практики. — 2021. — № 1. — С. 94 – 96.

[6] Крякина Т. А. Цифровые следы в криминалистике: понятие и значение в расследовании преступлений // Тенденции развития науки и образования. — 2020. — № 67-6. — С. 46 – 49.

[7] Ищенко Е. П. О цифровых технологиях в криминалистике // Современные проблемы отечественной криминалистики и перспективы ее развития: Сб. науч. ст. по мат-лам Всеросс. науч.-практ. конф. (с международным участием), посвященной 20-летию кафедры криминалистики. — М., 2019. С. 5 – 11.

[8] Шурухнов Н. Г., Гаврилин Ю. В. Некоторые направления использования автоматизированных рабочих мест при проведении следственных действий // Персональный компьютер на службе криминальной милиции и следствия. Возможности и перспективы. — М., 1997. С. 45 – 49.

[9] Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. // Казахстанская правда. 2014. 10 июля. № 133 (27754).

[10] Сильнов М. А. К вопросу о допустимости использования цифровых технологий в доказывании при расследовании преступлений. [Электронный ресурс]. — Режим доступа: www.silnov.newmail.ru/digitl.htm (дата обращения: 02.10.2021).

Плахота К. С.,
адъюнкт факультета подготовки научно-педагогическихи научных кадров
(Московский университет МВД России им. В. Я. Кикотя)

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА И ПРАКТИКИ ПРИМЕНЕНИЯ ВИДЕОКОНФЕРЕНЦСВЯЗИ НА СТАДИИ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ В СТРАНАХ БЛИЖНЕГО ЗАРУБЕЖЬЯ

В XXI в., в период формирования постиндустриального общества, информационные технологии активно развиваются на уровне государственных стандартов и внедряются во все сферы жизнедеятельности общества и государства. Анализируются реальные возможности их применения в уголовном судопроизводстве, в частности, при раскрытии и расследовании преступлений.

В соответствии с Федеральной целевой программой «Развитие судебной системы России на 2013 – 2024 годы», утвержденной Постановлением Правительства РФ от 27 декабря 2012 г. № 1406, в федеральных судах общей юрисдикции стало возможным применение видеоконференцсвязи (ВКС). «Согласно судебной статистике, за шесть месяцев 2020 г. суды первой инстанции рассмотрели с использованием ВКС 7 621 уголовное дело, 5 953 ходатайства об избрании (продлении) меры пресечения, 42 409 материалов в порядке исполнения приговора или судебного контроля»[1]. Более скромный опыт сложился на стадии предварительного расследования,«известные нам, примеры успешной реализации видеоконференцсвязи отмечаются в Ставропольском и Хабаровском краях. В условиях пандемии COVID – 19 наблюдается актуализация этой проблемы и необходимость ее повсеместного решения в территориальных органах внутренних дел»[2].

Выступая на расширенном заседании коллегии Министерства внутренних дел России 3 марта 2021 г., Президент Российской Федерации В. В. Путин обозначил потребность следственной практики в новых способах собирания доказательств. Нам представляется, что видеоконференцсвязь можно рассматривать в качестве одного из таких способов.

В уголовно-процессуальном законодательстве не содержится нормы, прямо разрешающей следователю / дознавателю осуществлять следственные действия дистанционно. Однако перечень технических средств, предусмотренный ч. 6 ст. 164 УПК РФ, не является исчерпывающим, и, следовательно, применение ВКС или электронных платформ не противоречит букве закона. На наш взгляд, в УПК РФ необходимо выделить отдельную норму, регламентирующую порядок и принципы использования технических средств, убрав, соответственно, их постатейное упоминание, причем весьма произвольное.

В научной литературе имеется несколько мнений по поводу реализации видеоконференцсвязи на практике: В. Л. Блудников считает, что ее применение на стадии предварительного следствия возможно по аналогии с получением видеопоказаний[3, 15]; А. П. Рыжаков полагает, что законодатель не наделил следователя в отличие от суда возможностью допрашивать граждан дистанционно[4]; некоторые ученые-правоведы придерживаются нейтральных позиций и предлагают обращаться к видеоконференцсвязи при исполнении международных запросов о правовой помощи и поручений по уголовным делам[5, 56]. По нашему мнению, данную технологию возможно и необходимо использовать в ходе следственных действий, руководствуясь рекомендациями, сложившимися на стадии судебного разбирательства.

В этой связи заслуживает внимания опыт Республики Казахстан в области приспособления высоких технологий целям уголовного судопроизводства. Так, например, представляет интерес институт дистанционного допроса (глава 26 УПК РК), который был введен в рамках реализации Указа Главы государства «О Концепции правовой политики на период с 2010 до 2020 года», Стратегии «Казахстан – 2050».

В ст. 213 УПК РК рассматриваются особенности дистанционного допроса потерпевшего и свидетеля с использованием научно-технических средств в режиме видеосвязи. Указанные участники уголовного процесса могут быть допрошены в органе досудебного расследования по месту жительства / нахождения при наличии уважительной причины.

Решение о применении технического средства принимает лицо, производящее расследование, по собственной инициативе, по указанию прокурора либо по ходатайству сторон. В ходе сеанса ВКС должны быть обеспечены информационная безопасность, надлежащее качество изображения и звука. Допускается изменение внешности и голоса лица в целях обеспечения его безопасности.

В научных трудах по криминалистике и уголовному процессу неоднократно поднималась проблема неявки граждан в орган досудебного расследования. Внедрение видеоконференцсвязи позволило снизить процессуальные издержки (в том числе по доставлению лиц, уклоняющихся от явки в правоохранительные органы), сократить сроки расследования, минимизировать риск побега и т. д.

Согласно упомянутой ст. 213 УПК РК производство дистанционного допроса возможно лишь в органе досудебного расследования. В ходе данного следственного действия присутствует широкий круг лиц, что может повлиять на психическое состояние допрашиваемого (вплоть до отказа от дачи показаний). Для решения данной проблемы может быть полезен опыт коллег из Республики Беларусь, где на правительственном уровне было принято решение о создании «дружественных комнат». В указанных комнатах менее строгая обстановка нежели в кабинете должностного лица, которая располагает малолетних / несовершеннолетних потерпевших и свидетелей рассказать о преступлении.

В Казахстане существует «Центр обслуживания населения» (ЦОН), который предоставляет услуги различных ведомств: МВД, Комитета дорожной полиции, Минсельхоза и др. Анализируя особенности работы ЦОНов, Б. К. Нургазинов, К. Е. Исмагулов предложили «включить в перечень предоставляемых услуг ЦОНов заполнение протоколов дистанционных допросов для органов досудебных расследований»[6, 85].

По нашему мнению, большим прорывом на стадии предварительного следствия явилось бы разрешение на законодательном уровне применять в ходе допроса электронные платформы (мессенджеры: Skype, WhatsApp, Viber, Telegram, Zoom и иные). Потерпевший / свидетель, находясь в знакомой и комфортной обстановке, более расположены для дачи показаний. Кроме того, современные смартфоны имеют функцию записи экрана, которая позволит дополнительно не проводить видеофиксацию, что также благоприятно скажется на качестве предоставляемой информации. На практике существует множество случаев, когда при использовании видеокамеры участники судопроизводства стеснялись, терялись, нервничали и не могли сообщить о произошедшемсобытии.

Посредством указанных мессенджеров следователь мог бы проводить в ходе допроса сеансы ВКС с переводчиками, сурдопереводчиками, так как нередко встречаются глухонемые, слабослышащие, тяжелобольные или граждане с ограниченными возможностями.

В 2020 г. в связи с тяжелой эпидемиологической обстановкой в Российской Федерации активно стали использоваться электронные платформы в судебных заседаниях. Так, В. Момотов, Председатель Совета судей, сообщил, что в условиях распространения коронавирусной инфекции судам разрешено использовать онлайн-сервисы при проведении заседаний, в качестве примера был приведен WhatsApp[7]. Например, ходатайство потерпевшего об участии в судебном заседании посредством WhatsApp было удовлетворено Волгоградским областным судом. Председатель этого суда, И. Трофимов сообщил, что для реализации данного права гражданину необходимо от руки написать ходатайство, сфотографировать его и по мессенджеру направить в суд.

На наш взгляд, подобные меры позволят сделать правосудие более доступным. А также сложившийся опыт можно положить в основу создания методических рекомендаций для стадии предварительного следствия.

Таким образом, необходимо чтобы теоретические положения об использовании технических средств соответствовали реалиям практики. Важно учитывать и в рамках возможного заимствовать опыт зарубежных стран. Применение видеоконференцсвязи и электронных платформ имеет множе-

ство перспектив: является дополнительным средством фиксации показаний, снижает процессуальные издержки, минимизирует риск побега, уменьшает сроки расследования, повышает производительность труда, позволяет вести многоточечные соединения и т. д. Однако ведение записи экрана и (или) видеосъемки требует от следователя / дознавателя надлежащих знаний законодательства, методических и тактических рекомендаций, а также определенного опыта работы.

[1] Официальный сайт Судебного департамента при Верховном Суде Российской Федерации URL: http://www.cdep.ru/index.php?id=79.

[2] Волынский А. Ф., Плахота К. С. Научно-технический прогресс — источник развития криминалистики и совершенствования следственной практики // Общество и право. — 2021. — № 1 (75). — С. 40 – 46.

[3] Будников В. Л. Видеопоказания в уголовном процессе России // Мировой судья. — 2010. — № 9.

[4] Рыжаков А. П. Допрос свидетеля (потерпевшего) с помощью систем видеоконференцсвязи: Науч.-практ. коммент. к Федер. закону от 20 марта 2011 г. № 39-ФЗ. [Электронный ресурс]. — Режим доступа: https://justicemaker.ru/view-article.php?id=22&art=2047 (дата обращения: 05.11.2021).

[5] Шиплюк В. А. Использование видеоконференцсвязи при осуществлении правовой помощи по уголовным делам // КриминалистЪ. — 2012. — № 1.

[6] Исмагулов К. Е., Нургазинов Б. К. Некоторые вопросы совершенствования института дистанционного допроса в казахстанском уголовном процессе // Вестн. Ин-та законодательства РК. 2018. № 1 (50). С. 82 – 90.

[7] ФГБУ «Редакция «Российской газеты». [Электронный ресурс]. — Режим доступа: https://rg.ru/2020/04/19/reg-urfo/sudam-razreshili-provodit-slushaniia-onlajn.html (дата обращения: 05.11.2021).

Подчинёнов А. В.,
руководитель проектов АО «ПАПИЛОН»
(Российская Федерация, Челябинская обл., г. Миасс)

НОВЫЕ ТЕХНОЛОГИИ, РЕАЛИЗОВАННЫЕ В АДИС «ПАПИЛОН – 9»

Новая версия АДИС «Папилон» предоставляет расширенный перечень реализованных автоматических и автоматизированных функций, обеспечивающих повышение результативности, максимальную степень автоматизации на всех этапах прохождения данных.

Ключевой новеллой АДИС «ПАПИЛОН – 9» является функция автоматического кодирования следов отпечатков пальцев и ладоней (наряду с дактилокартами). Данное усовершенствование позволяет существенно снизить трудозатраты на ввод новых следов в базу данных. При этом в системе реализованы новые алгоритмические решения по автоматическим поискам, благодаря чему обеспечиваются стабильно высокие вероятностные характеристики поиска в режимах След – След, След – Отпечаток, Карта – След в условиях исключения ручной фазы кодирования изображений следов.

В АДИС «ПАПИЛОН – 9» реализованы новые виды поисков как по дополнительным биометрическим модальностям – изображениям лиц и радужной оболочки глаз, так и по дактилоскопическим изображениям, в частности добавлены поиски следов по изображениям контрольных оттисков и поиски в режиме Карта – Карта по изображениям ладоней.

Мультибиометрический характер АДИС «ПАПИЛОН – 9» опирается, наряду с новыми биометрическими модальностями и режимами поисков, на расширяемый формат базы данных. Использование мультибиометрических технологий позволяет радикально повысить надежность и избирательность поисков за счет исключения возможности совпадения ошибок по различным модальностям. Преимущество использования мультибиометрической системы перед ее унитарным аналогом заключается в значительном затруднении возможных попыток предъявления подложных кандидатов за счет разнородности используемых модальностей и в существенном снижении вероятности случайных ошибок по той же причине.

Эффект от внедрения методов автоматизации процессов ввода может быть проиллюстрирован также на примере работы с дактилокартами. Так увеличение скорости ввода составляет порядка 15 – 20 % (относительно АДИС «ПАПИЛОН – 7»). Внедрение методов автоматизации позволит исключить случаи ошибок кодирования и связанных с ними пропусков совпадений и, как следствие, повысить результативность системы. Даже в тех случаях, когда операция кодирования все же необходима по критериям системы, процедура кодирования существенно упрощена. Это происходит, в частности, применительно к дактилокартам трупов, дактилокартам, в составе которых все содержащиеся изображения отпечатков пальцев имеют низкое качество, дактилокартам для которых установлено несоответствие порядка следования отпечатков.

Процедура кодирования заключается в проверке правильности установки продольной оси отпечатка.

Как следствие, усовершенствования, реализованные в АДИС «ПАПИЛОН – 9», позволяют обеспечить с высоким уровнем эффективности пополнение базы данных системы из различных источников, включающих мобильные и стационарные комплексы, а также носимые устройства.

Аналогично случаю кодирования дактилокарт, которое выполняется в ручном режиме только при выполнении ряда условий, процедура кодирования следов в АДИС «ПАПИЛОН – 9», вызываемая в интерактивном режиме также при определенных условиях, существенно упрощена по сравнению с АДИС «ПАПИЛОН» более ранних версий. Процедура включает установку продольной оси пальца с допуском и корректировку при необходимости скелетного изображения.

Реализованные в АДИС «ПАПИЛОН – 9» алгоритмы автоматического и автоматизированного кодирования следов позволяют совмещать кодирование в автоматическом и интерактивном режимах в необходимых случаях. Опытная эксплуатация системы применительно к подобной схеме работы показывает, что лишь 50 % количества следов от общего количества вводимых следов доходят в условиях реализации подобной схемы до стадии интерактивного кодирования. Оценка прироста количества идентификаций в случае реализации комбинированного способа кодирования, когда на этап интерактивного кодирования попадают только следы, которые не были идентифицированы после полностью автоматического кодирования перед вводом в базу данных, составляет 7 – 15 %.

В АДИС «ПАПИЛОН – 9» реализован целый ряд новых режимов поиска. В частности, перечень новых режимов включает поиск в режиме Карта – Карта по изображениям ладоней, поиск в режиме След – Дактилокарта по изображениям контрольных оттисков, поиск в режиме Карта – Карта по изображениям лиц, поиск в режиме Карта – Фотослед по фотоследам — записям, включающим изображения лиц, личность которых не установлена, поиск в режиме Фотослед – Карта по изображениям лиц, которые содержатся в составе карт, поиск в режиме Фотослед – Фотослед, поиск в режиме Карта – Карта по изображениям радужной оболочки глаз. Кроме того, добавлены реализации поисков в режиме оперативных проверок по изображениям лиц, по изображениям радужных оболочек глаз и по изображениям следов отпечатков пальцев.

Для наследуемых с более ранних версий режимов автоматических поисков Карта – Карта и След – Карта по изображениям отпечатков скорость поисков кратно возросла — не менее чем в 16 раз и не менее чем в 11 раз соответственно для вышеприведенных режимов.

В АДИС «ПАПИЛОН – 9» реализованы решения по оптимизации результатов перекрестных поисков между дактилокартами и следами, благодаря которым выявленные возможные совпадения в режиме Карта – След автоматически отображаются в ранее сформированных рекомендательных списка След – Отпечаток. Такой подход позволяет увеличить релевантность сохраняемых в системе результатов автоматических поисков. Общая эффективность поисков в АДИС «ПАПИЛОН – 9» применительно к режимам Карта – След и След – Отпечаток характеризуется высокими показателями избирательности — в 75 – 80 % случаев истинный кандидат оказывается на первом месте в рекомендательном списке.

Другое реализованное новшество применительно к дактилоскопической информации — базовой биометрической модальности, используемой в АДИС «ПАПИЛОН – 9», поиск по контрольным оттискам в режиме След – Дактилокарта не предполагает использования выделенных списков идентификаций и рекомендательных списков. Результаты, полученные с использованием контрольных оттисков, объединяются с результатами, полученными с использованием изображений отдельных отпечатков пальцев. Однако анализ результатов, полученных с использованием различных массивов данных, указывает на устойчивую величину доли идентификаций, получаемых с использованием контрольных оттисков – порядка 11 %.

Примечательно, что в режиме поиска по контрольным оттисков удается идентифицировать в том числе следы, оставленные средней и проксимальной фалангами пальцев рук.

Поиск в режиме Карта – Карта для новых биометрических модальностей – изображений лиц и радужных оболочек глаз позволяет расширить потенциальные сферы для применения АДИС. Комбинирование возможностей автоматической идентификации с использованием различных биометрических модальностей существенно улучшает вероятностные поисковые характеристики. Дополнение функциональных характеристик АДИС возможностями сбора, хранения, автоматических поисков и управ-

ления данными дополнительных модальностей позволяет получать из АДИС информацию на лиц, дактилоскопическая информация которых в базе данных АДИС отсутствует.

АДИС «ПАПИЛОН – 9» поддерживает опциональные возможности по модификации рекомендательных списков для того чтобы фокусировать внимание оператора на наиболее вероятных по дополнительным критериям отбора кандидатам. В частности, поддерживается алгоритм модификации рекомендательных списков След – Карта, когда особо выделяются совпадающие кандидаты, найденные для различных изображений, относящихся к одной карточке следов. Также поддерживается группировка записей лиц, относящихся к одному региону.

Мультибиометрическая архитектура АДИС «ПАПИЛОН – 9» обеспечивает возможности комплексной проверки лица на предмет нахождения относящихся к нему записей биометрической информации различных модальностей. Такая проверка может осуществляться в режиме оперативных проверок по удаленному серверу, который при наличии достаточной пропускной способности и наличия соответствующих вычислительных ресурсов, обеспечивает обслуживание запросов в режиме реального времени.

Применительно к использованию алгоритмов оперативной проверки дактилоскопической информации, наряду с поисками по содержащимся в базе данных дактилокартам, разработано программное обеспечение для проведения проверки по содержащимся в базе данных следам отпечатков пальцев.

Также поддерживается возможность проведения оперативной проверки следов, изымаемых при осмотре места происшествия. В отличие от перечисленных выше вариантов проведения оперативной проверки на основе биометрической информации, получаемой непосредственно от человека, процедура оперативной проверки следов отпечатков пальцев требует проверки полученных результатов с привлечением оператора. Другие стадии жизненного цикла прохождения запроса на оперативную проверку изъятого следа (за исключением процедуры выявления и фотографирования следа отпечатка пальца) полностью автоматизированы.

Процедура проверки результатов автоматических поисков совпадений для следов отпечатков пальцев в общем случае требует просмотра сформированных рекомендательных списков силами оператора. В целях оптимизации использования трудовых ресурсов операторов и повышения эффективности их работы может использоваться (совместно с АДИС «ПАПИЛОН – 9») специальное программное обеспечение, реализующее один из наиболее эффективных инструментов т.н. «искусственного интеллекта» — нейронную сеть глубокого обучения применительно к задаче анализа результатов автоматических поисков.

Преимущества, обеспечиваемые применением «искусственного интеллекта» в форме нейросети совместно с АДИС «ПАПИЛОН – 9», заключаются в возможности идентифицировать с приемлемыми трудовыми затратами т. н. «сложные», малоинформативные следы, а также обнаруживать истинные совпадения среди кандидатов, занимающих удаленные позиции в автоматически сформированных рекомендательных списках. По сути, функциональные характеристики ПО нейросети обеспечивают замещение работы оператора при просмотре рекомендательных списков, что позволяет радикально увеличить глубину их просмотра, при том что на долю настоящего оператора останется просмотр записей усеченных рекомендательных списков, содержащих кандидатов, чья вероятная истинность уже подтверждена искусственным интеллектом.

К настоящему времени данная технология апробирована на практике в ходе работы с реальными информационными массивами, находящимися в распоряжении крупных региональных подразделений МВД Российской Федерации, а именно силами ГУ МВД России по Ростовской области и ГУ МВД России по Челябинской области. В результате проведенной апробации получены данные, свидетельствующие о кратном, на несколько порядков снижении трудовых затрат на просмотр участков рекомендательных списков с низкими значениями индексов совпадения (ниже двадцатого места).

Прокопова А. А.,
старший преподаватель
кафедры криминалистики, подполковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Применение цифровых технологий и научно-технических средств как рациональный вектор ускорения процесса расследования

Ускорение процесса расследования в настоящий момент достигается в основном за счет сокращения его уголовно-процессуальной формы, посредством урезания предела доказывания, изъятием части процедурных механизмов, а также наличие требования о согласие подозреваемого с виной либо обвинением. Такие видоизменения часто влияют на качество расследования и создают риски нарушения прав участников ускоренных производств.

Принимая во внимание, что тенденция на оптимизацию уголовно-процессуальных механизмов неизбежна, считаем, что аналогичные результаты могут быть достигнуты путем повышения эффективности имеющихся ресурсов.

Одним из рациональных предложений которое может стать альтернативой ускорения уголовного судопроизводства, является исключение из деятельности органов уголовного преследования бюрократических элементов, интенсификация работы с акцентом на компьютерные технологии и внедрения блокчейн-технологий[1, 224].

С. М. Плешаков отмечает, что «по мере возрастания научных открытий и разнообразных изобретений рабочие места оснащаются всевозможными научно-техническими новинками, видоизменяются технологические процессы, происходит компьютеризация отдельных операций»[2, 5 – 6].

Л. А. Прокудина справедливо указывает, что внедрение электронных средств в судопроизводство способно вывести его на более высокий уровень развития, создать условия для системного управления движением дела, включающего определение режима прохождения дела в суде от его возбуждения до вынесения решения, ведение графика управления делом, контроль за продвижением дела, обеспечение эффективной связи с представителями сторон, непрерывную оценку работы системы, автоматизацию процесса управления делом, что, в конечном счете, повысит эффективность правосудия[3, 160].

Примером в данном случае, может случить уголовное судопроизводство Республики Казахстан, где в течение последних пяти лет проводятся широкомасштабные реформы, которые в том числе коснулись и внедрение в процесс расследования инновационных технологий.

В Уголовно-процессуальном кодексе 2014 г. (далее — УПК РК[4]) появился новый вид допроса с использованием научно-технических средств в режиме видеосвязи (дистанционный допрос)[5, 173]. Это обусловлено необходимостью разрешения проблем несвоевременности явки (доставки) свидетелей в установленное время, что зачастую является причиной затягивания расследования уголовных дел и, как следствие, нарушения прав и законных интересов участников процесса, а также уменьшения временных и материальных затрат на извещение свидетелей, находящихся на значительном удалении от места расследования уголовного дела, организацию командировок и выезд лица, производящего расследование, к месту нахождения потерпевшего (свидетеля). Дистанционный допрос является разновидностью допроса, производимого в режиме реального времени с отдаленным присутствием допрашиваемого посредством научно-технических средств в режиме видеосвязи, при котором возможен обмен аудио- и видеоинформацией[6].

Видеосвязь — это связь, осуществляемая посредством передачи и приема изображения и звука[7], одна из самых прогрессивных и перспективных связей, основное достоинство которой — возможность видеть своего собеседника на экране[8, 281]. Видеосвязь применяется во всем мире для эффективной и быстрой коммуникации между участниками, упрощает взаимодействие и сокращения количество переездов и расходов на них.

Дистанционный допрос применяется в случаях:

- невозможности непосредственного прибытия лица в орган, ведущий уголовный процесс, по месту расследования (рассмотрения) уголовного дела по состоянию здоровья или другим уважительным причинам;

- необходимости обеспечения безопасности лица;

- проведения допроса малолетнего или несовершеннолетнего свидетеля, потерпевшего;

- необходимости обеспечения соблюдения сроков досудебного расследования, судебного рассмотрения дела;

- наличия причин, дающих основания полагать, что допрос будет затруднен или связан с излишними затратами.

Основной целью дистанционного допроса является получение в кратчайшие сроки и без значительных материальных затрат показаний свидетеля и потерпевшего, которые находятся в отдалении от места производства досудебного производства. Допрос организовывается заинтересованным следователям, путем направления отдельного поручения в местонахождения необходимого участника процесса (ст. 213 УПК РК). Допрос осуществляется в общем порядке с учетом особенностей технических средств, применяемых в ходе следственного действия. Ходе и результаты допроса фиксируются в протоколе, который после его подписания направляется инициатору.

Дистанционный допрос значительно сокращают время на организацию и проведения допроса лично следователем (выезд в командировку) либо по поручению (длительное ожидание, некачественный результат), что во много ускоряет ход расследования.

Дистанционный допрос также можно проводить в рамках оказания правовой помощи по уголовным делам на основании международных договоров, с учетом требований уголовно-процессуального законодательства (ст. 576 УПК РК).

Еще одной инновацией досудебного производства в Республике Казахстан, стал электронной формат судопроизводства, который в 2017 г.[9] был официально закреплен, наравне с бумажным.

«Цифровизация уголовного процесса позволит решить ряд чувствительных для населения вопросов, а также упростить процедуру сбора доказательств и составления процессуальных документов, снизить риски фальсификации материалов дела и их утери, а также материальные затраты и нагрузку на следственные и судебные органы», — отметил генеральный прокурор РК Жакип Асанов[10].

Электронный формат расследования осуществляется на базе (модуля) «Е-уголовное дело» в системе Единого реестра досудебных расследований (ЕРДР). Модуль содержит алгоритмы действий по формированию уголовного дела, с момента начала расследования до момента исполнения приговора. Работа с системой осуществляется посредством заполнения определенных электронным шаблонов (бланков), позволяющих прикреплять сведения о полученных доказательствах, включая фото, аудиозаписи, видеоизображения, а также иные файлы и программные продукты, которые невозможно в последующем удалить.

Такой механизм направлен на максимальную прозрачность расследования, возможность доступа к материалам дела его участников и прокурора для ознакомления и изучения, а также исключение случаев фальсификации документов и потери уголовных дел.

Апробации нового формата расследования показала, что ускорение досудебного производства при расследовании в уголовных дел в электронном формате достигается путем сокращение сроков, при: направление ходатайств лицом, осуществляющим досудебное производство в прокуратуру, суд; передаче материалов досудебного расследования в органы прокуратуры и суда, для согласования решения о применении мер пресечения; получения разрешения на проведение отдельных следственных действий; направление материалов досудебного расследования процессуальному прокурору, следственному судье для рассмотрения по существу поступившие в рамках расследования жалобы, ходатайства и т. д.; ознакомление с материалами уголовного дела, путем одновременного прочтения всеми участникам досудебного расследования без привязки по времени и месту.

Все эти действия теперь возможно осуществлять, не выходя из кабинета, при помощи возможностей программного обеспечения.

Электронный формат расследования создает дополнительные гарантии обеспечения прав и законных интересов участников досудебного расследования. Так, участники процесса имеют доступ к процессуальной информации, и могут в онлайн-режиме следить за ходом расследования, дистанционно направлять документы для приобщения их к делу в качестве доказательств, знакомиться с материалами уголовного дела, приносить жалобы и т. д.

С учетом высказанных положительных моментов применения представленных инноваций, стоит отметить, что они находятся на этапе активной апробации и требуют корректировок с учетом выявляемых недостатков. Основной проблемой реализации данных новелл является значительные финансо-

вые средства необходимые для их повсеместного внедрения, а так же создание информационной среды способной обеспечить надлежащий уровень защиты процессуальной информации.

Таким образом, использование цифровых технологий и научно-технических средств в досудебном производстве с учетом всех достоинств и недостатков вполне действенно может ускорить процесс расследования без создания угрозы нарушения прав и законных интересов его участников.

Современные технологии призваны упрощать жизнь во всех ее сферах, уголовное судопроизводство не должно становиться исключением. Рационализация досудебного производства средствами современных технологий наиболее оптимальный способ ускорения на современном этапе развития уголовного процесса.

---

1 Григорьев В. Н., Победкин А. В. Тупиковые векторы «свертывания» уголовно-процессуальной формы? (концептуальный подход к проблеме) // Универсальный человек: Памяти Юрия Васильевича Астафьева / Под ред. А. Ю. Астафьева. — Воронеж, 2018.

[2] Плешаков С. М. Современные экспертные технологии в деятельности судебно-экспертных учреждений России: Автореф.дис. … канд. юрид. наук. — Н. Новгород, 2007.

[3] Прокудина Л. А. Система управления движением дела — фактор повышения эффективности отправления правосудия // Вестн. ВАС РФ. 2003. № 10. С. 160.

[4] Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V (с изм. и доп. по сост. на 21.01.2019 г.). [Электронный ресурс]. — Режим доступа: https://online.zakon.kz (дата обращения: 03.04.2019).

[5] Ахпанов А. Н. Депонирование показаний потерпевшего и свидетеля в уголовном процессе Республики Казахстан// Вестн. Омск.ун-та. Сер. «Право». 2015. № 4 (45).

[6] Прокопова А. А., Искакова Б. Е. Деятельность специалиста в ходе производства дистанционного допроса в досудебном производстве Республики Казахстан//Актуальные вопросы правовых научных исследований в системе органов внутренних дел: Мат-лыдистанц. международ. науч.-практ. конф. НИИ КА МВД РК. — Караганда, 2016. С. 229 —297.

[7] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. [Электронный ресурс]. — Режим доступа: http: //www.classes.ru/all-russian/russian-dictionary-Efremova-term-8952.htm (дата обращения: 20.03.2019).

[8] Морозов М. А. Информационные технологии в социально-культурном сервисе и туризме. Оргтехника: Учебн. 5-е изд. — М., 2004.

[9] Закон Республики Казахстан «О внесении изменении и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности» от 21 декабря 2017 г. № 118-VI ЗРК. [Электронный ресурс].— Режим доступа: http://adilet.zan.kz/rus (дата обращения: 03.04.2019).

[10] Уголовные дела в электронном формате апробируют в Казахстане. [Электронный ресурс].— Режим доступа: https://informburo.kz/novosti/ugolovnye-dela-v-elektronnom-formate-aprobiruyut-v-kazahstane.html(дата обращения: 03.04.2019).

Россинская Е. Р.,
заведующая кафедрой судебных экспертиз,
доктор юридических наук, профессор
(Московский государственный юридический университет
им. О. Е. Кутафина (МГЮА)

НАПРАВЛЕНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ КРИМИНАЛИСТИЧЕСКОЙ НАУКИ В РУСЛЕ ЕЕ ПРЕДМЕТА И СИСТЕМЫ[1]

Криминалистика — наука синтетической природы, постоянно интегрирующая и преобразующая для решения своей общей задачи — борьбы с преступностью и частных задач все новые достижения естественных, технических гуманитарных наук. Причем процессы синергии в криминалистике постоянно вызывали дискуссии о необходимости ее коренного изменения.

Приведем несколько примеров. Более 50 лет назад возникла о необходимости расчленения криминалистики и передачи криминалистической экспертизы медикам, биологам, химикам, физикам и другим представителям технических и естественных наук, которые в силу своей подготовки, в отличие от юристов, якобы лучше смогут производить исследование вещественных доказательств, фактически проповедовалось разделение криминалистики на «науку для экспертов» и «науку для следователей». Профессор А. И. Винберг, раскритиковал эту концепцию и обосновал существование в криминалистике общей теории криминалистической экспертизы, которую профессор А. Р. Шляхов выделил из криминалистики как самостоятельную науку, имеющую свой предмет, метод и систему. Однако большинство ученых не поддержали данную точку зрения. Общее мнение большинства криминалистов того времени выразил профессор С. П. Митричев, указав, что «криминалистическая экспертиза в составе науки криминалистики имеет все возможности для своего дальнейшего развития…».

В 60-е годы XX в. возникла новая дискуссия, касающаяся появления в криминалистике новой части — «общей теории криминалистики» (профессора Р. С. Белкин, А. А. Винберг), против которой категорически возражал профессор А. Н. Васильев.

Еще одна дискуссия, длившаяся в криминалистике более 40 лет — это идентификация и диагностика (профессора В. Я. Колдин, В. А. Снетков, Ю. Г. Корухов) или распознавание (профессора О. Е. Баев, В. А. Образцов).

Этот список можно продолжать, упомянув споры о включении в криминалистическую технику новых разделов «криминалистическое исследование веществ, материалов и изделий» (профессора В. С. Митричев, Е. Р. Россинская); «криминалистической ольфакторики (одорологии) (профессора А. И. Винберг, Т. Ф. Моисеева, доцент В. И. Старовойтов). Им категорически возражал профессор М. С. Строгович: «Пока я жив, не пущу собаку в уголовный процесс». В 70-е – 80-е годы XX в. в криминалистику вошли криминалистическая фоноскопия (профессор Е. И. Галяшина); математические и кибернетические методы, автоматизированные дактилоскопические идентификационные системы (профессора Н. С. Полевой, В. В. Крылов, Л. Г. Эджубов, С. С. Самищенко).

Но предмет криминалистики устоял. По классическому определению Р. С. Белкина, (которое с некоторыми вариациями, связанными с перечнем основных закономерностей) криминалистика — наука о закономерностях механизма преступления, возникновения информации о преступлении и его участниках, закономерностях собирания, исследования, оценки и использования доказательств и основанных на познании этих закономерностей специальных методах и средствах судебного исследования и предотвращения преступлений. Причем под судебным исследованием понимается вся юрисдикционная деятельность компетентных органов по расследованию преступлений, судебному рассмотрению уголовных, гражданских, административных дел, дел об административных правонарушениях.

В XXI в., когда резко возросли процессы развития новых родов и видов судебных экспертиз, снова возникли попытки ревизии самого понятия криминалистики в отрыве от ее предмета и системы, что было обусловлено появлением качественно новых классов и родов судебных экспертиз: речеведческих, лингвистических, экологических, молекулярно-генетических, а также бурное развитие новых родов в уже существующих классах судебных экспертиз (судебной экономической экспертизы операций с активами, созданными на основе технологии блокчейн и др.). Заметим, что новые экспертизы вначале проводятся не в судебно-экспертных учреждениях, а как правило, лицами весьма далекими от судопроизводства. Ученые и специалисты, привлекаемые для производства этих новых видов судебных экспертиз, не знают даже основ судебной экспертологии, азов материального и процессуального права. Они не понимают отличия научных исследований от практической экспертной деятельности, не представляют возможных последствий их выводов.

Лица, которые занялись производством новых родов и видов судебных экспертиз, не имеют представления о предмете, задачах, системе криминалистической науки, игнорируют ее общую и частные теории. Их представление о науке криминалистике обычно ограничивается знаниями, почерпнутыми из случайных источников, даже из детективной литературы, художественных фильмов.

Печально, что, несмотря на то, что уже более 20 лет в Российской Федерации существуют государственные образовательные стандарты высшего образования в по специальности «Судебная экспертиза» (сейчас это ФГОС ВО 40.05.03 3++), целый ряд экономических, филологических и других вузов пытается готовить судебных экспертов не по данной специальности, а изобретая собственные. Для этого в ряде вузов, зачастую не имеющих никакого отношения к юриспруденции, образованы даже кафедры лингвистической криминалистики, экономической криминалистики. В медицинских вузах, где в рамках клинических ординатур готовят судебно-медицинских экспертов, введены курсы медицинской криминалистики!!! Понятно, что вред наносится судебной экспертизе, но вдобавок происходит смешение понятий криминалистики и судебной экспертизы.

Нет и не может быть никакой медицинской криминалистики, лингвистической криминалистики, экономической криминалистики, молекулярно-генетической криминалистики, технической криминалистики и пр. Криминалистика едина! Это наука, имеющая свой предмет, систему, задачи, объекты и закономерности. Криминалистика — обосновывающее знание для всех родов и видов судебных экспертиз. Предметом судебной экспертологии являются методологические, правовые и организационные закономерности функционирования судебно-экспертной деятельности в целом; закономерности возникновения, формирования и развития классов, родов и видов судебных экспертиз и их частных

теорий на основе единой методологии, унифицированного понятийного аппарата и с учетом постоянного обновления и видоизменения судебно-экспертных знаний. Предмет криминалистики был нами определен выше.

Основанием разграничения двух родственных, но самостоятельных наук является различие их целей и функций. Предметом криминалистики служат, в том числе, закономерности деятельности по собиранию, исследованию, оценке и использованию доказательств. Предметом судебной экспертологии являются закономерности судебно-экспертной деятельности, как единого целого. Каждый вид деятельности имеет своего основного субъекта: соответственно следователя (дознавателя) и судебного эксперта, обладающих процессуальной самостоятельностью и кругом прав и обязанностей.

Проанализируем методологические функции криминалистики и судебной экспертологии: в криминалистике — методологическое обеспечение следственной практики: в экспертологии — методологическое обеспечение экспертной практики. Частично эти функции перекрываются, поскольку исследование доказательств происходит и в ходе следственных действий, и при производстве судебных экспертиз.

Конец XX – начало XXI вв. ознаменовались глобальным процессом цифровизации. Внедрение во все сферы человеческой деятельности современных информационных компьютерных технологий не могло не затронуть и сферу судопроизводства по уголовным, гражданским и административным делам. В криминалистике и судебной экспертологии произошли существенные трансформации, связанные с объектами исследования. На смену традиционным аналоговым способам отображения объектов пришли их электронные аналоги, представленные в цифровом виде. Криминалистически значимая информация запечатлевается в компьютерных средствах и системах в неявном виде, и для обеспечения возможности ее восприятия необходимо использовать специальные IT-технологии.

Существенные изменения произошли в способах преступлений, поскольку практически любые преступления: присвоения, кражи, мошенничества, фальшивомонетничество, лжепредпринимательство, преступления в банковской сфере и многие другие совершаются с использованием компьютерных средств и систем. Повсеместное распространение средств мобильной коммуникации привело к возникновению новых видов преступлений, таких как создание и распространение вирусных и вредоносных программ для мобильных телефонов, использование мобильных средств связи для совершения мошенничеств, вымогательств, поджогов, взрывов, террористических актов и пр. Поскольку способы компьютерных преступлений утратили жесткую связь с составом преступлений, дефиниция «компьютерное преступление» (кибепреступление) как в России, так и за рубежом употребляется в настоящее время не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом преступления и, соответственно, с методикой его раскрытия и расследования.

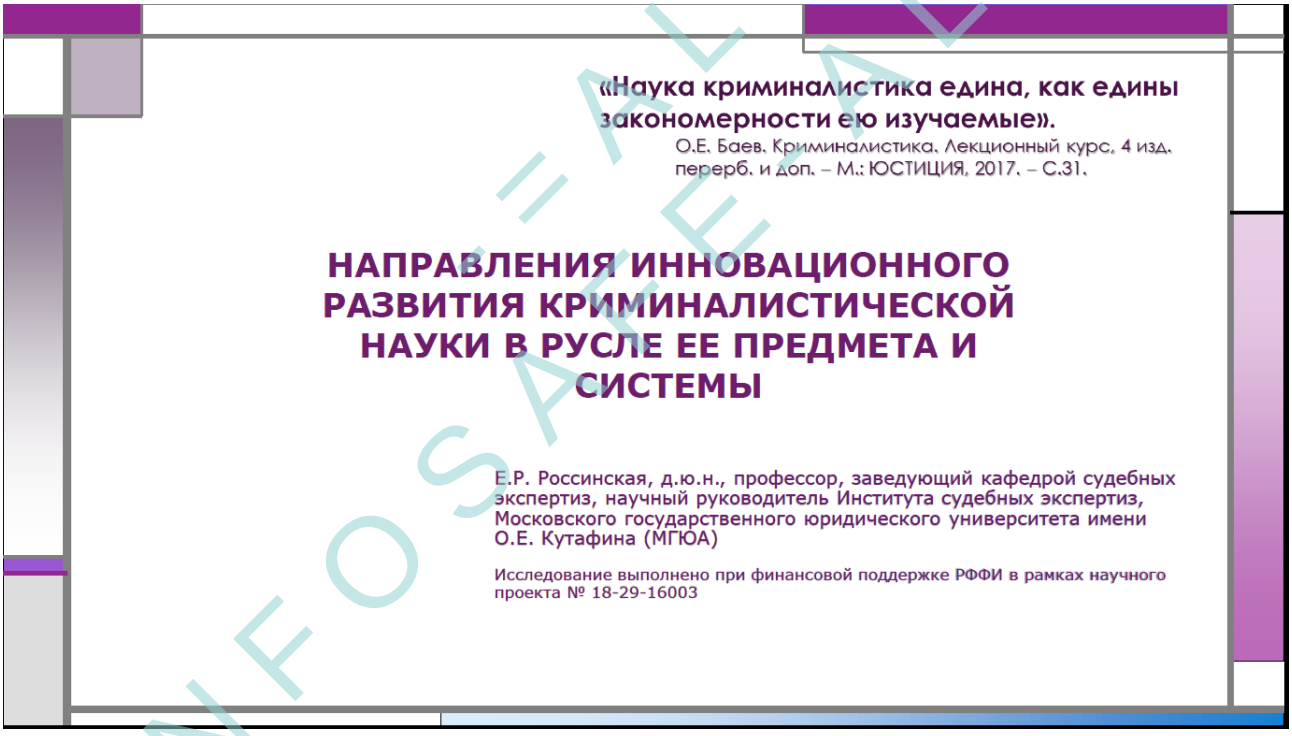
Снова в криминалистике возникли попытки изменения ее предмета и наименования, появление «новых криминалистик»: электронной криминалистики, компьютерной криминалистики, цифровой криминалистики. Еще раз подчеркнем, что криминалистика едина! Для ее развития нет необходимости и оснований менять название. Развитие идет за счет изучения новых закономерностей, новых механизмов следообразования, новых технологий собирания (выявления, фиксации, изъятия), исследования, оценки и использования криминалистически значимой информации, новаций в области криминалистической тактики и методики. Интеграция в криминалистику цифровых технологий идет не по пути создания какой-то новой цифровой криминалистики, а за счет создания новой криминалистической теории — Теории информационно-компьютерного обеспечения криминалистической деятельности, которая является новой частью общей теории криминалистики.

Предметом этой теории служат закономерности возникновения, движения, собирания, исследования и использования компьютерной информации при расследовании преступлений и судебном рассмотрении уголовных, гражданских и административных дел. Объектами являются: сами компьютерные средства и системы как носители розыскной и доказательственной криминалистически значимой информации, а также система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий выявления, фиксации, изъятия, сохранения, исследования и использования криминалистически значимой доказательственной и ориентирующей информации.

Система теории информационно-компьютерного обеспечения криминалистической деятельности включает целый ряд новых учений, на базе которых разрабатываются новации во всех разделах криминалистической науки. В систему входят:

1. Концепция теории информационно-компьютерного обеспечения криминалистической деятельности, включая предмет теории и ее объекты.
2. Учение о способах компьютерных преступлений преступлений/правонарушений.
3. Учение о цифровых следах как источниках криминалистически значимой компьютерной информации.
4. Учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники.
5. Учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий.
6. Учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений.
7. Учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений.
8. Учение о цифровизации системы криминалистической регистрации, в том числе, справочно-информационных фондов криминалистического и судебно-экспертного назначения, включающее взаимосвязи и разграничения цифровизации криминалистической и судебно-экспертной деятельности.

Приложение к докладу



Слайд 1

Криминалистика – наука синтетической природы, постоянно интегрирующая и преобразующая для решения своей общей задачи – борьбы с преступностью и частных задач все новые достижения естественных, технических гуманитарных наук.

Причем процессы синергии в криминалистике постоянно вызывали дискуссии о необходимости ее коренного изменения.

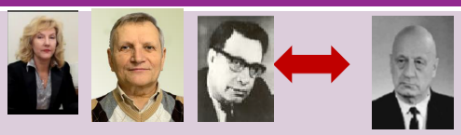
Слайд 2

Краткий исторический аспект проблемы

Этап	Предложения	Персоны
50-е – 60-е годы XX века	Разделение криминалистики на «науку для экспертов» и «науку для следователей»	
60-е – 70-е годы XX века	Развитие общей теории криминалистики	
70-е – 90-е годы XX века	Идентификация и диагностика или распознавание	
80-е годы XX века	Криминалистическое исследование веществ, материалов и изделий	

Слайд 3

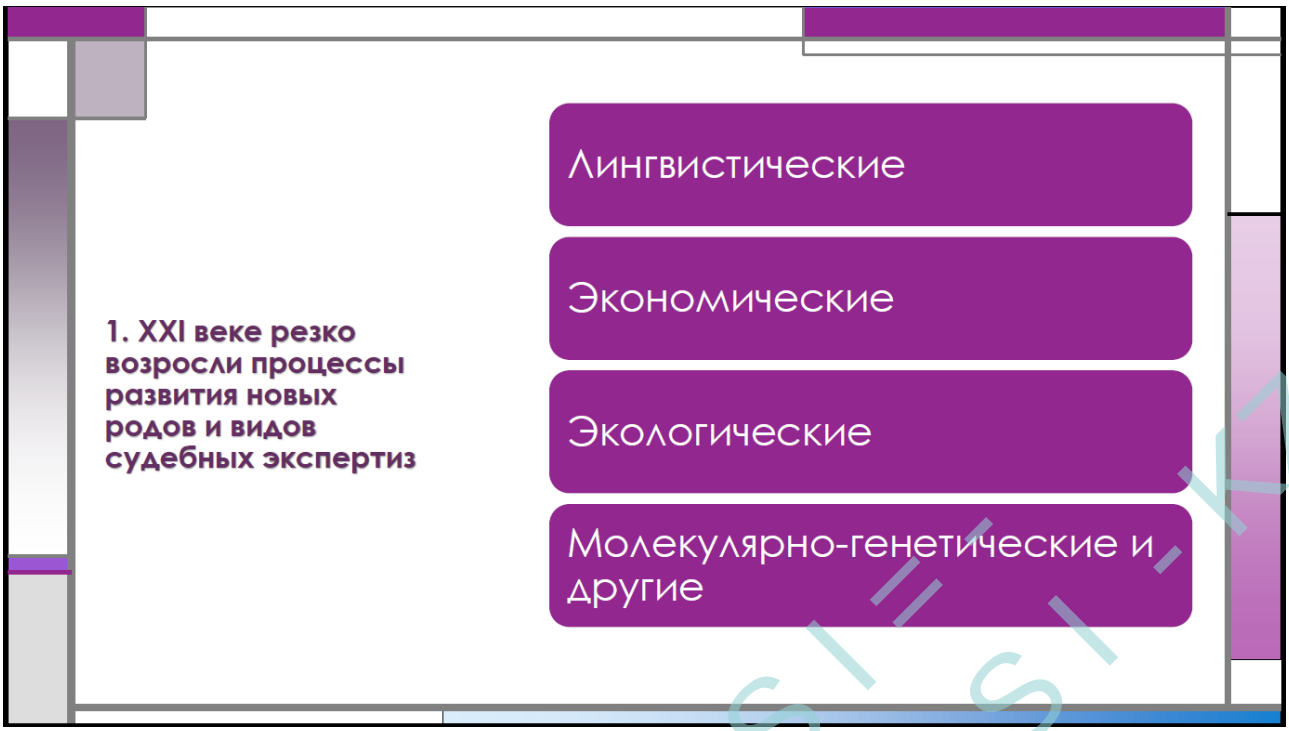
Краткий исторический аспект проблемы

Этап	Предложения	Персоны
60-е – 90-е годы XX века	Криминалистическая ольфакторика	
80-е – 90-е годы XX века	Криминалистическая Фоноскопия	
70-е годы XX века – 00-е годы XXI века	Математические и кибернетические методы методы в криминалистике (АДИС)	Полевой Н.С., Крылов В.В. 

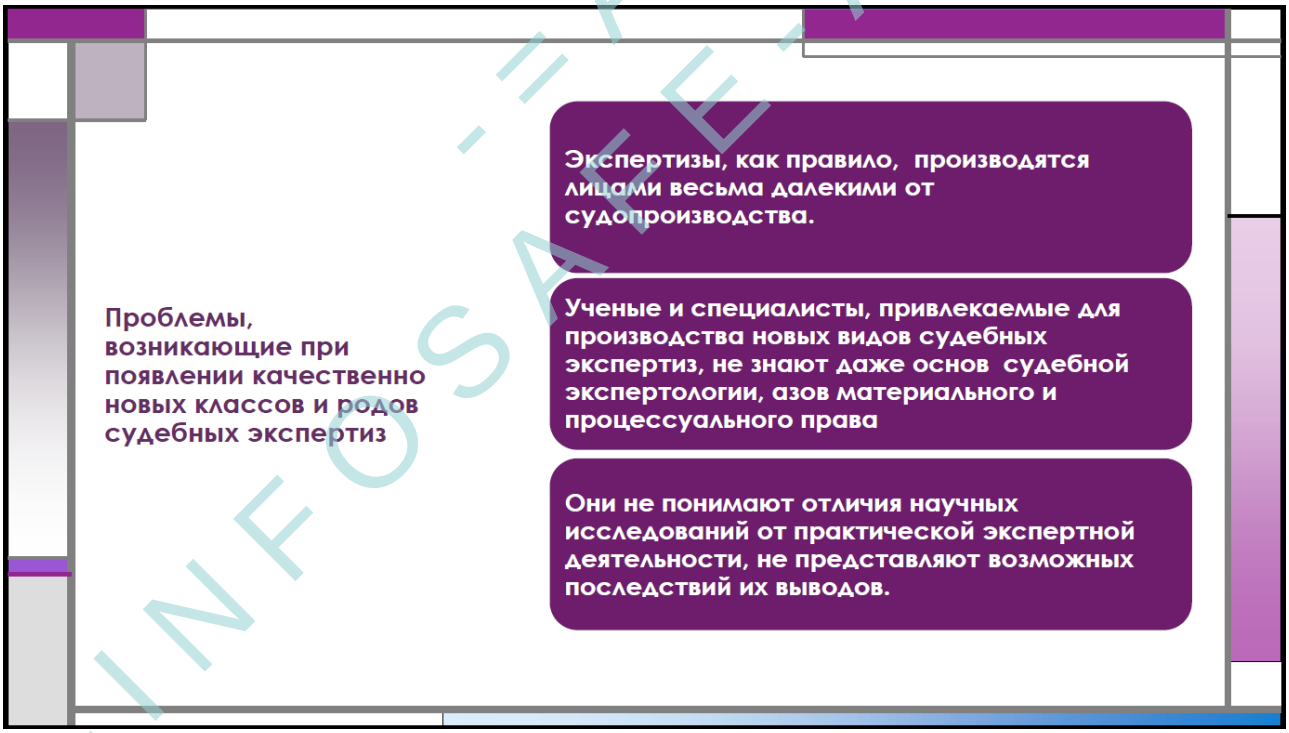
Слайд 4

В XXI веке снова возникли попытки ревизии самого понятия криминалистики в отрыве от ее предмета и системы

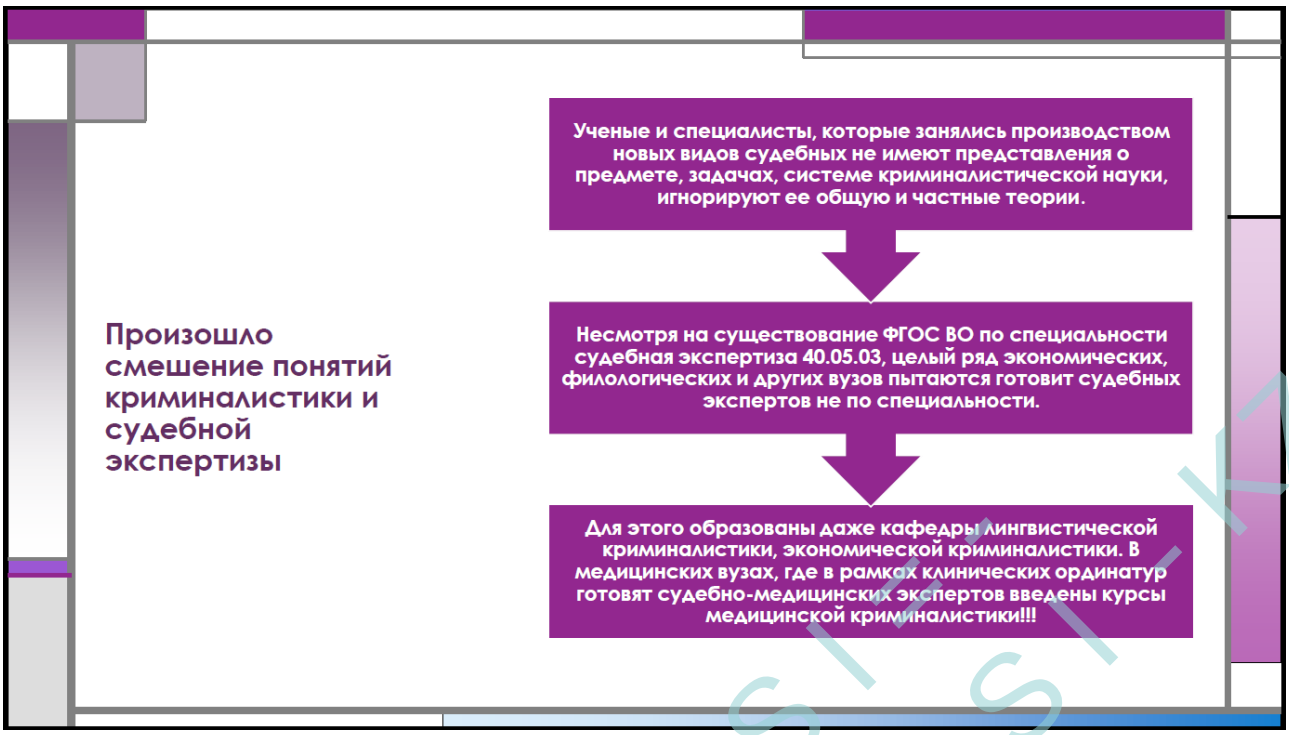
Слайд 5



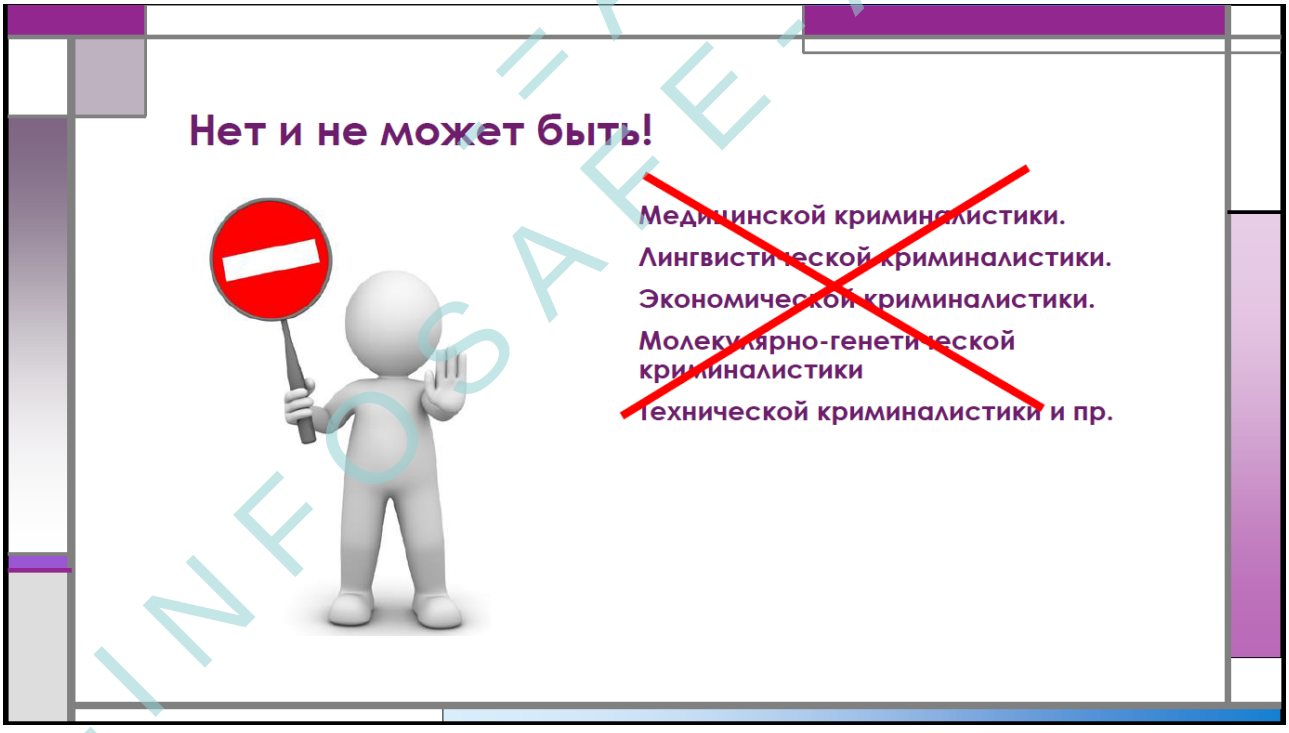
Слайд 6



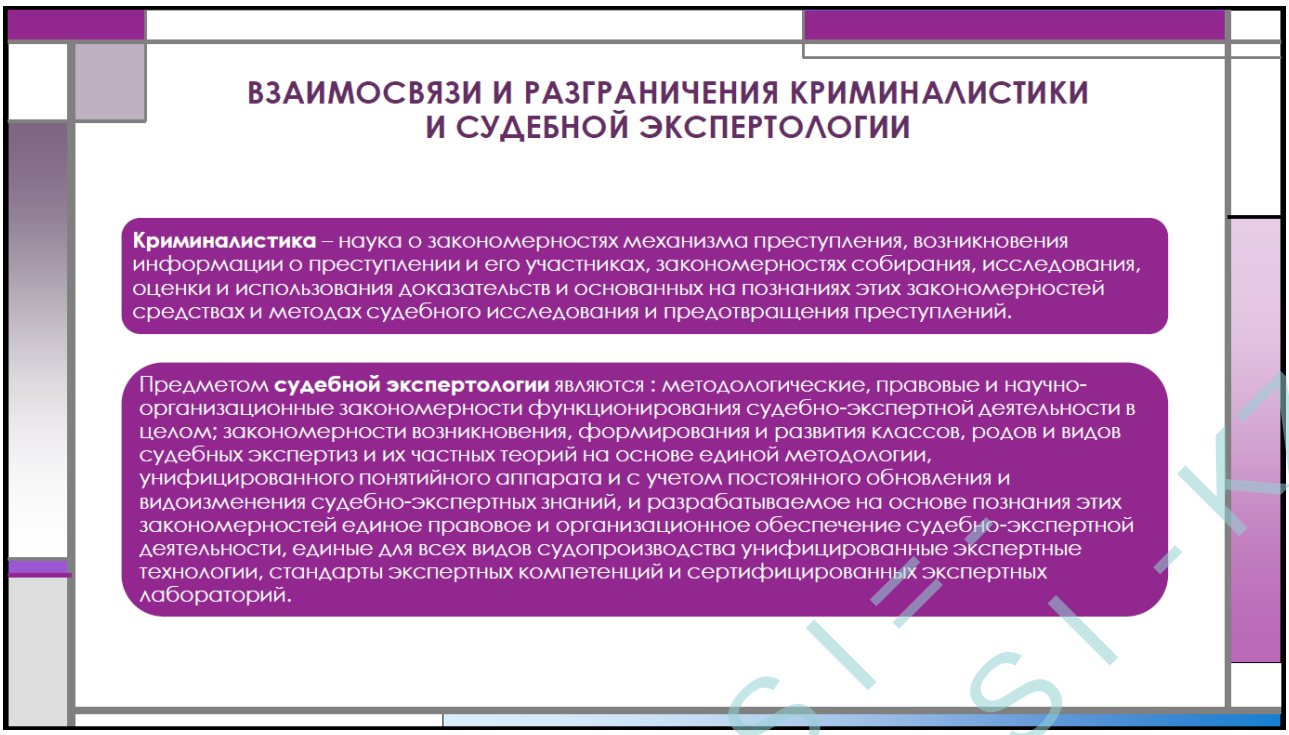
Слайд 7



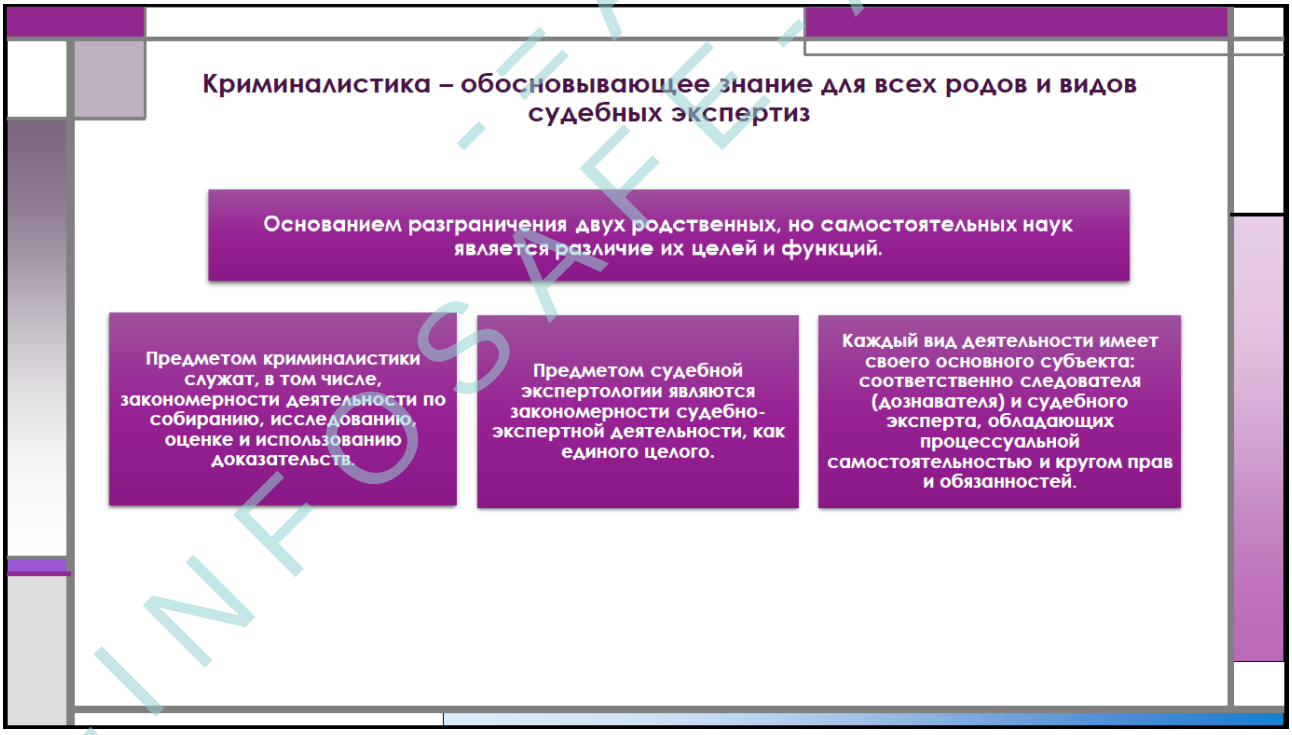
Слайд 8



Слайд 9

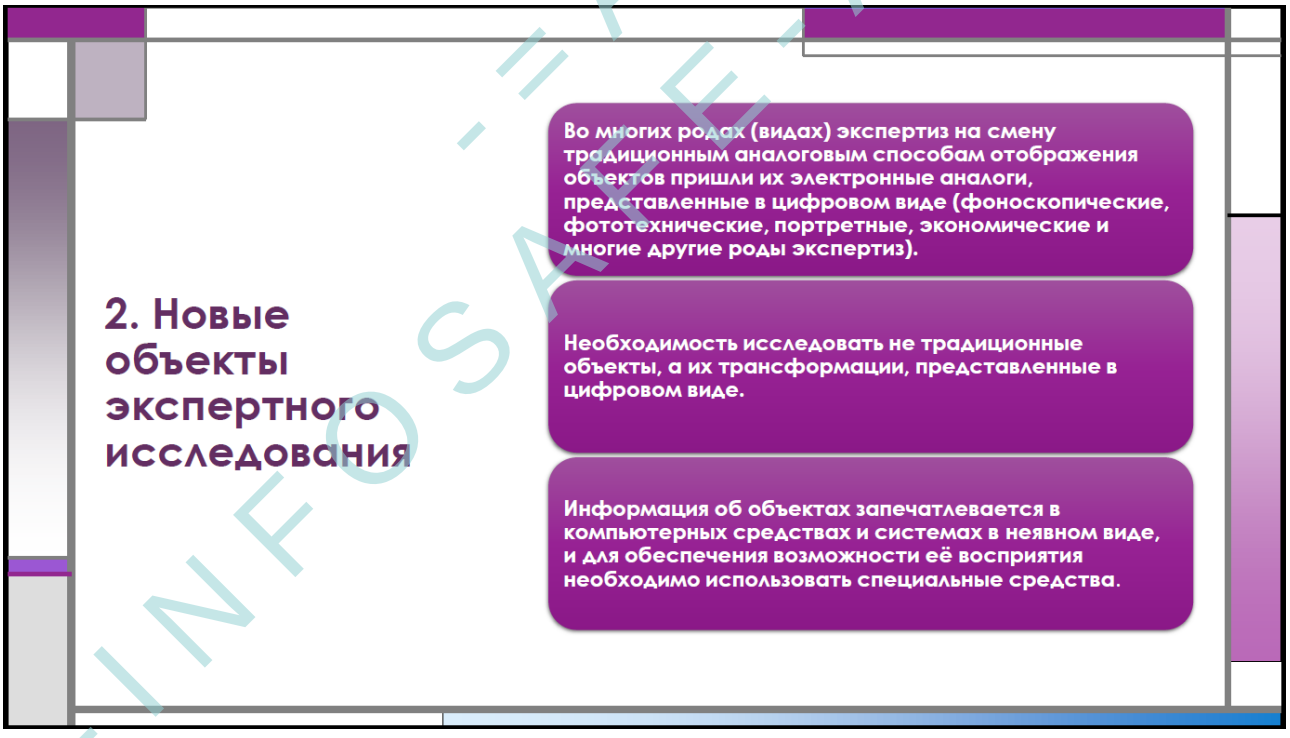


Слайд 10



Слайд 11

Слайд 12



Слайд 13

Внедрение во все сферы человеческой деятельности современных информационных компьютерных технологий не могло не затронуть и сферу судопроизводства по уголовным, гражданским и административным делам.

Существенные изменения произошли в способах «традиционных» преступлений, поскольку практически любые преступления: присвоения, кражи, мошенничества, фальшивомонетничество, лжепредпринимательство, преступления в банковской сфере и многие другие совершаются с использованием компьютерных средств и систем.

Повсеместное распространение средств мобильной коммуникации привело к возникновению новых видов правонарушений, таких как создание и распространение вирусных и вредоносных программ для мобильных телефонов, использование мобильных средств связи для совершения мошенничеств, вымогательств, поджогов, взрывов, террористических актов и пр.

Слайд 14

~~Электронная криминалистика»~~
~~Компьютерная криминалистика~~
~~Цифровая криминалистика~~

Криминалистика едина!

Это наука, имеющая свой предмет, систему, задачи, объекты и закономерности. Для ее развития нет необходимости и оснований менять название

Развитие идет за счет изучения новых закономерностей, новых механизмов следообразования, новых технологий собирания (выявления, фиксации, изъятия), исследования, оценки и использования криминалистически значимой информации, новаций в области криминалистической тактики и методики.

Слайд 15

ТЕОРИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОГО ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Предметом этой теории служат закономерности возникновения, движения, собирания, исследования и использования компьютерной информации при расследовании преступлений и судебном рассмотрении уголовных, гражданских и административных дел.

Объектами – являются:

- сами компьютерные средства и системы как носители розыскной и доказательственной криминалистически значимой информации,
- система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий выявления, фиксации, изъятия, сохранения, исследования и использования криминалистически значимой доказательственной и ориентирующей информации.

16

Слайд 16

Концептуальные основы теории информационно-компьютерного обеспечения криминалистической деятельности, включают:

- предмет теории, ее объекты, задачи, изучаемые закономерности;
- определение основных дефиниций информационно-компьютерного обеспечения криминалистической деятельности:
  - цифровых следов в информационно-компьютерном пространстве,
  - носителей криминалистически значимой компьютерной информации,
  - компьютерной системы в криминалистическом понимании;
  - криминалистического понятия вредоносных программ и контрафактных информационно-компьютерных продуктов

Слайд 17

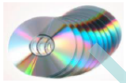
18

УЧЕНИЕ О ЦИФРОВЫХ СЛЕДАХ КАК ЧАСТЬ ТЕОРИИ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОГО ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Цифровой след – это криминалистически значимая компьютерная информация о событиях или действиях, отраженная в материальной среде, в процессе возникновения, обработки, хранения и передачи.


- Цифровые следы материальны, поскольку отражаются на материальных объектах, хотя в некоторых случаях период их существования весьма невелик.


- Цифровые следы технологические по происхождению, поскольку их формирование обусловлено реализации информационных технологий, и для их преобразования в доступную для восприятия форму также используются информационные технологии.

- По механизму следообразования они электронные либо электромагнитные в зависимости от носителей – твердотельных либо магнитных дисков. Возможны и механико-оптические следы в структуре материала оптического диска под воздействием лазерного луча.


Слайд 18

Использование вредоносных программ как способов компьютерных преступлений практически всегда носит полноструктурный характер, причем подготовка сразу предусматривает действия по сокрытию

ПРИЗНАКИ ВРЕДОНОСНОСТИ ПРОГРАММЫ:

- наличие функциональных возможностей уничтожения, блокирования, модификации, копирования пользовательской информации и нейтрализации средств защиты компьютерной информации;
- инсталляция без явного одобрения пользователем;
- скрытый либо замаскированный от пользователя режим работы;
- проведение операций с информацией, не санкционированных пользователем явно.

19

Слайд 19

«Криминалистическое исследование компьютерных средств и систем» как раздел криминалистической техники: исследование стационарных компьютеров, серверов, носителей данных, мобильных устройств сотовой связи, смартфонов, планшетных компьютеров и других устройств; содержит описание этих объектов, особенности собирания (выявления, фиксации, изъятия) криминалистически значимой компьютерной информации, возможности судебно-экспертного исследования этих объектов

20

Слайд 20

21

Учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий

Виды тактических приемов, тактических комбинаций и операций при расследовании компьютерных преступлений. Классификация и типизация следственных ситуаций, возникающих при расследовании компьютерных преступлений. Тактические рекомендации при расследовании компьютерных преступлений, специфика тактических решении и особенности тактического риска по делам данной категории.

Особенности тактики и технологии следственных действий (осмотр, обыск, допрос, осмотр предметов, документов, выемка, следственный эксперимент) по уголовным делам , сопряженным с неправомерным доступом к компьютерной информации, разработкой и использованием вредоносных программ, мошенничеств, незаконном обороте наркотических средств, преступлениях против личности, преступлениях в сфере экономической деятельности и пр.

Роль специальных знаний и специалистов в применении тактических приемов и тактических операций, ситуационный подход к выбору специалиста и его компетенции.

Д.ю.н., проф. Россинская Е.Р. ©

Слайд 21

Вследствие общности способов для различных видов компьютерных преступлений предлагается концепция учения об информационно-компьютерных криминалистических моделях компьютерных преступлений

Предмет этого учения составляют общие закономерности построения информационно-компьютерных моделей компьютерных преступлений на основе корреляционных связей между комбинациями IT-технологий, используемых для осуществления различных способов компьютерных преступлений, независимо от их вида, и следовой картиной в виде цифровых следов, а также с компетенциями в информационных компьютерных технологиях преступника и потерпевшей стороны.

Объектом учения является криминалистически значимая компьютерная информация:

- об использованных комбинациях компьютерных средств и систем для осуществления различных способов компьютерных преступлений;
- о цифровых следах, в том числе следах воздействия вредоносных программ;
- о контрафактных информационно-компьютерных продуктах;
- о степени владения информационными компьютерными технологиями лиц, совершающих данные преступления;
- о степени владения информационными компьютерными технологиями. потерпевших (потерпевшей стороны).

Основным принципом формирования информационно-компьютерных моделей является ранжирование их по сложности способов реализации противоправных действий, включая используемые IT-технологии и корреляции с этими способами уровня компетенции преступников, состава преступной группы или сообщества.

Корреляционные связи существуют также между способом компьютерного преступления и компьютерной грамотностью потерпевшего, которая также может иметь разные уровни по компетентности: пользователь; специалист в области IT-технологий.

Слайд 22

Система теории информационно-компьютерного обеспечения криминалистической деятельности

1. Концепция теории информационно-компьютерного обеспечения криминалистической деятельности, включая предмет теории и ее объекты.
2. Учение о способах компьютерных преступлений преступлений/правонарушений.
3. Учение о цифровых следах как источниках криминалистически значимой компьютерной информации.
4. Учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники.
5. Учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий.
6. Учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений.
7. Учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений.
8. Учение о цифровизации системы криминалистической регистрации, в том числе, справочно-информационных фондов криминалистического и судебно-экспертного назначения, включающее взаимосвязи и разграничения цифровизации криминалистической и судебно-экспертной деятельности.

Слайд 23

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003.

[2] Россинская Е. Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридич. вестн. Самарск. ун-та, Т. 5, № 4, 2019. С. 144 – 151.

[3] Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. — 2019. — № 3 (148). — С. 87 – 99.

[4] Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: Мат-лы международ. науч.-практ. конф. (19 февраля 2019 г.). — Алматы, 2019. С. 6 – 9.

[5] Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестн. Вост.-Сиб. ин-та МВД России, № 2 (89), 2019. С. 193 – 202.

[6] Россинская Е. Р., Семикаленова А. И. Основы учениюо криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестн. Санкт-Петербургск. ун-та. Право. Том 11, вып 3, 2020. С. 745 – 759.

[7] Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 5. — С. 699 – 709.

[8] Россинская Е. Р. Учение о криминалистическом исследовании компьютерных средств и систем как научная основа нового раздела криминалистической техники // XVth International Congress Criminalistics and Forensic Expertology: Science, Studies, Practice. September 19-21, 2020. Vilnius., Lithuania. С. 74 – 94.

[9] Россинская Е. Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестн. Вост.-Сиб. ин-та МВД России, № 2 (97), 2021. С. 190 – 200.

[10] Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russica. — 2021. — Том 74. — № 9 (178), сентябрь. — С. 102 – 118.

Савельева М. В.,
кандидат юридических наук, доцент
(Саратовская государственная юридическая академия,
Российская Федерация)

К ВОПРОСУ О НЕОБХОДИМОСТИ СОЗДАНИЯ ЕДИНОЙ ЦИФРОВОЙ СИСТЕМЫ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

В настоящее время очевидным является и для общественности, и для юристов-практиков, и ученых, что стране в целом нужен логически обоснованный, экономически целесообразный подход к формированию цифровой системы уголовного судопроизводства, опирающийся на реальные интересы и потребности населения и государства, способный эффективно обеспечивать доступ к правосудию в уголовном судопроизводстве, с учетом реализации потенциала дистанционный процедур.

Решение вопроса об активном использовании цифровых инноваций и цифровых технологий в ходе расследования преступлений, в частности, и в ходе уголовного судопроизводства в целом, упирается в необходимость создания единой замкнутой цифровой системы уголовного судопроизводства, направленной на обеспечение потребностей правоохранительных и судебных органов в решении задач уголовного судопроизводства.

В связи с этим в криминалистической литературе вводится в оборот понятие экосистемы уголовного судопроизводства. Так, Л. Н. Масленникова использует термин «экосистема начального этапа уголовного судопроизводства», понимая под ней сложную систему, включающую множество взаимосвязанных и взаимообусловленных элементов, по сути представляющую сферу, регулируемую уголовно-процессуальным законом, обеспечивающую доступ к правосудию, обладающую замкнутой системой взаимосвязей ее компонентов (регистрация сообщения о преступлении, расследование, надзор прокурора, судебная власть), придающих ей стабильность, связанную с другими устойчивыми системами (судебной системой), имеющую определенную продуктивность по обеспечению доступа к правосудию[1].

В принципе соглашаясь с подобным определением, полагаем необходимым отметить, что с технической точки зрения для реализации данного проекта должны быть соблюдены достаточно жесткие технические требования, обеспечивавшие унификацию и единые стандарты, применяемые ко всем цифровым ресурсам правоохранительных органов в области интерфейсов, совместимости способов коммуникации, формата анализируемого и реализуемого материала, используемого оборудования и программного обеспечения с учетом обеспечения защиты данного информационного пространства.

Таким образом, ключевыми представляются для создания и организации единой цифровой системы уголовного судопроизводства комплексные решения ряда вопросов.

Первое: возможность подачи информации, заявления о преступлении с помощью соответствующего технического оборудования (посредством видеоконференцсвязи, соответствующих приложений телефона или Интернета)[2].

Второе: обеспеченность уполномоченных органов (суд, прокуратура, МВД, следственный комитет и т. д.) возможностью ведения электронного документооборота в уголовном судопроизводстве, вплоть до ведения электронного уголовного дела (с учетом технических возможностей протоколирования следственных действий и реализации дистанционных технологий при их производстве).

Третье: законодательное урегулирование возможности дистанционного производства отдельных следственных действий, а в дальнейшем с учетом возможности производства следственных действий в условиях расширенной реальности (виртуальной и компьютерно-опосредованной)[3]. В условиях трансформации современной жизни в цифровую среду вынуждены трансформироваться и следственные действия, возможность производства которых дистанционно, удаленно (с использованием различных цифровых технологий) должны занимать в настоящее время первые места в законодательной и тактической разработках.

Так, законодатель в Казахстане уже разрешил ряд подобных проблем путем введения в УПК РК института дистанционного допроса потерпевшего и свидетеля с использованием научно-технических средств в режиме видеосвязи[4].

Полагаем, что с учетом рассмотрения сущности следственных действий и технических особенностей их производства следует выделять:

- следственные действия, проводимые в видео режиме с использованием видеоконференцсвязи и веб-связи / веб-конференции (дистанционные следственные действия);

- следственные действия, проводимые с использованием компьютерно-опосредованной реальности (виртуальные и иные дистанционные следственные действия).

Дистанционные следственные действия вербального характера, а в ряде случаев, и смешенного характера могут производиться с помощью расширенной реальности (с учетом выделения ее различных видов) и видеотехнологий (видеоконференцсвязь, веб-конференция). При этом необходимо учитывать при видеоконференцсвязи как телекоммуникационной технологии происходит передача информации по гарантированным каналам связи, а веб-конференция в смысле защищенности передаваемой информации более уязвима, поскольку представляет собой технологию передачи информации по негарантированным каналам сети Интернет. В тоже время повсеместная доступность сети Интернет обеспечивает более широкие возможности использования веб-конференции при взаимодействии субъектов уголовно-процессуальной деятельности, а с учетом реалий современной действительности потребность в использовании подобных технологий только увеличивается.

Четвертное: на законодательном уровне решение вопросов применения в доказывании электронных доказательств. Хотя в настоящее время дистанция от понятия «электронный носитель доказательств» до полноценного процессуально верно закрепленного доказательства начала сокращаться, все же еще достаточно много вопросов процессуального характера предстоит урегулировать. Полагаем, что ключевым для процессуалистов здесь является не только определение вопроса о понятийном аппарате[5] и сущности электронных доказательств, но и о том — требуется ли для электронных доказательств разрабатывать новые процессуальные правила, либо возможности их использования следует вписать в уже существующие требования уголовно-процессуального закона. В этом плане заслуживает внимание подход Е. И. Галяшиной указывающей на то, что при поиске, обнаружении, фиксации, изъятии, исследовании и хранении файлов, содержащих цифровую информацию, представленную в бинарном коде, необходимо руководствоваться принципами, закрепленными Международной организацией по цифровым доказательствам (ЮСЕ)[6].

Пятое: решение вопроса о роботизации отдельных этапов расследования либо отдельных действий с возможной интеграцией результатов данной деятельности в экосистему. Представляются перспективными идеи роботизации деятельности следователя, высказываемые Е. Н. Быстряковым и И. В. Усановым, которые предлагают следующие варианты их использования: «а) для профилактики, пресечения, предотвращения преступных посягательств и административных правонарушений; б) для исследования и запечатления обстановки содеянного и мест происшествий»[7].

Шестое: решение вопрос о возможностях использования искусственного интеллекта и интеграции результатов его деятельности в экосистему уголовного судопроизводства, а также интеграция возможностей использования — инновационных комплектов программ для анализа больших данных, позволяющих извлекать и анализировать электронную информацию, переводя ее из потенциально криминалистически значимой информации в необходимую для дальнейшего процесса расследования.

Таким образом, рассмотрение возможностей создания единой информационно-коммуникативной системы уголовного судопроизводства требует комплексного подхода и определения структурных элементов данной системы (с учетом полномочий каждого органа), технических возможностей по защите передаваемой и обрабатываемой информации, особенностей доступа и обработки информации и т. д. Каждый из данных вопросов может быть предметом самостоятельного исследования.

[1] См.: Масленникова Л. Н. Концептуальный подход к построению уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий // Вестн. Ун-та им. О. Е. Кутафина. 2020. № 10 (74). [Электронный ресурс]. — Режим доступа:https://cyberleninka.ru/article/n/kontseptualnyy-podhod-k-postroeniyu-ugolovnogo-sudoproizvodstva-obespechivayuschego-dostup-k-pravosudiyu-v-usloviyah-razvitiya (дата обращения: 24.09.2021).

[2] Более подробно эту возможность, рассматривая зарубежный опыт, описывают Л. Н. Масленникова и Л. Н. Топилина. См.: Масленникова Л. Н., Топилина Т. А. Зарубежный опыт использования онлайн-сервисов для подачи сообщения о преступлении // Законность. — 2020. — № 6. — С. 61 – 65.

[3] Так, отдельные возможности предъявления для опознания с использованием компьютерно-опосредованной реальности рассматривают: Пискунова Е. В. Использование 3D-технологий в криминалистике и судебной экспертизе// Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4. Государство и право: Реферативный журнал. — 2014. — № 4. — С. 153 – 164; Савельева М. В., Смушкин А. Б., Домнина О. В. Предъявление для опознания: психологические и тактические аспекты, перспективные методы производства// Психология и право. — 2020.— № 2.— С. 212 – 222.

[4] Более подробно см.: Нургазинов Б. К., Исмагулов К. Е. Некоторые вопросы совершенствования института дистанционного допроса в казахстанском уголовном процессе // Вестн.Ин-та законодательства и правовой информации Республики Казахстан. 2018. № 1 (50). С. 82 – 90.

[5] Понятие и характеристика, а также виды электронных доказательств рассмотрены В. Б. Веховым. См.: Вехов В. Б. Понятие, виды, классификация электронных доказательств // Развитие информационных технологий в уголовном судопроизводстве: Монография/ Под ред. докт. юрид. наук С. В. Зуева. — М., 2018. С. 71 – 83.

[6] См.: Галяшина Е. И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве: Мат-лымеждународ. науч.-практ.конф., посвящ. памяти д-ра юрид. наук, проф. П. А. Лупинской. — М., 2011.

[7] Более подробно см.: Быстряков Е. Н., Усанов И. В. Криминалистическая робототехника как новая отрасль криминалистической техники //Проблемы уголовного процесса, криминалистики и судебной экспертизы. — 2016. — № 1 (7). — С. 17 – 21; Быстряков Е. Н., Усанов И. В. Киберследователь //Проблемы уголовного процесса, криминалистики и судебной экспертизы. — 2017. — № 1 (9). — С. 29 – 32.

Сайдамарова В. В.,
начальник центра по исследованию проблем
криминалистического обеспечения деятельности ОВД
Научно-исследовательского института,
магистр юридических наук, полковник полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

ПЕРСПЕКТИВЫ И ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ 3D-СКАНИРОВАНИЯ В ОПЕРАТИВНОМ ОТОЖДЕСТВЛЕНИИ ЛИЧНОСТИ

Современное развитие науки и техники открывает различные возможности использования технологий получения подробной информации о структуре объектов в установлении личности человека. Технологии 3D-сканирования и принтинга, используемого на сегодняшний день в различных сферах науки и технике могут серьезно пополнить арсенал криминалистической техники и использоваться практически во всех видах криминалистических исследований. Технологии 3D-сканирования успешно используются в криминалистике и позволяют ее применять в реконструировании места преступления, что имеет преимущества перед простой фотографией или видеозаписью. Данная технология отражает не только декорации самого события, но и дает полное трехмерное представление о нем, что имеет особое значение при расчете расстояния отдельных следов друг от друга, а также их реальных размеров, не искаженных объективом фотоаппарата или видеокамеры.

Лаборатория Face Lab 3D (Ливерпуль, Англия) использует возможности 3D-сканирования и 3D-печати для криминалистического анализа и археологических исследований. С помощью трехмерного сканирования и специального программного обеспечения специалисты компании выполняют анализ черепно-лицевых костей неопознанных трупов для полиции, а также восстанавливают облик известных исторических личностей по их останкам[1].

Рассмотрим возможности использования 3D-технологий в криминалистической габитоскопии, а именно в оперативном распознавании внешности и при проведении портретных исследований/экспертиз. Оперативное отождествление можно сказать, что его результат дает система, ее решение не зависит от специалиста. Полученный результат будет зависеть от качества введенных исходных данных фото- и видеоизображений и имеющейся в базе данных информации подучетных лиц. Для производства криминалистических исследований/экспертиз должны применяться аппаратно-технические комплексы, предназначенные для целей портретного исследования, которые направлены для решения специалистом/экспертом диагностических и идентификационных задач. Данные комплексы должны соответствовать сегодняшним реалиям и отображать применение традиционных современных методов сравнения, оценки признаков внешности по фото- и видеоизображениям цифрового формата, с использованием возможностей нейронной сети[2, 218].

Проанализируем на примере систему, предложенную Зайде Дюраном, профессором инженерного факультета геоматики, Стамбульского технического университета, в Турции[3]. Данная система организована в виде комбинации детекторов — точек «интереса» и алгоритма идентификатора этих точек. Так точки «интереса» представляют собой аналог антропометрических точек, но на более локальном уровне в трехмерном пространстве. Несколько точек интереса образуют так называемое облако (поле, как совокупность точек характеризующих элементы и признаки внешности человека). Трехмерное распознавание лиц выполняется в три этапа. На первом этапе алгоритмы поиска точек интереса (ISS-LSP) реализуются на каждом трехмерном облаке точек[4; 5], так определяются основные точки элемента внешности. На втором этапе, обозначенные точки интереса определяются описательными алгоритмами (PFH-FPFH)[6]. Алгоритмы ISS-LSP и PFH-FPFH, являются альтернативными и выбираются специалистом по его усмотрению. В результате создаются гистограммы свойств, для каждого элемента. На третьем этапе вычисляется сходство между гистограммами двух разных точечных облаков (элементов внешности) и выполняется сопоставление, схематично алгоритм представлен (см. рис. 1).

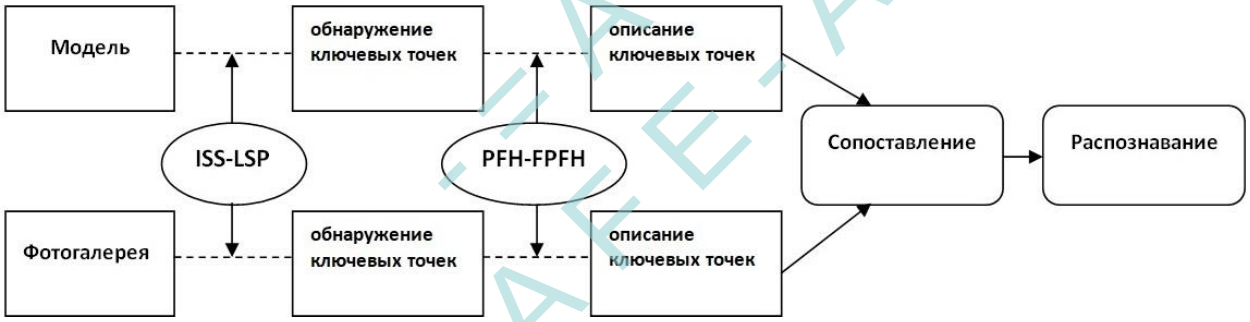


Рисунок 1. Алгоритм работы метода

В своих экспериментальных исследованиях Зайде Дюран продемонстрировал довольно высокую точность метода. Из 10 исследуемых лиц идентифицировано было 9. Однако необходимо обратить внимание, что используемые методы были эффективны только при распознавании лиц с естественным выражением лица: «… если выражение лица отличается, используемые двоичные файлы алгоритма не преуспевают. По этой причине одного использования алгоритмов для разных выражений лица недостаточно. Кроме того, небольшие движения во время сканирования изменили геометрию сканируемого лица, что значительно повлияло на результаты исследования. В целом, было установлено, что алгоритмы обладают сильным потенциалом для трехмерного распознавания лиц»[7]. То есть, сравнительные 3D лица в момент фиксации и моделирования находились в покое, мимика полностью отсутствовала. Один человек из десяти, чья внешность не была идентифицирована, двигался во время сканирования, в связи с чем, снимок исследуемого 3D лица существенно отличался от сравнительного, где испытуемый находился в полном покое.

Рассматривая использования 3D-сканирования в криминалистической трасологии и баллистики, полученный результат показывает высокую эффективность при исследовании следов применения огнестрельного оружия, рук, ног, обуви и др. материально фиксированных отображений.

В криминалистической габитоскопии 3D-сканирование демонстрирует высокие результаты при распознавании внешности с использованием программных систем, а также при проведении портретных исследований. Однако ввиду психомоторных свойств, человек не может оставаться в состоянии покоя постоянно. Небольшие движения лицевых мышц приводят к изменению геометрии лица, по-

этому процесс распознавания может происходить неправильно[8; 9]. Так в своей публикации В. Ю. Федорович, рассматривает апробацию метода 3D-сканирования и приводит пример использования класса систем предназначенных для портретной экспертизы, которые в дальнейшем необходимо развивать. К данным системам автор относит 3D-модули, модули обработки и сравнения, с помощью систем искусственного интеллекта. Данные системы направлены на выделение идентификационных признаков посредством нейронной сети, для этого в программу вводится 3D-изображения. Однако при проведении экспериментов, была подтверждена погрешность в идентификации, которая объясняется рефлекторными движениями живых лиц при получении 3D-проекции. Наряду с этим данная система показала положительный результат при получении статичных изображений, где погрешность при идентификации изображений не превышает допустимую норму[2, 218].

Выход из сложившейся ситуации нам видится в интеграции нескольких методов исследования внешности в единую систему. Для оптимизации процесса обработки, моделирования и распознавания внешности, нивелировав при этом влияние динамических искажений лица в процессе фиксации в последующем распознавании, необходима их интеграция. Модель строится на нескольких системах: 3D-сканирование и прогнозирование мимики, основанное на бихевиоризме и риггинге. Интеграция систем позволит повысить результативность использования 3D-сканирования, в криминалистической габитоскопии.

При более детальном рассмотрении приведенных выше методов можно отметить, метод «прогнозирования мимики» разработан и экспериментально подтвержден китайскими ученными Цзялей Ма, Сяншен Ли, Юаньюань Рен, Ран Ян и Цичао Чжао, из Университета Цзилинь, Чанчунь — Китай[10]. Метод учитывает динамические характеристики субъектов как личности. Модель прогнозирования интенсивности единиц действия использует трехмерные координаты по 68 ориентирам человеческого лица полученных на основе конволюционной локальной модели с ограничениями (CE-CLM)[11], которая позволяет зафиксировать динамические черты лица. На основе анализа ошибок алгоритма CE-CLM производится уменьшение размерности построенных признаков, с помощью анализа главных компонент (PCA)[12]. Для обучения моделей прогнозирования единиц действия, используется нейронная сеть с радиальной базисной функцией (RBF — Radial Basis Function Network)[13; 14]. В данном методе используется система кодирования лицевых движений FACS (Facial Action Coding System)[15; 16]. Впервые данная система была разработана Экманом и Фризеном в 1975 г.[17; 18], а затем усовершенствована в 2002 г., данная система основана на бихевиоризме[19].

Используя различные технологии распознавания лиц направленные на оперативное отождествление можно сказать, что результат отождествления дает система и ее решение не зависит от специалиста/эксперта, а полученный результат будет зависеть от качества введенных исходных данных фото- и видеоизображений. При усовершенствовании системы оперативного отождествления с помощью сканирования лиц даст нам возможность фотографически точно воспроизводить по цифровой копии внешний вид лица человека в любом положении, без каких либо специальных условий (освещение, положение лица и т. п.).

Сегодня актуальным остается вопрос получения доказательств при верификации или идентификации внешности в досудебном расследовании. Особенно в данном направлении используются материалы с камер видеонаблюдения. Однако существует ряд проблем, когда необходимо использовать для верификации и идентификации некачественно отснятый видеоматериал, зафиксировавший правонарушителя. Чаще всего используя такой видеоматериал установить личность правонарушителя не представляется возможным. В этих случаях 3D-сканирование возможно эффективно использовать, во-первых, по направлению реконструкции внешности и воссоздания субъективного портрета. Во-вторых, интегрировав и наладив взаимодействие между базами данных фото- и видеоучетов, использовать при постановке на учет 3D-сканирование с возможностями нейронной сети с радиальной базисной функцией (RBF — Radial Basis Function Network), основанной на искуственном интелекте, что даст реальную возможность верификации и идентификации внешности человека по видеоизображениям, полученным с различным ракурсом.

---

[1] Восстановление лиц с помощью 3D-сканера. [Электронный ресурс]. — Режим доступа: https://3d.globatek.ru/3d-scanners/case_studies/artec_visualizacia_lits/ (дата обращения: 20.10.2021).

[2] Федорович В. Ю. Интеграция в габитоскопии // Вестник экономической безопасности. — 2020. — № 2.

[3] 3D facial recognition using local feature-based methods and accuracy assessment / Muhammed Enes Atik , Zaide Duran Geomatics Engineering Department, Istanbul Technical University, Istanbul, 34469, Turkey, 2020.

[4] Chen H., Bhanu B. 3D free-form object recognition in range imagesusing local sur face patches, Pattern Recognition Letters, 28 (10), 1252-1262, 2007.

[5] Tombari F., Salti S., DiStefano L. Performanceevaluationof 3D keypointdetectors, InternationalJournalofComputerVision, 102 (1-3), 198 – 220, 2013.

[6] Rusu R. B., Blodow N., Beetz M. Fastpointfeaturehistograms (FPFH) for 3Dregistration, IEEEinternationalconferenceonroboticsandautomation, 3212 – 3217, 2009.

[7] 3D-распознавание лиц с использованием методов, основанных на локальных функциях, и оценка точности / Мухаммед ЭнесАтик, ЗайдеДюран, Инженерный факультет геоматики, Стамбульский технический университет, Стамбул, 34469, Турция 2020.

[8] Снетков В. А. Габитоскопия: Учебн. для вузов МВД СССР. — Волгоград, 1979.

[9] Габитоскопия: Учеб. пос. / А. М. Зинин, И. Н. Подволоцкий. — М., 2017.

[10] Landmark-Based Facial Feature Construction and Action Unit Intensity Prediction. Jialei Ma, Xiansheng Li, Yuanyuan Ren, Ran Yang, and Qichao Zhao School of Transportation, Jilin University, Changchun 130022, China 2020.

[11] Convolutional Experts Network for Facial Landmark Detection, Amir Zadeh, Tadas Baltrusaitis, Philippe MorencyCarnegieMellonUniversity 5000 ForbesAve, Pittsburgh, PA 15213, USA, 2017. = Конволюционная экспертная сеть для обнаружения ориентиров на лице, Амир Заде, Тадас Балтрушайтис, Филипп Моренси Университет Карнеги-Меллон 5000 Forbes Ave, Pittsburgh, PA 15213, США, 2017.

[12] Principal Component Analysis avid J. Olive Southern Illinois University Carbondale | SIU Department of Mathematics Ph.D. Statistics, USA 2017.

[13] Искусственные нейронные сети: Учебн. / В. С. Ростовцев. — Киров, 2014.

[14] Обучение сетей на основе радиально-базисных функций, Джеймс Маккафри, (Dr. James McCaffrey) Microsoft Research Редмонд (штат Вашингтон), 2015. [Электронный ресурс]. — Режим доступа: https://docs.microsoft.com/ru-ru/archive/msdn-magazine/2013/december/test-run-radial-basis-function-network-training (дата обращения: 20.10.2021).

[15] Тюрин А. И., Безъязыкорнов Д. С. Адаптация системы кодирования лицевых действий для работы с нейронными сетями // Современные проблемы науки и образования. — 2015. — № 1 (ч. 2).

[16] Facial Action Coding System The Manual, by Paul Ekman, Ph. D. WallaceV. Friesen, Ph. D. Joseph C. Hager, Ph. D. Salt Lake City UT United States of America, 2002

[17] P. Ekman and W. V. Friesen, Facial Action Coding System: A Technique for the easurement of Facial Movement, Consulting Psychologists Press, Palo Alto, CA, USA, 1978.

[18] P. Ekman and W. V. Friesen, Facial Action Coding System, the Manual, Research Nexus Division of Network Information Research Corporation, South Atlanta, GA, USA, 2002.

[19] Большой психологический словарь. [Электронный ресурс]. — Режим доступа: https://psychological.slovaronline.com/248 — BIHEVIORIZM (дата обращения: 20.10.2021).

Сайдамарова В. В.,
начальник центра по исследованию проблем
криминалистического обеспечения деятельности ОВД
Научно-исследовательского института,
магистр юридических наук, полковник полиции;
Шакаримова Г. М.,
научный сотрудник центра по исследованию проблем
криминалистического обеспечения деятельности ОВД
Научно-исследовательского института,
магистр юридических наук, капитан полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

СОВЕРШЕНСТВОВАНИЕ ТЕОРИИ И ПРАКТИКИ ПРОВЕДЕНИЯ КРИМИНАЛИСТИЧЕСКИХ ПОРТРЕТНЫХ ИССЛЕДОВАНИЙ

Одним из обязательных условий привлечения лица к уголовной ответственности является установление его личности. Существующий метод установления личности по личным документам, которые содержат установочные данные человека, является наиболее распространенным. Список документов, удостоверяющие личность человека предусмотренные в ч. 1 ст. 6 Закона Республики Казахстан от 29 января 2013 г. № 73-V «О документах, удостоверяющих личность»[1]. Установочные данные, представляют собой совокупность определенных биографических фактов, которые характеризуют личность[2].Сегодня, посредством программно-аппаратных методов само лицо человека становится одним из способов идентификации личности с помощью техник распознавания. Международная организация гражданской авиации (ICAO) утвердила новый стандарт паспортов, куда рекомендуется

включать изображение лица с высоким разрешением, помещаемое в чип как дополнение фотопортрета, что по мнению ряда авторов означает, переход от привычного сопоставления фотографии и человека к исследованию лица как измеряемого биометрического параметра. Все это направлено на создание единого банка биометрических данных и системы видеомониторинга.

Установление личности преступника является важной частью процесса раскрытия преступления. Не установив личности подозреваемого (обвиняемого), следователь, дознаватель и суд не выполнят важнейшие задачи уголовного судопроизводства — привлечение к уголовной ответственности лиц, их совершивших, защита лиц, общества и государства от уголовных правонарушений, предусмотренную ч. 1 ст. 8 Уголовно-процессуального кодекса Республики Казахстан[3]. Цели обеспечения этого положения закона во многом служит криминалистика и, в частности, ее раздел — криминалистическая техника, содержащий в себе серьезный арсенал приемов, способов и методов, направленных на идентификацию личности. К одним из основных методов по установлению личности человека является портретная экспертиза/исследование. На данный момент именно в данной отрасли специально научных знаний происходит разработка наиболее эффективных методов, направленных на применение личных данных о элементах и признаках внешности человека для точной идентификации его личности в досудебном расследовании.

Следует отметить, что портретная экспертиза/исследование используется не только для установления личности виновного, она обладает достаточно широкими возможностями идентификации человека по внешности, отобразившейся на различных объектах (фото- и видеоматериалах). Портретная экспертиза/исследование активно применяется для розыска лиц, скрывающихся от следствия и суда, сбежавших из мест заключения, пропавших без вести и т. п. И конечно, она имеет немаловажное значение для идентификации неопознанных трупов. В основе портретной экспертизы лежит сравнительное исследование элементов и признаков внешности.

Основы портретной экспертизы/исследования были сформированы в 60 – 70-е годы XX в. Объектами являлись фотоснимки с отобразившимися на них элементами и признаками внешности лица, к которым применялся один из способов идентификации личности — проективная геометрия. Предлагавшиеся в то время методы оценки признаков внешности человека были все еще несовершенны и требовали изменений в соответствии с современными реалиями[4].

Развитие средств и способов фотографирования позволило ввести в практику деятельности правоохранительных органов так называемую» цифровую фотографию»[5]. Особым преимуществом цифрового фотографирования является облегчение процесса получения изображения, не требующего большого объема подготовительных работ. Кроме того, большинство современных средств фотосъемки и печати позволяют получить качественные изображения с хорошей передачей объекта, цвета и полутонов. Еще одним немаловажным преимуществом цифрового изображения является то, что оно может храниться длительное время без потери своих качеств в отличие от фото, сделанного на пленку и полученного с нее позитивного изображения.

Другим и очень актуальным способом отображения внешнего облика человека является система видеофиксации, как средство объективного контроля, способная отразить картину окружающего мира. Системы видеонаблюдения стали привычным атрибутом современной жизни: ими пользуются не только правоохранительные органы, но и различные юридические лица, их размещают в местах большого скопления людей (в торгово-развлекательных центрах, аэропортах, на вокзалах, стадионах, на улицах, различных объектах городов и т. д.). Зафиксированные, средствами и приборами видеонаблюдения, анатомические и функциональные признаки человека являются на сегодняшний день одними из основных и необходимых источников информации для последующего установления личности (правонарушителя)[6, 77]. В настоящее время в связи с развитием цифровых технологий объектами портретных экспертиз/исследований все чаще становятся изображения, полученные с помощью видеозаписывающей и видеовоспроизводящей аппаратуры. Однако, несмотря на все достоинства подобных устройств, как показывает статистика органов досудебного расследования, в подавляющем большинстве случаев видеозаписи оказываются бесполезными для следствия из-за невозможности идентификации по ним преступника[7]. Кроме того, видеозапись «подлежит оценке с точки зрения относимости, допустимости, достоверности» для того, чтобы считаться полноценным доказательством.

Есть несколько объяснений подобной ситуации:

1. Использование видеокамер с небольшой разрешающей способностью приводит к появлению низкокачественного видеоматериала;

2. Портретная экспертиза/исследование ориентирована на фотоснимки с хорошо отобразившимися на них элементами лица, в меньшей степени на видеоизображения;

3. Слабая готовность центра судебных экспертиз и оперативно-криминалистических подразделений к производству портретных экспертиз/исследований по видеоизображениям из-за следующих причин:

- видеозаписи низкого качества (причиной может быть, как завышенный ракурс съемки камеры, так и оптическое искажение объектива);

- для просмотра и качественного исследования видеозаписей часто требуется специальная аппаратура и знания по ее эксплуатации, которыми эксперт/специалист может не обладать;

- возникновение процессуальных сложностей в оценке источника доказательств[8].

На данный момент в сфере портретной экспертизы/исследования существуют проблемы, которые определенным образом усложняют проведение комплексного и всестороннего изучения видеоматериалов с последующей идентификацией подозреваемого. Чаще всего сложности возникают на предварительном и детальном этапе при проведении исследования.

На предварительной стадии возникают проблемы с подготовкой видеоматериалов к проведению портретной экспертизы, в частности это касается тех случаев, когда отсутствует возможность предоставить эксперту/специалисту видеоизображение высокого качества. Хотя на данный момент разрабатываются технологии, основанные на глубоком обучении, способные не только улучшить качество видео с точки зрения идентификации лиц и объектов. Кроме того, существуют сложности установления наличия или отсутствия монтажа. Особенно затруднительно оказывается сопоставление в случае использования «морфинга»[9], когда в фотографии сохраняется сходство изначального владельца документа и использующего его мошенника. Еще одной из причин возникновения сложностей при проведении данного рода экспертизы/исследования является отсутствие четких критериев, по которым то или иное видеоизображение может быть признано пригодным для идентификации человека по признакам внешнего облика.

Что касается сравнительного исследования, на данном этапе может быть проблематичным проведение раздельного и сравнительного исследования лиц, запечатленных на видеоизображении с различным ракурсом. Несмотря на совершенствование технологии распознавания лиц, она далеко не всегда оказывается эффективна в случае идентификации подозреваемых, стремящихся не допустить своей фотофиксации. В ряде случаев возможно использование технологии создания изображения, «субъективного портрета» (фоторобот, рисованный портрет, идентификационный комплект рисунков и т. п.), основанный на воспоминании потерпевшего или очевидца. В этом случае подчас оказывается невозможным прямое сопоставление с фотографией из-за большей доли абстракции в рисунке.

Как показывает практика, для решения задач портретной экспертизы/исследования наиболее эффективным является:

Во-первых, сочетание описательных (включающих субъективную оценку экспертом комплекса значимых идентификационных признаков) и количественных (математических алгоритмов) методов решения идентификационных задач с применением современного специализированного программно-аппаратного инструментария, благодаря чему вывод по экспертизе становится более объективным, а значит и достоверным, а работа по составлению заключения портретной экспертизы/исследования выполняется в более сжатые сроки.

На сегодняшний день в Республике Казахстан отсутствует высокоэффективная специализированная программа, позволяющая выполнить все действия, необходимые для проведения портретных исследований. Существующее программное обеспечение в виде «Портретной экспертизы» — автоматизированной системы, позволяющей решать вопросы, связанные с портретными исследованиями, устарела в техническом плане и имеет ограниченные функциональные возможности, но позволяет в некоторой степени обрабатывать и подготавливать материалы, необходимые для проведения исследования. Зачастую специалистами или экспертами используются графические редакторы, не предназначенные для целей проведения портретных исследований, однако, обладающих достаточно широкими функциональными возможностями для улучшения признаков внешности на изображениях, а также позволяют подготавливать необходимые иллюстрационные материалы.

В связи с тем, программа имеет недостатки, основными из которых являются малое количество инструментов и фильтров, необходимых для улучшения отображения признаков внешности на цифровых изображениях, простые графические редакторы получили широкое распространение, которые

специально не предназначены для проведения портретных исследований. Однако их использование позволяет специалистам обработать цифровые изображения таким образом, что непригодные или условно пригодные изображения становятся пригодными для сравнительного исследования. Да и в целом инструментарий для приведения изображений к масштабу по антропометрическим точкам удобней, чем в вышеописанных программах. В целях обработки и преобразования изображений для проведения портретных исследований в системе МВД используется графический редактор «Adobe-Photoshop», обладающий достаточно широкими функциональными возможностями, в том числе необходимыми для производства портретных исследований, а именно, позволяющий менять: яркость и контрастность, резкость изображений, приводить их к единому масштабу, выравнивать по горизонтали, кадрировать. В данной программе содержится большое количество фильтров, позволяющих улучшить качество отображения признаков внешности. Однако в связи с тем, что программа бесплатна и разработана сторонней компанией, существует риск утечки информации, что недопустимо в рамках досудебного расследования.

Во-вторых, прослеживается тенденция к проведению комплексных экспертиз/исследований в силу объективной взаимосвязи портретной экспертизы/исследования с видеотехнической (для установления наличия/отсутствия признаков монтажа видеозаписи, посредством которой будут изготавливаться видеокадры для портретной экспертизы, а также для определения на ней локализации и степени изменения элементов внешности) и компьютерно-технической (для исследования технических особенностей использования программных средств, посредством которых осуществлялась фиксация цифрового изображения внешнего облика человека, а также установление факта, объема и вида его преображения)[10].

В-третьих, необходимо рассмотреть возможность выделения нового вида комплексного криминалистического исследования внешнего облика человека по видеоматериалам. Указанный вид криминалистического исследования определить следующим образом: криминалистическая идентификация внешнего облика человека по видеоматериалам — это процесс установления наличия или отсутствия тождества человека на основе отобразившихся материально-фиксированных как анатомических (статических), так и функциональных (динамических) признаков внешности на видеоизображении[11].

В 2020 г. на базе Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова Центром по исследованию проблем криминалистического обеспечения деятельности ОВД был проведен дистанционный международный Круглый стол «Современные возможности методов распознавания человека по анатомическим и функциональным признакам внешности с использованием информационных систем». По итогам работы круглого стола участники пришли к определенным выводам и были сформулированы методические рекомендации[12].

На основании вышеизложенного можно предложить следующие пути решения проблем портретной экспертизы:

- разработка регламентов применения методов и технических средств;
- развитие комплексных подходов в идентификации личности;
- усовершенствование программ, проводящих оценку идентификационной значимости выявленных признаков;
- проведение комплексной экспертизы, в рамках которой участвуют как эксперты в области цифровой фото- и видеосъемки, так и владеющие методологией портретной идентификации;
- разработка методических рекомендаций для проведения судебно-портретной экспертизы по видеоизображениям с учетом особенностей каждой стадии экспертного исследования;
- адаптировать методы оценки информативности и достоверности отображения признаков внешнего облика человека, запечатленных на видеоизображениях, к практике производства исследований на современном этапе;
- проработать вопрос о создании специализированных программных средств для производства не только исследований, но и правильного отбора сравнительных образцов, в том числе для формирования, ведения и использования криминалистического видеоучета;
- внести в учебные программы подготовки и повышения квалификации экспертов, специалистов-криминалистов новые тематические разделы, направленные на приобретение навыков исследования внешнего облика человека по видеоизображению[13, 26].

Подводя итоги вышеизложенного, необходимо отметить широкую распространенность данной проблематики. Выходом из которой, может являться только разработка отечественного специализиро-

ванного программного обеспечения для проведения портретных экспертиз/исследований от стадии предварительного исследования до оценки результатов исследования и формулирования выводов. Будущая автоматизированная система должна позволять производить обработку изображений на основе нейронной сети (искусственного интеллекта). Использование данной программы должно позволять проводить измерения на изображениях между антропометрическими точками с возможностью трекинга видеоизображений, отдельной опцией должен быть инструментарий методов сравнения портретной идентификации, возможность использования большого количества фильтров и инструментов, позволяющих не только проводить графические правки для улучшения изображения, возможно даже его восстановления, но и подготавливать иллюстрации каждого этапа исследования. Данная автоматизированная система должна обладать мультиплатформенностью, исправно работать на любых современных операционных системах, поколения Windows, Linux или Ubuntu. Технически программа должна быть проста в освоении и не вызывать трудностей работы даже у людей с недостатком знаний работы компьютера.

---

[1] Закон Республики Казахстан «О документах, удостоверяющих личность» от 29 января 2013 г. № 73-V.

[2] Белицкий В. Ю. Проблема уголовного преследования лица, личность которого не установлена, и вариант ее решения // Юридическая наука и правоохранительная практика. — 2016. — № 2 (36). — С. 110 – 111.

[3] Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК.

[4] Зинин А. М. Проблемные вопросы методического обеспечения судебно-портретной экспертизы // Вестн. Московск. ун-та МВД России. 2013. № 4. С. 7 – 8.

[5] Криминалистическая цифровая фотография: Учеб. пос. / А. Аубакиров, С. Коваленко. — Алматы, 2001.

[6] Сайдамарова В. В., Шакаримова Г. М. Особенности использования цифровых видеоизображений в криминалистических исследованиях // Хабаршы — Вестник Карагандинск. акад. МВД РК им. Б. Бейсенова. 2021. № 3 (73).

[7] Бубербаев Н. Д. О состоянии выявляемости уголовных правонарушений камерами видеонаблюдения // Хабаршы — Вестник Карагандинск. акад. МВД РК им. Б. Бейсенова. 2021. № 2. С. 4 – 5.

[8] Попов В. Л. Особенности производства портретных экспертиз по низкокачественным видеоизображениям // Юридическая наука и правоохранительная практика. — 2015. — № 4. — С. 157 – 161.

[9] Морфинг (англ. morphing, трансформация) — технология в компьютерной анимации, визуальный эффект, создающий впечатление плавной трансформации одного объекта в другой. Используется в игровом и телевизионном кино, в телевизионной рекламе. Встречается в трехмерной и двухмерной (как растровой, так и векторной) графике.Материал из Википедии — свободной энциклопедии. [Электронный ресурс] //https://wikipedia.ru/

[10] Хайрусов Д. С. Портретная экспертиза // Технологии в инфосфере. — 2021. — № 2 (2). — С. 54 – 67.

[11] Saidamarova V. V. Methodological basis of the person's external appearance study using video images // Ғылым. — 2021. — № 2 (69). — С. 30 – 35.

[12] Современные возможности методов распознавания человека по анатомическим и функциональным признакам внешности с использованием информационных систем: Мат-лы международ. дистанц. науч.-практ. конф. — Караганда, 2021. С. 50 – 52.

[13] Сайдамарова В. В. Современный подход к проведению судебно-портретной экспертизы по видеоматериалам // Современные возможности методов распознавания человека по анатомическим и функциональным признакам внешности с использованием информационных систем: Мат-лы международ. дистанц. науч.-практ. конф. — Караганда, 2021.

Сайдамарова В. В.,
начальник центра по исследованию проблем
криминалистического обеспечения деятельности ОВД
Научно-исследовательского института,
магистр юридических наук, полковник полиции;
Шарипов С. С.,
старший научный сотрудник центра по исследованию проблем
криминалистического обеспечения деятельности ОВД
Научно-исследовательского института,
магистр юридических наук, майор полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Использование 3D-технологий в криминалистическом отождествлении человека по походке

Криминалистическое исследование походки человека являет собой систематическое изучение локомоции человека с целью дальнейшего сравнения, анализа и оценки особенностей походки подозре-

ваемого лица для его последующей идентификации. Наука о походке человека является частью развивающейся в настоящее время криминалистической биометрии и габитоскопии. Следы локомоции человека могут встречаться во многих типах дел, таких как кража со взломом, ограбление, сексуальное нападение, наезд и бегство, кража из магазина, убийство, похищение и т. д. Общий источник доказательственной информации для криминалистического исследования походки включает в себя как серию следов ног или обуви на месте происшествия, так и записи камер видеонаблюдения. Рассмотрим эти два источника подробнее.

1. Анализ рисунка походки на поверхности (состоящей минимум из 3 – 4 последовательных следов ног/обуви) проводится с учетом различных параметров, включая размеры: общую форму следа, линию направления движения ходьбы, длину шага левой / правой ходьбы, ширину постановки ног, угол разворота стоп, а также отдельные анатомические признаки следа. Измерения, относящиеся к шагу и длине шага, могут указывать на характер походки человека, например, нормальная походка, бег и т. д. и связанные с этим отклонения, если таковые имеются. Этот анализ также может помочь в определении роста, пола, возраста и массы тела подозреваемого. Может быть составлено общее представление о внешности человека, оставившего след. Сравнение между лицом, совершившим преступление, и подозреваемым производится путем систематического анализа и оценки походки. Информация, касающаяся взаимосвязи длины шага и длины следа с ростом, может дать ценную информацию в процессе сравнения и анализа походки. Некоторые исследователи обнаружили статистическую корреляцию между длиной шага с ростом человека с учетом различных контролируемых условий[1].

2. Анализ походки по записям/видеозаписям камер видеонаблюдения: Появление камер видеонаблюдения и устройств, позволяющих записывать видео (видеокамеры, мобильные телефоны, камеры на приборной панели, камеры наблюдения, дорожные камеры и т. д.), вывело методику исследования походки на новый уровень. В настоящее время для изучения походки человека используются видеозаписи и записи с камер видеонаблюдения[2]. До изобретения и использования систем видеонаблюдения следственные органы полагались на очевидцев, которые могли «увидеть» на месте человека с определенной «манерой ходьбы». Однако научные данные свидетельствуют о том, что на дискриминационную силу таких показаний нельзя полагаться как на единственное доказательство. Хотя в отсутствие других биометрических идентификаторов на видеозаписи, криминалистическое исследование походки играет важную вспомогательную роль. Записи камер видеонаблюдения с места совершения правонарушения, записи камер наблюдения, записи дорожных камер, записи с камер, установленных на приборной панели автомобилей, записи с мобильных телефонов (потерпевшего, свидетеля или других лиц) и т.д. должны быть собраны в соответствии с установленным порядком и исследованы.

Походка человека уже давно является предметом активного изучения, не только в криминалистике, но и в медицине (выявление аномалий походки и нарушений, вызванных инсультом или церебральным параличом)[3], биометрии[4], и ряде других дисциплин в своей сфере так или иначе соприкасающихся с изучением двигательных проявлений человека. Как следствие, на современном этапе развития информационных технологий, разработано внушительное количество средств и методов цифровой фиксации и исследования признаков внешности человека, в частности походки. Такие как: специальные датчики пола (педальное давление)[5]; инерциальные датчики, такие как акселерометры и гироскопы, в настоящее время широко используются в целях фиксации динамики походки[6]; радар с непрерывной волной[7]; нейронной сети[8]; с помощью 3D-моделей; и даже использованием Wi-Fi-устройств[9].

Учитывая ограниченный формат статьи, мы рассмотрим исключительно проблематику 3D-фиксации и идентификации признаков походки человека.

С развитием методов компьютерной визуализации появляется множество подходов к идентификации человека по движениям в видео, использующих как естественные биометрические характеристики (скелет человека, его силуэт, их изменение во время ходьбы), так и абстрактные признаки. Современные методы объединяют в себе классические алгоритмы анализа видеоизображений и новые подходы, демонстрирующие высокие результаты. Однако в случае с использованием 3D-моделей, как сравнительного материала, подобные решения абсолютно неприменимы. Это связано с тем, что сканируемый человек в момент регистрации с помощью 3D должен, находиться в состоянии покоя, не проявляя ни малейшего движения. В противном случае, движения во время фиксации меняют геометрию сканируемого участка тела, что в результате приводит к отрицательному изображению и дальнейшей невозможности идентификации[10]. При условии, что объектом исследования в нашем случае выступают функциональные признаки внешности, в частности походка, то на первый взгляд приме-

нение 3D-технологий, не представляется возможным, и исключительные возможности создания и исследование 3D-моделей походки человека, обходят стороной столь актуальное проявление человеческого бытия, как локомоция. К решению данной проблемы, мы подошли нестандартным образом и обратились в сферу компьютерной мультипликационной анимации.

Система «MoCap — Motioncapture» разработана для записи движений, выполняемых человеком, и используется в компьютерной анимации для создания анимированных персонажей в видеоиграх или в кино. Но эти системы также используются в терапевтических целях или для профессиональных спортсменов. Измерение движения осуществляется с помощью датчиков, закрепленных на теле человека, или с помощью маркеров, положение которых в пространстве легко отличить от окружающей среды с помощью сенсорной системы. Положение и ориентация каждого из датчиков дискретизируется во времени и может быть получена в трехмерном пространстве сразу после измерения или после постобработки. Полученные данные могут использоваться в компьютерных моделях для создания движений синтезированного персонажа[11].

За последние несколько лет большинство представленных характеристик походки были основаны на геометрической основе. Они обычно сочетают статические параметры тела (длина костей, рост человека) с динамическими характеристиками походки, такими как длина шага, скорость ходьбы, углы наклона суставов и межсуставные расстояния, а также различные статистические данные (среднее, стандартное отклонение или локальные / глобальные экстремумы) их сигналов. Мы же акцентируем внимание на выделение и фиксацию непосредственно динамических параметров.

В целях усовершенствования метода распознавания походки человека с помощью 3D-моделей, минуя отрицательное влияние локомоции как таковой на результативность 3D-сканирования, мы предлагаем объединить три системы: 3D-сканирование, MoCap, и глубокую рекуррентную нейронную сеть (DCNN)[12]. Данная нейронная сеть свертывает входные сигналы в пространственной области и хорошо подходит для обработки массивных сигналов, например, изображений.

Необходимо отметить, что представленная в статье система применима исключительно к криминалистической видео регистрации и исключает возможность распознавания личности человека по походке онлайн.

Рассмотрим алгоритм работы данной системы. На первоначальном этапе регистрируемое лицо сканируется в полный рост (вертикальное сканирование)[13], после чего информация о внешнем облике оцифровывается и создается 3D-модель. Затем, в соответствии с инструкцией по постановке регистрируемого лица на криминалистический видеоучет (Приказ Министра внутренних дел Республики Казахстан от «21» июля 2014 г. № 75 ДСП «Правила осуществления оперативно-криминалистической деятельности в органах внутренних дел»), человеку предлагается пройти. Предварительно к нему прикрепляются специальные датчики движения, для того, чтобы считывать информацию о работе суставов во время ходьбы. Процесс передвижения человека соответственно фиксируется на видеокамеру, параллельно линии его передвижения.

Полученная информация анализируется. Компьютерный анализ включает алгоритмы, которые могут быть либо на основе моделей, либо на основе внешнего вида. В случае криминалистической регистрации анализ будет осуществляться на основе внешнего вида с использованием программы DCNN. Подход, работает на фиксированных ориентирах для извлечения особенностей походки. Это делается путем предварительного определения ориентиров с помощью модели человека. В дальнейшем модель на основе внешнего вида функционирует путем извлечения последовательностей силуэтов идущего человека. Заключительным этапом будет передача информации о походке через рекуррентную нейронную сеть с последующим наложением и адаптацией на 3D-модель регистрируемого лица. В итоге мы имеем цифровую трехмерную копию регистрируемого лица, которую при необходимости, можно заставить и пройтись. При этом манера походки будет соответствовать оригиналу со 100 % идентичностью.

В заключении хотелось бы отметить, что современное развитие цифровых технологий, открывает правоохранительным органам колоссальные возможности в раскрытии и расследовании преступлений. Их использование в повседневной работе сотрудниками органов досудебного расследования во многом будет экономить время расследования, и повысит результативность.

[1] Трасология и трасологическая экспертиза: Учебн. / И. В. Кантор (отв. редактор), В. А. Ярмак, Н. Ю. Жигалов, П. П. Смольяков (отв. секретарь). — М., 2002.

[2] Методические основы криминалистической идентификации и диагностики человека по его динамическим признакам: Монография / В. Г. Булгаков; под ред. А. М. Зинина. — М., 2014.

[3] Особенности сенсомоторных нарушений у пациентов в разных периодах после ишемического инсульта / Е. В. Екушева, Е. С. Кипарисова, Е. В. Ширшова. Федеральное государственное бюджетное образовательное учреждение дополнительного профессионального образования «Институт повышения квалификации Федерального медико-биологического агентства». — М., 2017.

[4] Сазанов В. А., Тихонов С. Г., кафедра интеллектуальных систем, ФРФиКТ, Белорусский государственный университет, Беларусь, г. Минск, 2015.

[5] Spatiotemporal Analysis by Deep Learning of Gait Signatures From Floor Sensors, Abdullah S. Alharthi; Alexander J. Casson; Krikor B. Ozanyan, Department of Electrical and Electronic Engineering The University of Manchester, Manchester, U. K., 2021.

[6] Gait Phase Recognition Using Deep Convolutional Neural Network with Inertial Measurement Units, Q. Zouand, Y. Zhao are with the School of ComputerScience, Wuhan University, Wuhan 430072, P. R. China, 2020.

[7] Classification of human motion using radar micro-doppler signatures with hiddenmarkovmodels, Padar, Mehmet Onur M. S., Department of Electrical and Electronics Engineering, 2016.

[8] Соколова А. И., Конушин А. С. Методы идентификации человека по походке в видео // Тр. ИСП РАН, 2019.

[9] Gait Recognition Using WiFi Signals WeiWang Alex X. Liu Muhammad Shahzad State Key Laboratory for Novel Software Technology, Nanjing University, China Department of Computer Science and Engineering, Michigan State University, USA, 2016.

[10] 3D-распознавание лиц с использованием методов, основанных на локальных функциях, и оценка точности / Мухаммед Энес Атик, Зайде Дюран, Инженерный факультет геоматики, Стамбульский технический университет, Стамбул, 34469, Турция 2020.

[11] Motioncapture, Damien Courouss´e, Enactionadnen active interfaces: a handbook of terms, Damien Courouss´e CEA — Département Architectures Conception Logiciels Embarqués, 2007.

[12] Deep Learning-Based Gait Recognition Using Smartphones in the Wild Qin Zou, Yanling Wang, Qian Wang, Yi Zhao, Qingquan Li, IEEE Transactions on Information Forensics and Security. Vol. 15, no. 1, pp. 3197 – 3212, 2020.

[13] 3D-сканирование тела человека от А до Я. [Электронный ресурс]. — Режим доступа: https://www.artec3d.com/ru/learning-center/3d-body-scanner (дата обращения: 08.11.2021).

Свободный Ф. К.,
старший преподаватель кафедры управленияи психологии
следственной деятельности, кандидат психологических наук,
доцент, майор юстиции
(Московская академия Следственного комитета
Российской Федерации)

ОПРЕДЕЛЕНИЕ ОСВЕДОМЛЕННОСТИ ЛИЦА ОБ ОБСТОЯТЕЛЬСТВАХ ПРЕСТУПЛЕНИЯ В ПРОЦЕССЕ ПСИХОФИЗИОЛОГИЧЕСКОГО ЭКСПЕРИМЕНТА

Событие преступления, как и любое другое значимое для человека событие, становится частью жизненного опыта его личности, представленного в виде психологических феноменов — определенных сведений, знаний, представлений о преступлении, а также отношений, оценок, установок по отношению к произошедшему преступлению и т. д. Наличие сведений, знаний о чем-либо, обладание информацией о чем- либо, называется осведомленностью, а хорошая осведомленность, владение большим объемом информации — информированностью[1]. Лицо, совершившее преступление, наиболее полно информировано о преступном событии и обладает, так называемой, «виновной осведомленностью»[2] — т. е. знает такие обстоятельства совершения преступления, которые неизвестны лицам, непричастным к преступлению.

В процессе расследования преступлений следователи часто сталкиваются с ситуацией отрицания допрашиваемым лицом своей осведомленности об обстоятельствах преступления. При этом допрашиваемые лица демонстрируют, так называемые, «улики поведения»[3]: вербальные (слова, интонации, паузы в речи т. д.) и невербальные (движения, мимика, жесты и т. д.) реакции, которые, косвенно, могут свидетельствовать о знании ими обстоятельств конкретного преступного события.

Но если термин «виновная осведомленность» больше подходит преступнику, то относительно других участников расследуемого события (свидетель, потерпевший) более корректным будет говорить просто об осведомленности или информированности данных лиц о конкретных деталях преступления.

«Информированность личности о расследуемом событии» — это составляющая опыта личности, выражающаяся в наличии у человека относительно устойчивой системы объективных знаний и субъ-

ективных представлений о конкретном событии его жизни, обстоятельства которого сейчас расследуются правоохранительными органами[4].

Исследование специфики, структуры и содержания таких психологических феноменов как знания, сведения, осведомленность, информированность, представления и т. п. входит в компетенцию психолога, а разрешение вопросов, возникающих перед следствием и судом при необходимости квалифицированной оценки психических явлений, требует проведения судебной психологической экспертизы. К эмпирическим методам психологического исследования относить такие методы, как: биографический или архивный метод, наблюдение, беседа, эксперимент. Указанные методы, в соответствующей модификации, успешно применимы для целей диагностики осведомленности лица о преступлении.

Одним из эффективных методов выявления информированности лица об обстоятельствах преступления является специально организованный психологический эксперимент (ассоциативный эксперимент[5], сопряженная моторная методика[6], исследование с использованием полиграфа, исследование с использованием технологии отслеживания движений глаз и т. д.), направленный на выявление субъективной значимости для подэкспертного стимулов, которые в виде вопросов (фраз) предъявляет подэкспертному эксперт и которые содержат информацию о деталях (настоящих, возможных, вымышленных) расследуемого события. Данный метод, при строгом соблюдении методологии психологического эксперимента (в частности: серийного предъявления независимых переменных, качественной фиксации зависимых переменных, контроля и учета дополнительных переменных[7]) позволяет на основе выявленной субъективной значимости для подэкспертного стимулов, несущих информацию о деталях расследуемого события, сформулировать вероятностный вывод об особенностях осведомленности или неосведомленности подэкспертного лица о реальных обстоятельствах произошедшего преступления.

Исследование на полиграфе предполагает восприятие испытуемым стимулов, содержание которых им осознается[8]. В процессе исследования испытуемый может получать информацию о преступлении от специалиста, что значительно затрудняет дальнейшую диагностику осведомленности лица о преступлении.

В связи с этим перспективным представляется экспериментальное изучение осведомленности лица о деталях преступления через анализ его реакций на неосознаваемые стимулы. Реакции на неосознаваемые стимулы являются важной составляющей организации психической деятельности человека, при этом неосознаваемые стимулы, имеющие для человека эмоциональную значимость, вызывают более выраженные реакции организма по сравнению с другими неосознаваемыми стимулами[9].

В нашем исследовании, мы предприняли попытку выявить осведомленность лица о деталях преступления через анализ динамики его кожно-гальванической реакции (КГР) на неосознаваемые визуальные стимулы, содержащие информацию об обстоятельствах расследуемого преступления.

Исследование проводилось в одном из отделов полиции г. Барнаула и строилось в соответствии с методологией психологического эксперимента. В качестве испытуемого выступил подозреваемый в совершении кражи, отрицавший групповой характер совершенного преступления и факт своего знакомства с человеком, который, по оперативным данным, являлся сообщником подозреваемого.

Для эксперимента нами были отобраны 4 фотографии лиц мужского пола, сопоставимых с фотографией предполагаемого сообщника подозреваемого. Были составлены четыре последовательностей фотографий для предъявления их испытуемому в стробоскопическом режиме, исключавшим осознание фотографий подозреваемым. При этом одна из четырех последовательностей фотографий содержала фотографию предполагаемого сообщника подозреваемого. Последовательности фотографий предъявлялись испытуемому серийно 10 раз. В каждой серии порядок предъявления последовательностей фотографий менялся. В процессе предъявления фотографий осуществлялась запись динамики КГР с фаланг указательного и среднего пальцев руки испытуемого.

В результате проведенного нами эксперимента было установлено, что кожно-гальванические реакции подозреваемого на последовательность фотографий, содержащих фотографию предполагаемого сообщника подозреваемого, по интенсивности и длительности устойчиво превышали КГР, возникавшие в ответ на последовательности фотографий, не содержащих фотографию предполагаемого сообщника подозреваемого. Был сделан вывод, что фотография предполагаемого сообщника подозреваемого является для подозреваемого эмоционально значимой и, вероятно, подозреваемый знаком с предполагаемым сообщником.

Результаты исследования были озвучены следователю и подозреваемому, после чего подтвердились признательными показаниями подозреваемого и результатами других следственных действий.

Полагаем, что применение экспериментальных методов психологической диагностики способствует решению задач по определению особенностей осведомленности обследуемого лица об обстоятельствах расследуемого события и положительно сказывается на качестве расследования преступлений.

---

[1] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. — М., 2000. [Электронный ресурс].— Режим доступа:https://www.efremova.info/word (дата обращения: 12.09.2021).

[2] Мозяков В. В. Руководство для следователей. — М., 2005.

[3] Чегодаева С. С. Криминалистическое исследование улик поведения: Автореф. дис. … канд. юрид. наук. — М., 2000.

[4] Свободный Ф. К. Судебная психофизиологическая экспертиза с использованием полиграфа как новый вид судебной психологической экспертизы // Вестн.Алтайск. акад. экономики и права. 2011. № 1(19). С. 163 – 168.

[5] Тойм К. Ассоциативный эксперимент в психодиагностике в XIX веке // Учен. зап.Тартуск. ун-та. 1978. № 465.

[6] Лурия А. Р. Сопряженная моторная методика и ее применение в исследовании аффективных реакций // Проблемы современной психологии. — М., 1928.Т. 3.

[7] Дружинин В. Н. Экспериментальная психология: Учебн. для вузов. — СПб, 2008.

[8] Детков А. П. Определение предмета, объектов и компетенции судебной психологической экспертизы информированности личности о расследуемом событии // Изв.Алтайск. гос. ун-та. 2015. № 2/2. С. 32 – 36.

[9] Костандов Э. А. Восприятие и эмоции. — М., 1977.

Стамбеков О. Е.,
криминалист Управления криминалистического обеспечения
досудебного расследования Оперативно-криминалистического департамента
МВД Республики Казахстан
(г. Нур-Султан)

ИСТОЧНИК ЭКСПЕРТНОГО СВЕТА. ВОЗМОЖНОСТИ ЕГО ИСПОЛЬЗОВАНИЯ ПРИ ВЫЯВЛЕНИИ СЛЕДОВ В ХОДЕ ОСМОТРА ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ НА МЕСТЕ ПРОИСШЕСТВИЯ

Как правило, любое общественно опасное деяние сопровождается изменением вещной обстановки. Данный процесс обусловлен законом отражения и носит объективный характер. В науке криминалистике подобного рода изменения получили название следов уголовных правонарушений. Кокин А. В. разделяет следы преступлений на две категории. При этом относя к первой категории материальные следы, возникающие в результате контакта разного рода объектов, а идеальные следы, отображающиеся в сознании человека ко второй[1, 9]. Так как следы преступления причинно связаны с событием преступления, они являются источником доказательственной информации как о лице его совершившим, так и обстоятельствах совершения деяния. Однако для того, чтобы можно было использовать данные сведения в ходе раскрытия и расследования уголовных правонарушений следы для начала должны быть обнаружены, зафиксированы, изъяты, и затем исследованы. Для решения данных задач проводятся оперативно-розыскные мероприятия и следственные действия, в процессе которых обычно применяются различные криминалистические средства и методы.

Вместе с тем в безотлагательных случаях, когда необходимо получить розыскную и доказательственную информацию, предварительное исследование следов целесообразно проводить на месте происшествия.

Обнаружение предполагает совершение действий по выявлению невидимых, слабо видимых и видимых следов преступления, к которым можно отнести следы рук, следы биологического происхождения (кровь, слюна, сперма и др.), транспортных средств, взлома, применения огнестрельного оружия и др. Зачастую следы на месте происшествия очень малы и фрагментарны, слабо различимы или и вовсе невидимы. Кроме того, лица совершающие деяния принимают необходимые меры, направленные на сокрытие следов (их уничтожение). Для выявления таких следов специалисты используют специальные поисковые технические средства.

По мнению О. А. Бариновой успешность расследования и раскрытия преступления, установления лица, совершившего общественно опасное деяние, зачастую зависит от информации, которая была получена в ходе проведения осмотра места происшествия[2]. При этом на наш взгляд необходимо учи-

тывать, что при подготовке к проведению данного следственного действия сложно заранее спрогнозировать, какие технические средства будут необходимы для работы со следами на месте. В этой связи немаловажное значение приобретает наличие в арсенале специалиста-криминалиста многофункциональной криминалистической техники, которая позволила бы осуществить поиск и обнаружение вещественных доказательств, а также осуществить их предварительное исследование. Поэтому мы хотим в данной статье остановиться на рассмотрении модуля криминалистического света.

Ультрафиолетовые осветители позволяют обнаруживать невидимые и слабовидимые следы биологического происхождения, некоторых химических веществ (нефтепродуктов, клея и пр.), которые под действием ультрафиолетовых лучей люминесцируют либо отличаются по оттенку от фона поверхности, на которой они находятся.

Важнейшими элементами источников света являются различные светофильтры, влияющие на интенсивность, направление, диапазон волн и иные характеристики светового потока.

Возможности источника экспертного света мы постараемся раскрыть на примере комплексе «SVX-3Ki», который позволяет проводить широкий спектр обнаружения следов на качественно новом уровне; получать цифровые изображения с возможностью дальнейшего их использования в работе.

Так, сотрудниками Оперативно-криминалистическим департамента МВД Республики Казахстан была проведена апробация источников экспертного света «SVX-3Ki»: модуля криминалистического света — ультрафиолетовый SVX-K365 (365 нм ± 5 нм), модуля SVX-K450 криминалистического света — синий (450 нм ± 10 нм), производства компании ООО «Евразийская Технологическая Группа» (Россия).

Источники позиционируются производителем как инструменты для эффективного обнаружения следов рук и различных видов следов биологического происхождения, непосредственно на месте происшествия или в лабораторных условиях.

Источники экспертного света представляют собой источники светодиодного типа, свет генерируется с использованием инновационных полупроводников на базе SMD светодиодов. Высокая мощность прибора и длительное время работы от одного заряда аккумуляторов достигается путем применения новых LED технологий.

Источники экспертного света выполнены из ударопрочного алюминиевого сплава с защитным изоляционным покрытием, устойчивым к механическим воздействиям и температурным перепадам. Степень защиты IP65. Специальная электронная система обеспечивает равномерность светового потока в течение всей продолжительности работы модуля.

Для отслеживания уровня заряда аккумулятора имеется световой индикатор. Отличительной особенностью источников является равномерное, бестеневое освещение по всей площади. В качестве источника питания использованы перезаряжаемые рукоятка — аккумулятор (зарядное устройство и инвертер 12 – 220 В). При работе каждая рукоятка-аккумулятор, оснащенная магнитом, позволяет надежно фиксировать прибор на ферромагнитных поверхностях с возможностью крепления его как на горизонтальных, так и на вертикальных поверхностях.

Для каждого источника света в комплекте имеется индивидуальный накамерный светофильтр (с резьбовым креплением для крепления к объективу фотоаппарата). Светофильтры выполнены из оптического стекла. Вместе с тем, с учетом мощности источника в целях безопасности участников в комплекте имеются очки-светофильтры.

Целью апробации являлась оценка эффективности использования источников света для выявления различных следов (невидимых и слабовидимых) при осмотре вещественных доказательств на месте происшествия и в лабораторных условиях. В качестве критериев оценки, брались такие показатели, как удобство, практичность и надежность конструкции, время работы, мощность освещения, и собственно возможность выявления заявленных видов следов. В ходе работы с источниками в лабораторных условиях было установлено следующее.

Модуль SVX-K365 длиной волны 365 нм проявил себя с положительной стороны при обнаружении волокон и микрочастиц.

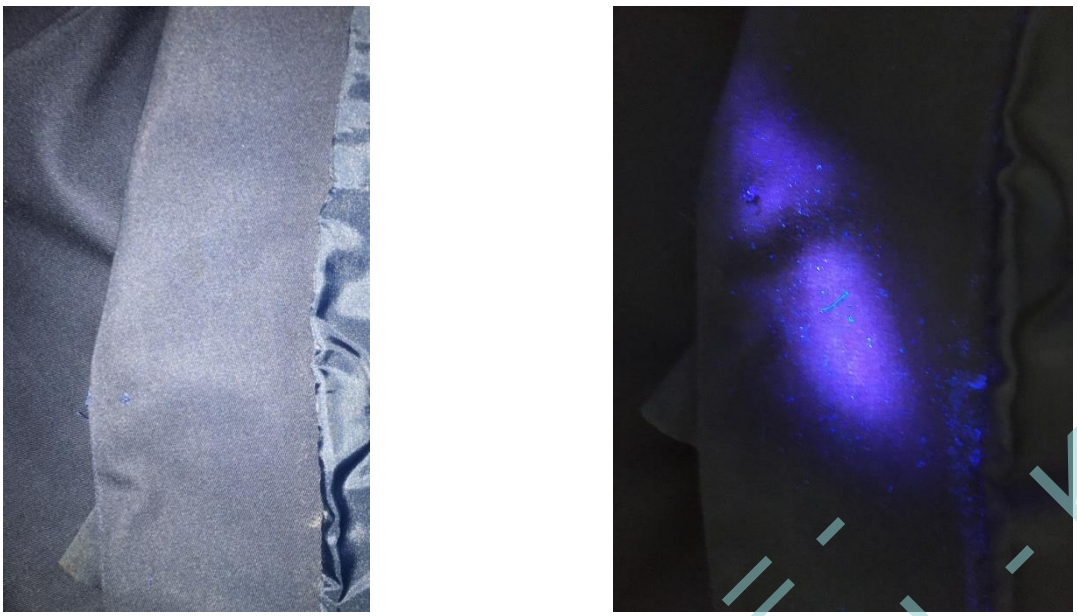


Рис. 1. Визуализация скрытых волокон, микрочастиц с помощью комплекса экспертного света

Модуль SVX-K450 с длиной волны 450 нм проявил себя особенно хорошо при поиске старых следов рук на оштукатуренных стенах, а также потожировых следов на тканях.

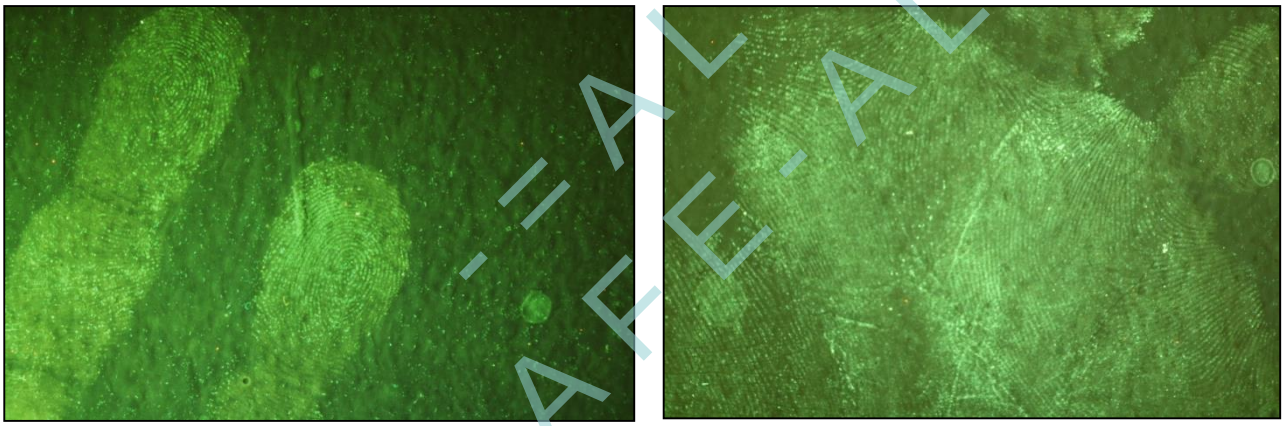


Рис. 2. Визуализация скрытых следов рук
на оштукатуренных стенах с помощью комплекса экспертного света

Результаты апробации показали:
конструкция источников света надежна, удобна, используемые компоненты и технологии предназначены для интенсивной отказоустойчивой работы в сложных условиях окружающей среды. Источники экспертного света позволяют выполнять заявленные задачи в реальных условиях работы специалистов, способны существенно облегчить обнаружение заявленных следов и объектов.

Использование излучения в двух (УФ/Синий) диапазонах значительно увеличивает вероятность обнаружения искомых следов.

В заключении хотелось бы отметить, что полученные результаты апробации позволили сделать вывод о допустимости использования исследованных источников экспертного света для обнаружения невидимых и слабовидимых следов как при работе в ходе осмотров мест происшествия, так и в лабораторных условиях.

[1] Криминалистическая техника: Учебн. / Под ред. К. Е. Демина. — М., 2017.

[2] Баринова О. А. Использование мобильного источника криминалистического света «МИКС – 450» для обнаружения следов преступления // Российский следователь. — 2020. — № 12. — С. 3 – 5.

Степаненко Д. А.,
профессор кафедры криминалистики,
судебных экспертиз и юридической психологии
Института юстиции, доктор юридических наук, профессор
(Байкальский государственный университет,
Российская Федерация, г. Иркутск)

КРИМИНАЛИСТИЧЕСКИЕ ТЕХНОЛОГИИ НОВОГО ПОКОЛЕНИЯ: СИНЕРГИЯ КРИМИНАЛИСТИКИ, ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И НЕЙРОТЕХНОЛОГИЙ

В 1992 г., определяя предмет криминалистики, профессор В. А. Образцов акцентировал внимание научной общественности на том, что криминалистика — это наука о принципах, методах, технологиях реализации норм уголовного материального права и процессуального права в антикриминальной деятельности органов дознания и предварительного следствия[1, 38]. Не будем анализировать новаторский подход автора к трактовке предмета криминалистики, хоть и уходящего корнями в гроссовское определение криминалистической науки, остановимся на том, что существенно для этой статьи — использование термина технология. Виктор Александрович один из первых ввел в оборот криминалистического языка данный термин, придав ему криминалистическое звучание. Сегодня этот термин используется широко, а проблематика исследований технологического характера вышла на уровень общетеоретического криминалистического анализа.

«Криминалистическая технология — продукт научно-исследовательской деятельности, разрабатываемая в криминалистике типовая информационно-функциональная модель структуры и содержания задач, процесса и средств ее решения, реализуемых в целях уголовно-процессуального выявления, раскрытия, пресечения, предотвращения преступлений и осуществления от имени государства уголовного преследования (изобличения) подозреваемых и обвиняемых в приготовлении к совершению и (или) совершении инкриминируемых им деяний»[2, 59]. Безусловно, эта модель имеет уровни, рассчитанные на решение тех или иных тактических задач, стоящих перед лицами, осуществляющими криминалистическое исследование преступного события: тактические задачи доследственного производства; задачи, реализуемые на отдельных этапах поисково-познавательной деятельности до и после возбуждения уголовного дела; тактические задачи производства отдельных следственных, иных процессуальных действий…

Теоретический конструкт криминалистических технологий в основном построен. Сегодня криминалистика готова начать создавать реальные практикоориентированные технологии, позволяющие решать структурированные в теории тактические задачи с учетом тех возможностей, которые нам открывает научно-технический прогресс.

Постнеклассический этап развития науки[3], на котором мы находимся, предполагает смену вектора в подходах исследований. Наука может исследовать сложные и сверхсложные системы, открытые и способные к самоорганизации. Объектом наук становятся «человекоразмерные» комплексы, в которых человек — основной компонент. Признаками этого этапа развития современной науки является междисциплинарность, синергетика, учет вероятности и некоторой неупорядоченности элементов (компонентов) исследуемых систем, нелинейности и т.п. Думается, что для криминалистической науки это не ново. Функциональная составляющая криминалистики детерминировала ее мультиинтегративный характер и сосредоточенность на субъекте, с одной стороны совершающем преступление и таким образом преобразующем действительность для реализации своей потребностно-мотивационной сферы, с другой — на лице, осуществляющем криминалистическую деятельность для раскрытия и расследования преступного события, действующего в различных криминалистически значимых ситуациях. Решение тактических задач[4] связано, прежде всего, с осмыслением и анализом информации, полученной и имеющейся в распоряжении следователя (дознавателя) и следственной ситуации, формированием цели решения задачи в соответствии и в рамках уголовно-процессуальных требований; выявление всех возможных вариантов решения стоящей задачи; подбор средств, методов, технологий достижения цели; определение субъектного состава, участвующего в решении задачи; планирование действий по использованию технико- и тактико-криминалистических средств, сроков; контрольная проверка построенной мысленной модели решения тактической задачи; принятие итогового решения о реализации плана. Сформированное криминалистическое мышление[5] следователя,

несомненно, помогает быстрой ориентировке в поступающей информации, анализе факторов, условий и обстоятельств, в которых он работает, но происходящие изменения в укладе общественной жизни и интенсивно меняющейся среды с «аналоговой» на «цифровую», следователю все сложнее «барахтаться» в многослойных информационных потоках, большая часть которых появляется с помощью информационно-телекоммуникационных сетей, а информация все больше накапливается и функционирует в Интернет. Закономерно стоит вопрос о создании продвинутых технологий, позволяющих оптимизировать интеллектуальную, коммуникативную, организационную, удостоверительную, реконструктивную деятельность следователя в процессе расследования преступлений. И для решения этих прикладных задач мы опять поворачиваемся к человеку и его мыслительным процессам.В информационно насыщенном обществе следователю необходим дополнительный ресурс оптимизации и активизации познавательной и поисковой деятельности. Криминалистика приняла данный вызов, о чем свидетельствует бурное развитие так называемой цифровой криминалистики. Использованию возможностей цифровой среды посвящены многочисленные работы отечественных криминалистов[6].

Как известно, существует две смежные области, занимающиеся исследованием когнитивных функций головного мозга человека и их применением для решения прикладных задач: «Искусственный интеллект» и «Нейротехнологии».

Искусственный интеллект (ИИ) — это область информатики, которая занимается разработкой интеллектуальных компьютерных систем, то есть систем, обладающих возможностями, которые традиционно связывают с человеческим разумом, — понимание языка, обучение, способность рассуждать, решать проблемы и т. д. Нейротехнологии — это набор технологий, связанных с пониманием принципов работы мозга и различных аспектов сознания, мыслительной деятельности, высших психических функций[7].

Искусственный интеллект пытается всего лишь имитировать когнитивные функции человека, создать их математическую модель, то разработки в области нейротехнологий ставят перед собой задачу выяснения основных принципов устройства человеческого мозга и особенностей его работы. Для криминалистики наиболее интересно, на наш взгляд, такое направление нейротехнологий как нейрообразование, в рамках которого ученые занимаются развитием нейроинтерфейсов и технологий виртуальной и дополненной реальности в обучении, разработкой образовательных программ и устройств, созданием устройств для усиления памяти и анализа использования ресурсов мозга. Получаемые в рамках данных исследований знания во многом обеспечили возможность разработки искусственных систем, копирующих когнитивные функции человека и определили направление развития систем Искусственного интеллекта[8]. Не случайно развитию искусственного интеллекта пристальное внимание уделяет руководство нашей стран. В октябре 2019 г. была утверждена «Национальная стратегия развития искусственного интеллекта на период до 2030 года», создан технического комитета «Искусственный интеллект», который и будет разрабатывать российские стандарты в сфере искусственного интеллекта. Ожидаемые эффекты внедрения ИИ: повышение эффективности планирования управленческих решений; повышение безопасности сотрудников; автоматизация рутинных (повторяющихся) операций; использование автономного интеллектуального оборудования и робототехнических комплексов…

Основным продуктом исследований искусственного интеллекта являются интеллектуальные системы. Это технические или программные системы, которые реализуют некоторые черты человеческого интеллекта, дающие возможность выполнить трудоемкие задачи, решение которых человеком в реальном времени не представляется возможным.

Интеллектуальные системы достаточно тесно внедрились в нашу жизнь. Современные технологии искусственного интеллекта реализуются по следующим направлениям:

- компьютерное зрение;
- обработка естественного языка;
- распознавание и синтез речи;
- интеллектуальные системы поддержки принятия решений;
- перспективные методы ИИ.

Одним из примеров подобных систем является система автоматической фиксации дорожных нарушений, производящая контроль за соблюдением правил на наблюдаемом дорожном участке. Работа данной системы, связанная с контролем за соблюдением правил дорожного движения, основыва-

ется на распознавании образов участников дорожного движения — автомобилей, пешеходов, велосипедистов, а также распознавании и определении элементов дорожно-транспортной инфраструктуры — линий разметки, светофоров, знаков и прочих элементов.

Другим примером, интеллектуальных систем в повседневной жизни могут служить многочисленные устройства бытового назначения, такие как роботы-пылесосы. В число их функций входит построение карты помещения для уборки, вычисление оптимального маршрута для перемещения и избегания столкновений с подвижными объектами — людьми и домашними животными. Разработкой такого рода устройств занимается направление «Робототехника».

Но интеллектуальные системы не обязательно содержат в себе аппаратную составляющую. Многие интеллектуальные системы представляют собой исключительно программные решения. Примером может служить чат-бот, который осуществляет информационную или информационно-техническую поддержку пользователей некоторого продукта. Он содержит в себе компоненты, производящие анализ запроса пользователя и экспертную систему, содержащую ответы на распространенные вопросы.

Сферы применения ИИ достаточно широки и охватывают как привычные слуху технологии, так и появляющиеся новые направления, далекие от массового применения. Искусственный интеллект активно применяется для решения задач, связанных с:

- Автоматическим переводом, что может помочь решить вопросы с использованием в уголовном процессе специальных знаний такого участника как переводчик. Сегодня имеется множество программных приложений в свободном доступе, например, MicrosoftTranslator — облачный сервис машинного перевода, поддерживающий работу с текстом, голосом и изображениями. С его помощью можно автоматически переводить и озвучивать беседы с несколькими пользователями. При помощи системы TalkaoTranslate можно переводить голос на несколько языков, распознавать голоса и слушать перевод.

- Проведением аналитики. Это особенно актуально при расследовании многоэпизодных преступлений, серийных преступлений и преступлений прошлых лет. Кроме того, эти возможности искусственного интеллектаиспользуются и для организационно подструктуры деятельности правоохранительных органов. Так, в МВД РФ внедрена и успешно используется единая система информационно-аналитического обеспечения деятельности (ИСОД). Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства. ИСОД — единая система информационно-аналитического обеспечения деятельности МВД России.

Примером может служить и сервис «Аналитика», при помощи которого осуществляется формирование статистических данных, расширенный поиск документов, гибкие условия формирования выборок; создание запросов по шаблону, поиск по связанным документам, поддержку параметрических запросов, а также поддержку SQL в тексте запросов, поддержку сохранение запросов и дублирование условий запросов; генерацию, создание, редактирование и печать отчетов. Сервис «Оперативные ориентировки» направлен на информационную поддержку АРМ на мобильных устройствах.

- Распознаванием зрительных образов, позволяющих расширить возможности криминалистической идентификации и поиска преступников. Так, па практике активно используются «Автоматизированная информационно-поисковая система (АИПС) «Портрет – Поиск», позволяющая проводить поиск по четырем направлениям: «лицо – лицо», «лицо – портрет», «портрет – портрет» и «портрет – лицо», для чего используются формализованные (словесные — возраст, рост, телосложение и проч.) и графические параметры лица (по 18-ти точкам); Автоматизированная информационно-поисковая система идентификации личности по изображению лица (АИПС «СОВА»), обеспечивающая идентификацию неизвестного объекта известному на основании совпадения признаков. Существуют еще информационно-поисковые системы «Видеопоток», «Граница», «Консул», «Портрет+». АИПС «Облик» и др.

- Созданием интеллектуальных экспертных систем.

- Распознаванием текстов и символов.

- Извлечением требуемой информации. Разработан ПО «Мобильный Криминалист Детектив» — универсальный инструмент для извлечения и анализа информации, охватывающий широкий спектр мобильных устройств, дронов, облачных сервисов и ПК; Cellebrite UFED — это автономное устрой-

ство для снятия с мобильного телефона данных для расследования ИТ-инцидентов, как на месте происшествия, так и в криминалистической лаборатории. UFED расшифровывается как Universalforensicextractiondevice, универсальный прибор для извлечения криминалистических данных.

- Анализом различных изображений.

Эти возможности искусственного интеллекта криминалистика адаптирует к задачам уголовного судопроизводства и постепенно внедряет в практикуправоохранительных органов. Такое использование искусственного интеллекта связано с нисходящим уровнем развития ИИ (слабый ИИ). Но нас интересует и восходящий уровень развития ИИ (сильный ИИ), исследования, связанные с машинным обучением, изучением методов построения алгоритмов, способных самостоятельно обучаться, с целью решения определенного набора задач, аналитическомпрогнозировании. Данные методы являются наиболее актуальными в тех ситуациях, когда не существует четкого решения какой-либо поставленной задачи. Ключевой особенностью машинного обучения является то, что оно позволяет не задавать формальные строгие правила поведения, а обучаться на основании накопленных примеров в некоторой предметной области. Однако, для эффективного обучения требуется достаточно большое количество данных. И третьим видом ИИ является сверхсильный, не только сопоставимый, но и превосходящий человеческий мозг, которому будет подвластна предиктивная аналитика, включающая анализ информации, извлекаемой из набора имеющихся данных, определение закономерностей и прогнозирование будущего результата с учетом многих факторов и условий развертывания события, процесса, явления. И на этом этапе развития ИИ, нам придется вернуться к теме «интеллектуальных агентов» и их роли в расследовании и доказывании.

Используя современную терминологию, дорожная карта развития современной криминалистики должна включать:

- поддержку научных исследований в области цифровой криминалистики;
- разработку и развитие программного обеспечения, в котором используются технологии искусственного интеллекта для целей расследования преступлений;
- повышение доступности аппаратного и программного обеспечения, необходимого для решения задач предварительного расследования;
- повышение уровня информированности и обеспечения правоохранительных органов технологиями искусственного интеллекта, квалифицированными кадрами;
- создание комплексной системы взаимодействий между правоохранительными и экспертными органами, учитывающей уровень развития и использования технологий искусственного интеллекта.

Современный этап развития криминалистики обусловлен происходящей в обществе цифровой трансформацией, характеризующейся непрерывным управлением информацией, включая автоматизированный сбор, хранение, обработку и анализ разновариантных данных; особым интересом к вопросам кибербезопасности; распространением цифровых двойников различных объектов; электронным документооборотом; оперативным интернет-взаимодействием и т. п. Появление цифровых технологий в криминалистике — закономерный процесс, детерминирующий модернизацию криминалистической науки, появлению новых частных криминалистических учений о цифровой информации и электронных следах, криминалистических и экспертных разработок, основанных, прежде всего, на широких возможностях искусственного интеллекта и тех областей знаний, которые его изучают.

---

[1] См.: Корма В. Д., Образцов В. А. О совершенствовании парадигмы криминалистики как теории здравого смысла // Криминалистика XXI века: стратегия и тактика развития: Коллективная монография / Отв. ред. Е. П. Ищенко. — Гл. 2. — М., 2016.

[2] Корма В. Д. Криминалистическая технология: проблемы и пути решения // Криминалистика XXI века: стратегия и тактика развития: Коллективная монография / Отв. ред. Е. П. Ищенко. — Гл. 3. — М., 2016.

[3] См.: Степин В. С. Теоретические знания. — М., 2000.; Черникова И. В. Постнеклассическая наука и философия процесса. — Томск, 2007.

[4] См., например: Миликова А. В. Следственная ситуация как критерий алгоритма принятия решения о производстве следственных действий // Вестн.Волгоградск. гос. ун-та. Сер. 5: Юриспруденция. 2012. № 2 (17). С. 299–303; Соловьева Н. А., Шинкарук В. М. Механизм принятия решений следователем // Современные тенденции развития науки и технологий: Сб. науч. тр. по мат-лам международ. науч.-практ.конф. В 5-ти частях. Белгород, 29 апреля 2017 г. / Под общ. ред. Ж. А. Шаповал. — Белгород, 2017. С. 159–162; Колоколов Н. А. Риск в принятии процессуального решения в уголовном судопроизводстве // Юридическая техника. — 2019. — № 13. — С. 47–58; Себякин А. Г. Искусственный интеллект в криминалистике: система поддержки принятия решений // BaikalResearchJournal. — 2019. — Т. 10. — № 4. — С. 21. — DOI

10.17150/2411-6262.2019.10(4).21;Брянцев А. Ю. Рациональный способ принятия тактического решения // Вестн.экономич.безопасн. 2020. № 3. С. 185 – 188. DOI 10.24411/2414-3995-2020-10181.

[5] Степаненко Д. А. К вопросу об определении категории «криминалистическое мышление» // Российский следователь. — 2016. — № 7. — С. 13–17.

[6] См.: Ищенко Е. П. У истоков цифровой криминалистики // Вестн. ун-та им. О. Е. Кутафина (МГЮА). 3/2018, 2019. С. 15–27; Вехов В. Б. Электронная криминалистика в XXI веке: тенденции развития // Криминалистика — наука без границ: традиции и новации: Мат-лы ежегодной всеросс. науч.-практ.конф., Санкт-Петербург, 2 ноября 2018 г. / Сост. О. С. Лейнова. — СПб, 2019. С. 51–54; Мещеряков В. А. Криминалистика в цифровой век // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): Сб.ст.международ. науч.-практ.конф., Москва, 18 мая 2018 г. — М., 2018. С. 180–185; Смушкин А. Б. О природе электронной цифровой криминалистики // Lexrussica (Русский закон). — 2020. — № 6(163). — С. 110–121. — DOI 10.17803/1729-5920.2020.163.6.110-121;Рудых А. А. Трансформация криминалистической и преступной деятельности в условиях развития информационных технологий // Российский следователь. — 2020. — № 2. — С. 3–6. – DOI 10.18572/1812-3783-2020-2-3-6.

[7] Нейротехнологии [Электронный ресурс].—Режим доступа: https://intalent.pro/industry/neyrotehnologii.html (дата обращения: 05.11.2021).

[8] Дорожная карта развития «Сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» [Электронный ресурс].— Режим доступа: https://digital.gov.ru/ru/documents/6658/ (дата обращения: 05.11.2021).

Стихеев С. А.,
заместитель начальника
Оперативно-криминалистического департамента
МВД Республики Казахстан, подполковник полиции
(г. Нур-Султан)

Состояние и перспективы развития оперативно-криминалистической службы в МВД Республики Казахстан

За годы независимости деятельность экспертно-криминалистических подразделений органов внутренних дел Казахстана претерпела значительное реформирование в связи с передачей экспертных функций из органов уголовного преследования в систему юстиции и с 1998 г. была преобразована в оперативно-криминалистическую.

В этот период служба осуществляла технико-криминалистическое обеспечение досудебного производства, формирование криминалистических учетов. Вместе с тем, из-за отсутствия экспертных функций получили развитие лишь те виды учетов, которые не были связаны с исследованием вещественных доказательств (учеты фотоизображений, отпечатков рук и т. п.).

Но время вносит свои коррективы. В 2012 г. с целью повышения процессуального статуса заключений специалистов органов внутренних дел по поручению Главы государства в УПК были включены нормы, позволяющие криминалистам правоохранительных и специальных государственных органов проводить исследования, признаваемые доказательством.

Это сыграло положительную роль в качественном и своевременном расследовании преступлений, в том числе по упрощенной форме досудебного производства и дала новый импульс для развития системы криминалистических учетов.

За годы независимости МВД приобрело аппаратные комплексы для формирования учетов следов обуви, транспортных средств, орудия взлома, следов на пулях и гильзах, изъятых с мест преступлений, отстрелянных из криминального оружия, субъективных портретов, производства портретных исследований, ДНК и физико-химической лаборатории, последняя для исследования продуктов применения взрывных устройств и веществ. Также для оснащения оперативно-криминалистических подразделений приобретены передвижные криминалистические лаборатории, комплексы трехмерного моделирования места происшествия, рабочие места криминалиста с автоматизированным информационно-поисковым программным обеспечением, автоматизированные поисковые баллистические комплексы, пулеулавливатели со скоростомерами, дроны и многое другое.

С 2013 г. в Департаменте функционирует ДНК лаборатория, которая в 2019 г. автоматизирована.

Хочу отметить, что Департаментом активно ведется работа по внедрению новейших изобретений науки в области геномно-молекулярных исследований в целях раскрытия преступлений, одним из которых является секвенатор. С его помощью можно составить «портрет» преступника по ДНК, оставленных на месте происшествия биоследам. Использование секвенатора позволяет установить внеш-

ние признаки человека, такие как цвет глаз, кожи, волос и национальность (биогеографическое расположение). Со временем при пополнении библиотеки маркеров увеличится скорость установления личности по ДНК.

Применяемые же в настоящее время генетические маркеры при проведении молекулярно-генетических исследований позволяют проводить только генетическую идентификацию человека и определять биологическое родство по ДНК-профилю.

Также Департаментом проведен научный эксперимент по установлению малого количества ДНК на поверхности отстрелянных гильз. Актуальность исследования заключается в установлении наличия бионаслоений на поверхности гильз после выстрела и возможности проведения идентификации личности преступника по его ДНК, содержащейся в биологических следах, изъятых с места происшествия.

Результаты научного эксперимента показали, что на поверхности отстрелянных гильз остается ДНК преступника и установление его личности по оставленным биологическим следам на месте осмотра происшествия возможно.

Как вы знаете, с 1 января 2021 г. вступил в действие Закон «О дактилоскопической и геномной регистрации» в части геномной регистрации, в части же дактилоскопической регистрации срок вступления в действие норм Закона перенесено на 1 января 2023 г.

Вместе с тем в рамках реализации Закона Департаментом осуществляется деятельность по созданию автоматизированной дактилоскопической информационной системы МВД автоматизированной информационной системы «Биометрическая идентификация личности» (АДИС АИС «БИЛ»).

Оперативно-криминалистическим департаментом активно внедряются компьютерно-технические исследования, целью которых является получение доступа к информации с носителей, позволяющих провести их анализ и восстановить цепочку событий.

С этой целью проведена презентация новейшего программно-аппаратного комплекса для компьютерно-технических исследований с возможностью изъятия информации с мобильных устройств, видеорегистраторов и компьютерных средств. Использование данного комплекса позволит получать удаленные данные из памяти устройств, извлекать открытые и закрытые данные из самых популярных социальных сетей, файлов резервного копирования (облачных данных), поиск и распознавание людей, мест и предметов на изображениях и другое.

Современной передовой технологией, используемой криминалистами является криминалистический источник света, применяемый для обнаружения следов рук и биологических следов. Использование данного оборудования позволяет при помощи излучения источников света с различной длиной волн и разных оптических фильтров проводить обнаружение латентных следов руки, микрочастиц и биологических следов на месте происшествия. Вместе с тем исключает порчу имущества граждан, позволяя проводить «точечную» обработку следов рук дактилоскопическими порошками.

Наряду с этим, Оперативно-криминалистическим департаментом подготовлено мобильное приложение «Справочник криминалиста».

Это первый современный интерактивный Справочник, который позволит сотрудникам ОВД получить электронное описание по любому изымаемому объекту и следу, процессуально грамотно составить протокол, находясь на месте происшествия. Справочник будет доступным даже при отсутствии интернета.

Справочник содержит алгоритмы проведения различных видов следственных действий, описание отдельных объектов, изъятой следовой информации в протоколах следственных действий. Также в него включены основные вопросы, решаемые в ходе проведения криминалистического исследования, правила заполнения основных процессуальных документов.

Необходимо отметить, что Справочник является уникальным в своем роде и по функциональности аналогов данного приложения на территории СНГ не имеет.

Вместе с электронной версией мобильного приложения «Справочник криминалиста» имеется книжный вариант.

Кроме того, мы изменили подход к подаче информации, сделав акцент на особенности ее восприятия новым поколением.

Впервые за многие годы Департамент подготовил цикл учебных видеофильмов:

Справочно:

- отбор биологического материала у живых лиц;

- обнаружение следов рук и биологических объектов с помощью экспертного света;
- выявление следов рук с помощью нингидрина;
- выявление следов рук с помощью паров йода;
- обнаружение и изъятие следов рук на влажных поверхностях;
- обнаружение и изъятие следов рук на липких поверхностях;
- малое количество ДНК на поверхности гильзы;
- затяжной выстрел.

А также ряд учебно-методических пособий.

Справочно:

- справочник криминалиста;
- сборники вопросов и ответов по методикам дактилоскопических и трасологических исследований;
- практические вопросы одорологии;
- алгоритм постановки на криминалистический;
- учет и опознания по фотоизображениям;
- алгоритм работы с АРМ «Криминалист» модуля е-УД.

В целях дальнейшего развития оперативно-криминалистической службы Департаментом запланирована разработка новых методик криминалистических исследований, соответствующих требованиям технического регулирования;

- завершение автоматизации баллистического учета;
- аккредитация криминалистических лабораторий и приведение их в соответствие с международными стандартами, а также правовое совершенствование оперативно-криминалистической деятельности.

Тасжуреков М. М.,
докторант, магистр юриспруденции
(Академия государственного управления
при Президенте Республики Казахстан, г. Нур-Султан);
Әкім К. С.,
PR-менеджер, докторант, магистр журналистики
(ТОО «KazdreamTechnologies», Республика Казахстан, г. Нур-Султан)

ИНСТРУМЕНТЫ ИДЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ДЛЯ СНИЖЕНИЯ КОРРУПЦИОННЫХ РИСКОВ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Процессы глобализации экономического пространства стремительно меняют мир, и традиционные подходы государственного управления в Казахстане получили новый этап развития. Современному обществу нужна новая политика управления государством, учитывающая возможности цифровых технологий и их применения. Переход на новый уровень государственного управления, формирование и развитие механизмов цифрового правительства, расширяет пространственные связи через призму международной практики, оценивает экономику инноваций в контексте современных цифровых технологий, трансформирует парадигму мышления в цифровой экономике инноваций, предоставляет новые горизонты для развития инновационных проектов национальных бизнес компаний.

В нашей стране началоразвития политики цифровизации обозначеносо временем подписания Указа Президента РК «О Стратегическом плане развития Республики Казахстан до 2020 года», от 1 февраля 2010 г. На основании этого документа были разработаны и приняты Государственные программы «Цифровой Казахстан – 2020», «Информационный Казахстан – 2020». Политика практической реализации основных направлений программ выполнялась Национальным холдингом «Зерде». На современном этапе реализация целей государственной политики цифровизации, направлены на создание в стране высокотехнологичной цифровой инфраструктуры, развитие цифровой индустрии, человеческого капитала. Это комплексная программа повышения уровня жизни граждан и формирования в стране условий для новой траектории цифровой экономики будущего[1].

Переход Казахстана к информационному обществу сопровождается внедрением механизмов совершенствования государственного управления путем создания институтов открытого и мобильного

правительства и обеспечения роста доступности информационной инфраструктуры для граждан страны. Созданы условия для развития технологического предпринимательства и внедрения инноваций в производственные циклы реального сектора экономики, с устойчивыми связями между бизнесом, научными разработками ученых и государством.

Модернизация государственного управления в стране проводится за счет использования потенциальных возможностей информационных и инновационных технологий и имеет достаточно нерешенных проблем. Если сравнивать Казахстан с другими странами постсоветского пространства, то страна находится в середине рейтинга. По оценке экспертов наш регион имеет относительно невысокий уровень проникновения Интернета из-за высокой стоимости предоставляемых информационных услуг[2].

Несмотря на это в стране высокий уровень потребности общества на качественные услуги в сфере информационных продуктов. Стремление к использованию в государственном и частном секторах современных подходов определения коррупционных рисков, привело к возникновению новых интересных решений в национальных IT-компаниях по техническим разработкам для улучшения качества жизни, обеспечения безопасности общества и сокращения рисков государства, бизнеса.

Программисты «KazdreamTechnologies» разработали технологию AI Vision, основанную на видео сканировании лиц. К примеру, камеры видеонаблюдения, которые можно использовать для сканирования лиц посетителей, будут передавать информацию о вакцинации и статусе вакцинации граждан в ТРЦ, бизнес-центре, торговом доме, госоргане, и других общественных местах. Владельцам бизнеса и госорганам не нужно будет приобретать что-то дополнительно, достаточно использование имеющихся камер и компьютеров. Причем не обязательно, чтобы камеры имели высокое качество, технология AI Vision распознает человека абсолютно с любых камер на расстоянии 7 метров.

Инженерные разработки ТОО «KazdreamTechnologies» обеспечивают полный цикл программных и аппаратных решений с нуля. ТОО «KazdreamTechnologies» разрабатывает продукты для бизнеса и государства в сфере оперативно-розыскной деятельности, информационной и экономической безопасности. Все программные решения ТОО «KazdreamTechnologies» могут интегрироваться в единую экосистему и дополнять возможности друг друга[3].

В настоящее время внедряется проект FaceRecognitionSystem (FRS) — это система для идентификации и верификации лиц по внешним признакам, который можно активно использовать для содействия обеспечению честности и неподкупности в сфере оказания государственных услуг, в сфере государственных закупок и управления государственными финансами.

Возможности системы идентификации и верификации лиц по внешним признакам следующие: круглосуточный автоматизированный контроль по видеонаблюдению; автоматизация пунктов пропуска с помощью идентификации лиц по базе; ведение базы нарушителей с целью их обнаружения.

Технологический продукт компании имеет ряд преимуществ следующего характера, это:

- идентификация лица путем загрузки имеющейся фотографии;
- верификация лица путем сравнения предъявленного образца с эталонным образцом;
- распознавание нахождения перед камерой «живого» лица, а не изображения человека на физическом носителе;
- выявление лиц, состоящих в определенной базе;
- поиск дубликатов лиц в базе данных;
- детекция и идентификация лиц на потоковом видеоизображении;
- детекция предметов;
- снижение человеческого фактора при идентификации и верификации лиц.

Эффективные функциональные решения IT продукта включают серверные приложения: для идентификации лиц по фото и видео изображениям, для идентификации объектов по видео изображениям; для создания и редактирования баз шаблонов; для интеграции со сторонними системами API для возможности интеграции со сторонними системами. Функционируют реляционная база данных, не реляционная база данных.

Составными компонентами программного обеспечения FRS являются:

а) высокое качество идентификации и верификации лиц, в том числе по части лица (лица в масках, кепках, солнечных очках), под разными углами и под разным уровнем освещения;

б) высокая производительность системы, в части быстрого получения результата среди более чем 1 миллиарда записей.

Инженерные разработки в IT — AI Vision, FaceRecognitionSystem, являются новыми инструментами противодействия коррупции, которые помогают правоохранительным органам выявлять связи между субъектами (госслужащие, представители бизнеса, частные лица), путем нахождения их фотографий, которые были сделаны тогда, когда они были вместе, в тех или иных местах, и сохраненные с помощью систем видеонаблюдения — в интернете, в социальных сетях, в открытых информационных источниках.

Тенденции совершенствования эффективности и прозрачности государственного управления, методы формирования качественных механизмов цифровизации, направленные на снижение уровня коррупции в стране, отмечены повышенным вниманием со стороны общественности, выявленным по результатам исследований экспертов ООН по электронному правительству[4]. В 2016 г. Казахстан занял 33 место в группе стран с высоким уровнем развития электронного правительства, его индекс составил в 2012 г. 0,68; в 2014 — 0,73; в 2016 — 0,72 (рис. 1). Анализ показал высокие показатели роста индекса по компоненту «Онлайн-услуги» (в 2016 г. 0,77); быстрый рост показателей индекса по компоненту «Телекоммуникационная инфраструктура» за соответствующий период: в 2012 — 0,36; в 2014 и 2016 гг. рост до 0,57.

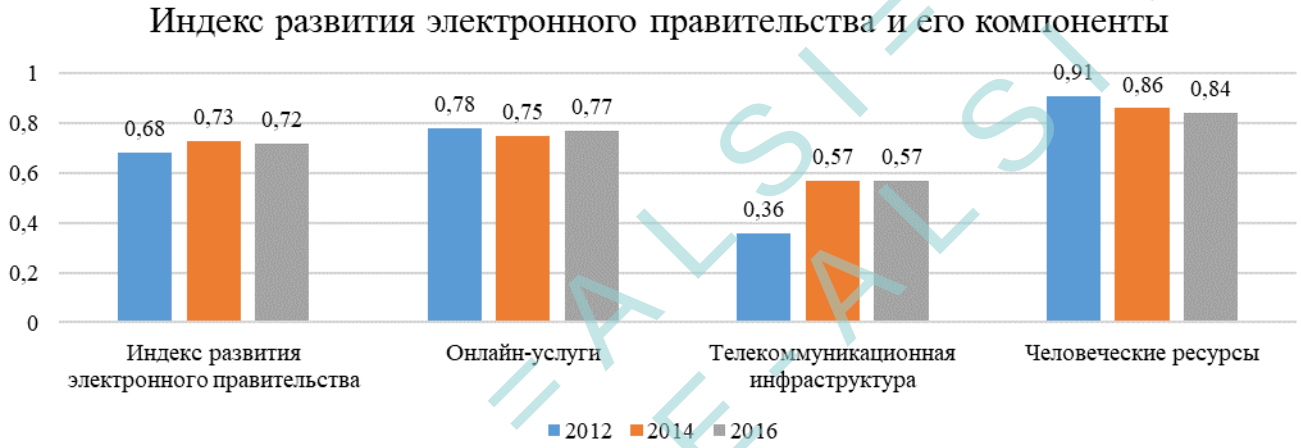


Рисунок 1 — Динамика Индекса ООН «E-government» по Казахстану за 2012, 2014 и 2016 гг.4

Исследования ООН по Индексу развития электронного правительства в Казахстане подтверждаютпродолжающиеся этапы реализации и развития государственной политики в сфере цифровизации, которые расширили горизонты внедрения телекоммуникационной инфраструктуры в стране. Достижения в области современных технологий привели к быстрому доступу к огромным объемам данных об обществе, экономике и окружающей среде. Информационные технологии открывают потенциальные возможности для продвижения антикоррупционной политики государства, используя для этого инструменты и методы обработки информации, которые позволяют выявлять, предотвращать, анализировать причины и условия способствующие коррупции, мошенничеству и нарушениям в государственном секторе.

Технологии BigData позволяют идентифицировать подозрительные транзакции и выявлять нарушения в сферах налогообложения и здравоохранения. Интеллектуальный анализ данных DataMining, применяемый в процедурах государственных закупок в качестве аудитора, позволяет отслеживать действия правительства при подаче заявок и выявить случаи сговора, подачи ложной информации. При изучении объема торговой информации или спорных результатов, IT-технологии, с помощью визуализации индивидуальных данных, позволяют отслеживать коррупционные намерения, выявить зоны рисков, в тех случаях, когда отсутствует конкуренция на государственных закупках или при неоднократно выигранных торгах и других моментах[5].

Выводы: Внедрение инструментов и механизмов противодействия коррупции в практику правительства в области электронного управленияприводят к улучшению политических решений, способствуют эффективной реализации поставленных государством задач, обеспечивают высокую степень прозрачности принимаемых решений и повышение подотчетности в государственном управлении. Обеспечение сбора качественных, доступных, актуальных данных в мобильных технологиях и приложениях позволяют успешно использовать их в борьбе с коррупцией.

[1] Айту Д. Цифровой Казахстан: от концепции к воплощению. [Электронный ресурс]. — Режим доступа: https://www.kazpravda.kz/articles/view/tsifrovoi-kazahstan-ot-kontseptsii-k-voploshcheniu1/ (дата обращения: 05.11.2021).

[2] Рейтинг стран мира по уровню развития Интернета (2016). Retrieved from http://gtmarket.ru/ratings/internet-development/info.

[3] Сембаев Б. Д., Әкім К. С. Национальные продукты ТОО «KazdreamTechnologies» в сфере информационных технологий // Современные возможности методов распознавания человека по анатомическим и функциональным признакам внешности с использованием информационных систем: Мат-лымеждународ. дистанц. кругл. стола. — Караганда, 2021. С. 44 – 48.

[4] Исследования ООН «E-governmentsurvey». [Электронный ресурс]. — Режим доступа: https://publicadministration.un.org (дата обращения: 05.11.2021).

[5] DigitalKazakhstan (2019). О программе. [Электронный ресурс]. — Режим доступа: https://digitalkz.kz/ru/o-programme/ (дата обращения: 05.11.2021).

Телемисов Б. С.,
криминалистика кафедрасының профессоры,
заң ғылымдарының магистрі, полиция полковнигі
(Қазақстан Республикасы ІІМ
Б. Бейсенов атындағы Қарағанды академиясы)

МОБИЛЬДІ ИНТЕРНЕТ КЕҢІСТІГІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ШАРАЛАРЫНЫҢ КЕЙБІР СҰРАҚТАРЫ

Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаев 2021 жылғы 1 қыркүйектегі «Жаңа жағдайдағы Қазақстан: Іс-қимыл кезеңі» Қазақстан халқына Жолдауында: «Цифрландыру — сәнге айналған үрдіске ілесу емес, ұлттың бәсекеге қабілеттілігін арттырудың негізгі құралы. Ең алдымен, цифрлы теңсіздікті жойып, барлық азаматты интернетпен және сапалы байланыспен барынша қамтамасыз ету керек. Бүгінде бұл жолдар мен электр қуаты сияқты негізгі қажеттілікке айналып отыр. «Деректермен» жұмыс істеуді жаңа деңгейге көтеру керек. Мәліметтер базасының бірыңғай жүйесімен қамтамасыз ету және оны әрі қарай дамыту — Үкіметтің басты міндетінің бірі» — деп атап көрсеткен болатын-ды[1]. Сондықтан қазіргі таңда халыққа қызмет көрсетуді цифрландыру мәселесі өте өзекті және қажет болып табылатын міндеттердің бірі болып табылады. Қылмыстық сот ісін жүргізуде де мұның атқаратын маңызы орасан зор. Осындай қызметтерді жүзеге асыру барысында ақпараттардың, деректер мен мағлұматтардың тыска шығып кетуін болдырмауға ерекше көңіл бөлген жөн.

Қазіргі уақытта бүкіл әлемде мобильді интернет кеңістігіндегі ақпараттық қауіпсіздік проблемасына қатысты мәселелерге назар аудару күрт ұлғая түсті. Бұл қоғамның барлық салаларына енетін ақпарат ағындарының тез кеңеюімен байланысты. Ақпарат ұзақ уақыт бойы өндіріс үшін қажетті көмекші ресурс немесе кез келген қызметтің жанама көрінісі болып қалуда. Бұл өз кезегінде материалдық құндылық салмағына ие бола түсуде, яғни оны пайдалану кезінде алынған нақты пайда немесе залал мөлшерімен, ақпараттың иесіне тигізетін ықтималдығының әртүрлі деңгейімен нақты анықталады. Алайда, ақпаратты өңдеу саласын құру бірқатар күрделі проблемаларды туындатып отыр. Осындай проблемалардың бірі ақпараттық-есептеу жүйелері мен желілерінде айналатын және өңделетін ақпараттың сақталуы мен белгіленген мәртебесін сенімді қамтамасыз ету болып табылады[2].

Бүгінгі таңда мобильді Интернет кеңінен танымал бола бастады және оның таралуы жақын арада дәстүрлі сымды аналогқа да жетеді. Деректерді беру жылдамдығы арта түсіп, байланыстық технологиялар да дамып келеді және кез-келген заманауи гаджет мобильді байланыс мүмкіндіктерін толық пайдаланады. Мобильді Интернет — бұл іскер адам үшін сапарға шығу және іссапарлар кезінде тамаша көмекші болып табылады. Смартфон әрқашанда өз иесімен бірге саяхатта болады және электрондық поштамен жұмыс істеу, құжаттарды толтыру және өңдеу, сондай-ақ мобильді құрылғының көмегі арқылы веб-серфинг сияқты мәселелерді жедел шешу ұзақ уақыттан бері ерекше болып табылатын нәрсе емес.

Алайда, әлемнің кез келген нүктесінен Бүкіләлемдік ғаламторға сымсыз кіру мүмкіндігі бірқатар нақты қауіптерге ие. Компьютерлерде, мобильді интернет кеңістігінде антивирустар мен қауіпсіз сүзілетін зиянды бағдарламалар сіздің құрылғыңыздың қауіпсіздігіне де қауіп төндірумен айқындала түседі. Абоненттің жеке шотының балансы арсыз контент-провайдерлер мен түрлі алаяқтар үшін үлкен қызығушылық тудыратынын ұмытпаған жөн.

Мобильді интернеттің негізгі қауіптері.

Сарапшылар мобильді алаяқтық саласындағы негізгі қауіптер мобильді банкингпен байланысты болады деген келісімге келуде. Мобильді платформалар интернет-сайттар немесе банкоматтар сияқты жоғары қорғаныс деңгейімен ерекшеленбейді, сондықтан алаяқтар үшін осал болып табылады[3]. Зиянкестер шотты бақылау мақсатында браузерге және пайдаланушының мобильді қосымшаларына кіруге және оның дербес деректерін иелену үшін барлық әдіс-тәсілдерді қолдануға тырысатын болады. Жақын арада алаяқтардың p2p-төлемдеріне деген қызығушылығының арта түсетінін күтуге болады, яғни бұл мамандардың пікірінше жуық арада біздің елімізде де танымалдылыққа ие болуы тиіс.

Смартфон иелерінің жеке деректерін біле түсу үшін қылмыскерлер көбінесе әлеуметтік инженерия әдістеріне жүгінеді, яғни бұл адамның әлсіздіктерін манипуляциялау арқылы техникалық құралдардың көмегінсіз пайдаланушының әрекеттерін басқару. Қазіргі уақытта шартты түрде «техникалық қолдау қызметкерінің қоңырауы» деп атауға болатын алаяқтық схема белгілі. Қоңырау шалушы өзін ұялы байланыс операторының техникалық қолдау қызметкері ретінде таныстырады және техникалық жұмыстарға байланысты телефонды жаңа параметрлерге қайта бағдарламалау қажеттілігі туралы хабарлайды. Содан кейін құрылғының иесінен қандай да бір әріптер мен сандардың тіркесін енгізуді өтінеді. «Жалған қызметкердің» талабын орындаған жағдайда құрылғы иесі өзінің шотындағы белгілі бір қаражат сомасынан айырылады.

Белгілі бір ресурстарға барған кезде алаяқтардың құрған торына түсіп қалу ықтимал. Яғни, вебсерфинг кезінде бағдарламалық қамтамасыз етуді «жаңарту» ұсыныстарын жиі кездестіруге болады. Мұндай хабарламаларды, мысалға алатын болсақ, басқа да қауіпсіз сайттардан қайта бағыттау кезінде алуға болады. Осындай ақпараттық баннермен өзара әрекеттесуден кейін зиянды бағдарлама жүктеледі, ол автоматы түрде ақылы қысқа нөмірлерге SMS-хабарламалар жібереді. Ақылы бағдарламалардың бұзылған нұсқаларын ұсынатын көптеген сайттардан бағдарламалық қамтамасыз ету орнататын пайдаланушылар SMS-хабарламаларды автоматы түрде жіберу проблемасына тап болады.

Сонымен қатар, келесідей де схема бар, яғни: құрылғыға осы нөмір үшін MMS хабарламасы келгені туралы хабарлама түседі. Ақпараттық хата көрсетілген сілтеме бойынша ауысқан кезде зиянды бағдарлама жүктеледі, содан кейін ақылы нөмірлерге SMS-хабарламалар жіберіледі. Жуық арада зиянды бағдарламаны автоматы түрде жүктеу үшін мұндай хабарламаны ашу жеткілікті, әсіресе егер алынған сілтемелер арқылы автоматы түрде өту мүмкіндігі бар болатын жүзеге асырылады.

Әртүрлі интернет-ресурстарды ұсынатын ақылы қызметтерді пайдалану арқылы ерекше сақтық таныту керек. Кейде олар дұрыс емес ақпаратты көрсетеді, ұсынылған мазмұнның құны төмендей түседі.

Ірі шрифтпен жазылған сома мазмұнын жүктеуге әрекет жасау арқылы астында әрең көрінетін аталмыш бағаның тек бір тәулікке ғана көрсетілгендігі жөніндегі ескертуді байқамауға болады. Бұл жағдайда сіз жазылымды бірден бірнеше айға төлейсіз. Сондай-ақ сайта сатып алу үшін жіберу қажет болатын SMS-хабарламалардың саны көрсетілмеуі мүмкін. Смартфондарға MMS, Интернет және орнатылған қосымшалар арқылы енетін вирустарға ерекше назар аудару керек. Вирусты жұқтырғаннан кейін құрылғы алаяқтардың ақылы қысқа нөмірлеріне SMS-хабарламаларды өз бетімен жолдай бастайды.

Өз аппаратына зиянды Java-қосымшаларын жұқтыру вирусты ойындарды жүктеу және орнату кезінде орыналуы мүмкін. Алайда қаражаттан тек қана алаяқтардың кінәсі салдарынан айырылып қоймастан, сонымен қатар өз салғырттығы нәтижесінде айырылу қаупі бар. Мысалы, мультимедиялық құрылғыны қате орнату нәтижесінде де қаражаттан айырылу мүмкін болады. Смартфон немесе ноутбук болсын, кез келген гаджет жыл сайын интернет-трафикті тұтынуды арттырады. Мобильді құрылғы үшін бұл әртүрлі синхрондау процестері, карталарды жүктеу және навигаторды пайдалану кезінде басқа да қажетті ақпарат (мысалы, кептелістер, жол оқиғалары туралы ақпарат) болуы мүмкін. Мұндай құрылғының әдеттегі параметрлері деректер алмасу функцияларына қатысты көптеген опцияларды қамтиды. Ноутбукпен жұмыс істеу кезінде интернет байланысы әртүрлі жаңартуларды автоматы түрде жүктеу үшін қолданылады: ОЖ өзі де, орнатылған бағдарламалық қамтамасыз ету.

Интернет — трафиктің шығыны бойынша шектеусіз, құрылғының әдеттегі параметрлермен жұмысы пайдаланушының үй аймағында ол үшін де, оның абоненттік шотының жағдайы үшін де қолайлы болуы мүмкін. Бұл трафиктің төмен бағасымен және әртүрлі жоспардағы жеңілдікті пакеттердің болуымен түсіндіріледі. Роумингте 1 Мб мобильді интернеттің бағасы күрт өскен кезде жағдай мүлде басқаша болады. Кез келген тұрақты жаңарту, ақпаратты үнемі жүктеу, сондай-ақ абонент үшін таныс басқа әрекеттер оның шотының балансына теріс әсерін тигізуі мүмкін.

Сапарларда мобильді интернетті пайдаланудың қымбаттығы туралы ескертулерге, сондай-ақ сүйікті сериялардың бірнеше сериясын жүктегеннен кейін байланыс операторларына қомақты қаражат қарыз болған отандастарымыздың тарихына қарамастан, мұндай жағдайлар әлде де орын алуда. Біздің бақытымызға орай, роумингтегі мобильді Интернет бағасының жағдайы бірнеше жыл бұрын ұялы байланыс қызметтері нарығындағы жағдайдан мүлдем өзгеше. Бүгінгі таңда үлкен үштік операторлары үй аймағынан тыс жерде мобильді және Интернет шығындарын оңтайландыруға арналған арнайы трафик пакеттері мен саяхат және саяхат тарифтерін ұсынады. Алайда, кейбір жағдайларда жергілікті SIM картасын сатып алу әлі де негізделіп отыр[4].

Смартфонға кез-келген қосымшаларды орнатқан кезде пайдаланушы келісімдерін мұқият танысып шығу, сонымен қатар орнату кезінде бағдарлама сұрайтын опциялар мен процестердің тізімін қарап шығу ұсынылады. Жүктелген қолданбаларға қатысты пікірлер мен танысып шығу да артық етпейді, өйткені кейде басқа тұтынушылардың пікірлеріндегі ақпарат орнатудың жағымсыз салдарын болдырмауға көмектеседі. Тек ресми Google Play Market дүкенінен қосымшалар алғандарға смартфонның опцияларында сенімсіз көздерден қосымшаларды орнату мүмкіндігін өшіру ұсынылады. Егер Google Play туралы айтатын болсақ, онда Apple Store-дан айырмашылығы, Android операциялық жүйесіне арналған қосымшалардың ресми репозиторийінде соңғы уақытқа дейін құрылғыларға зиян келтіретін көптеген вирустық және басқа бағдарламалар болды. Кейінірек модерация күшейтілді, ал жүктелетін бағдарламалық қамтамасыз ету енді антивирус арқылы тексеріледі. Осы шаралардың арқасында көптеген зиянды бағдарламалар мен жалған бағдарламалар жойылды. Мұндай бағдарламалар мен күресу үшін смартфонның параметрлеріндегі жоғарыда аталған опцияларды өшірумен қатар, антивирустық қорғау құралдары да өз көмегін тигізеді.

Смартфондар, ноутбуктар мен планшеттердің иелері кездестіруі мүмкін тағы бір проблема — бұл қандай да бір қосымшаны байқаусызда сатып алу. Google Play Market және Apple Store-да ұсынылған бағдарламалардың кең таңдауын ескере отырып, мұндай жағдайдың болу ықтималдығы өте жоғары. Бұл жағдайда жұмсалған ақшаны қайтару тәртібі қарастырылған. Сатып алудан бас тартуға болатын уақыт аралығы-App Store үшін 24 сағат және Google Play үшін 15 минут.

Әлеуметтік желілерге шабуылдар.

Әлеуметтік желілер — трояндар мен басқа да зиянды бағдарламаларды тарату үшін тамаша алаң. Миллиондаған жазылушылары бар Twitter, Facebook және Linked In аккаунттары алаяқтар үшін өте жақсы, өйткені оларды иемденіп, вирусты көптеген пайдаланушыларға жіберуге болады. Яғни пайдаланушылар қайнар көзге сене отырып, қате сілтемені басады немесе файлды ашады.

Әлеуметтік желілер зиянды коды бар сайтқа кірген кезде пайдаланушының компьютері жұқтыратын drive-by деп аталатын шабуылдарды жүргізуді жеңілдетеді[5]. Егер осы ресурсқа сілтеме әлеуметтік желіде таратылса, соның салдары апатты болып табылады. Мысалы, 2010 жылы жүздеген мың пайдаланушылар бір нидерландылық жаңалықтар сайтына кіргеннен кейін Trojan Carberp-тің құрбаныболған[6].

Осыған ұқсас қауіпсіздеу жүйелерін белсенді пайдалану болып табылады. «Көзге елестетіп көріңізші, көптеген адамдар Google-ден бір және тек сол ғана оқиға туралы ақпаратты іздейді, ал шабуылдаушылар оны суреттейтінең жақсы фото суреттерді тауып, оларға түрлі вирусты жұқтырады. Суреттерді қарау кезінде пайдаланушылардың компьютерлеріне аталмыш вирустар жұғады». Мұндай жағдайларда ең жақсы қорғаныс — бұл пайдаланушыларды хабардар ету болып табылады. Технологияны қолдана отырып, қылмысты жеңу мүмкін емес — бұл ой соңғы жылдардағы қауіпсіздік индустриясында маңызды болып табылады. Бірақ антивирустық бағдарламалар мен патчтарды уақытылы жаңартуды елемеуге болмайды: ұйымдардың қауіпсіздік қызметтері кәсіпорын қызметкерлері мен клиенттердің өз жүйелерін жаңартуды және қауіпсіз пайдаланудың негізгі ережелерін сақтауды ұмытпауы керек.

Man-in-the-Browser шабуылдары.

Man-in-the-Browser — зиянды бағдарламалық қамтамасыз ету клиенттік интернет-браузерге енгізілетін және ақша қаражатын аударуды бастау кезінде санаулы секунд ішінде транзакция параметрлерін алаяқтың қалауынша өзгертетін шабуыл. Бұл процесті анықтау өте қиын[7]. «Зиянкестер вирусты белгілі бір ұйымға шабуыл жасау үшін дамыта алады. Мұндай шабуылдар күн сайын жасалмайды, бірақ ол болатын болса сәтті орындалады». Мұндай шабуылдардың алдын алудың екі жолы бар — сервердегі аутентификация процесін бақылау және транзакциялық ауытқуларды бақылау[8]. Егер

«клиент» өзін АҚШ-тамын деп мәлімдесе және американдық шотқа кіруге тырысса, алайда аккаунтқа кіруге тырысатын құрылғы басқа елде болатын болса, бұл алаяқтықтың жоғары қаупін көрсетеді.

Жеке құрылғыларды қызметтік мақсатта пайдалану.

Соңғы уақытта компания қызметкерлерінің көптеген саны жұмыс барысында корпоративтік деректер базасына қол жеткізе алатын жеке техникаға жүгінеді және бұл алаяқтық үшін кең мүмкіндіктер туғызады[9]. Осыған байланысты ұйымдар жеке құрылғылардан құнды ақпаратқа қол жеткізуді шектеу керек. Бұл үшін серверлерге қашықтан қолжетімділікті анықтау және қылмыстық әрекетке теориялық тұрғыдан ықпал етуі мүмкін әрекеттерді бақылау үшін алаяқтықты анықтау жүйелері болуы керек.

«Қаскүнемдермен күрес жүргізу кәсіпорынның әртүрлі бөлімшелерінің өзара әрекеттесу ынтымақтастығының нәтижесі болуы керек. Нашар қорғаныс — бұл жақсы шабуыл жасау үшін ең жақсы стимул. Өкінішке орай, көптеген ұйымдар бұл ақиқатты әлі түсіне қойған жоқ»[10]. Жоғары технологиялар дәуірінде ақпарат алатыннан қымбат, сондықтан құпия деректер жиі және көбірек ұрланады. Бұл өте маңызды мәселе, өйткені өзінің коммерциялық құпияларын жоғалтқан компания жабылып қалуы мүмкін. Әсіресе, егер бұл жоғары бәсекеге қабілетті ортада жұмыс істейтін орта немесе шағын бизнес болатын болса[11].

Мобильді құрылғылармен алынбалы тасымалдағыштар арқылы тысқа шығып кетуден қорғаудың ең сенімді әдісі — шифрлау болып табылады. Шифрлауды жүзеге асыратын құралдарды табу қиын емес. Олардың ішінен ең тиімдісін таңдау әлдеқайда қиын.

Ақпаратты қорғаудың негізгі қағидасы — бұл соған кететін шығындардың осы ақпаратты жоғалту немесе ұрлау салдарынан болатын зияннан аспауы керек.

Сондықтан, деректерді қорғау үшін, кемдегенде, қолдау үшін күрделі енгізуді және мамандар құрамын қажет етпейтін жүйені пайдалану оңтайлы, бірақ бұл мобильді құрылғылармен флэш-дискілердегі деректерді шифрлаудан гөрі кең функционалдылыққа ие болады.

Заманауи шифрлау жүйесі деректерді тек алынбалы тасымалдағыштарда ғана емес (флэш-дискілерді қоса алғанда, бірақ тек олармен ғана шектелмейді), сонымен қатар бұлтты қоймаларда, локальдық және желілік ресурстардағы файлдар мен папкаларда қорғауы керек.

Шифрлау мөлдір режимде жүзеге асырылатын болса ыңғайлы болады, яғни бұл пайдаланушылар үшін байқалмайды. Бұл ретте жүйе әкімшісінде ақпарат мәжбүрлі түрде, не пайдаланушының бастамасы бойынша шифрланатын деректердің түрлерімен сценарийлерін көрсету мүмкіндігі болуы тиіс.

Шифрланған ақпаратқа қол жеткізу құқығын неғұрлым икемді және көп деңгейлі бөлуді жүйе ұсынған сайын, оны пайдалану тиімдірек және ыңғайлы болады.

Әкімші жеке қызметкерден немесе бөлімнен бастап, бүкіл компанияға дейінгі әртүрлі ережелерді баптай алу мүмкіндігіне ие болуы керек. Сондай-ақ парольдің көмегімен жақтас компьютерлердегі файлдардың шифрын ашу мүмкіндігі де болуы керек. Егерде корпоративтік деректерді қорғау жүйесі жоғарыда аталған талаптарға жауап беретін болса, онда пайдаланушының жұмысындағы ақпараттың тысқа шығып кетуінен қорғауға болатын сенімді құрал бар деп санауға болады.

---

[1] Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаевтың 2021 жылғы 1 қыркүйектегі «Жаңа жағдайдағы Қазақстан: Іс-қимыл кезеңі» Қазақстан халқына Жолдауы. Қазақстан Республикасы Президентінің ресми сайты. https://www.akorda.kz/kz/.

[2] Основы информационной безопасности хозяйственной деятельности: Учеб. пос. / И. П. Михнев. — Волгоград, 2013.

[3] Сальникова Н. А., Астафурова О. А. Автоматизация поискового конструирования сложных СВЧ-устройств // Изв. Волгоградск. гос. техническ. ун-та. 2013. Т. 17. № 14 (117). С. 122 – 126.

[4] Астафурова О. А., Сальникова Н. А., Кулагина И. И. Интеграция научных разработок в обучении бакалавров экономического профиля // Изв. Волгоградск. гос. техническ. ун-та. 2014. Т. 11. № 14 (141). С. 12 – 14.

[5] Михнев И. П. Мультимедийные технологии в образовательном процессе // Современные наукоемкие технологии. — 2004. — № 2. — С. 109 – 112.

[6] Михнев И. П. Обучение и контроль знаний студентов с помощью UniTest // Фундаментальные исследования. — 2008. — № 1. — С. 94 – 95.

[7] Мединцева И. П. Организационные аспекты использования информационных технологий в высшей школе // Изв. Волгоградск. гос. техническ. ун-та. 2007. Т. 4. № 7 (33). С. 171 – 173.

[8] Лопухов Н. В., Сальникова Н. А. Логистический паспорт региона // Изв. Волгоградск. гос. техническ. ун-та. 2014. Т. 11. № 14. С. 82 – 84.

[9] Правовое регулирование и кадровая обеспеченность органов местного самоуправления: исторический аспект и современные основы: Учеб. пос. / Н. В. Сорокина, С. В. Михнева. — Волгоград, 2013.

[10] Михнев И. П. Информационная безопасность в современном экономическом образовании // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 4. — С. 111 – 113.

[11] Сальникова Н. А., МихневИ. П. Проведение аттестации знаний студентов с помощью компьютерного тестирования // Изв. Волгоградск. гос. техническ. ун-та. 2007. Т. 4. № 7 (33). С. 182 – 185.

Тулеуова А. С.,
преподаватель кафедры криминалистики,
магистр, майор полиции
(Карагандинская академия
МВД Республики Казахстан им. Б. Бейсенова)

Цифровая реальность и криминалистика

Цифровая трансформация является глобальным мировым трендом, а цифровые технологии играют все более важную роль в развитии человечества.Вместе с тем, цифровизация общественных отношений отразилась на преступности и способах противодействия этому явлению.

Цифровизация — это внедрение современных цифровых технологий в различные сферы жизни и производства, где юриспруденция не исключение. Так, в криминалистической науке активно формируется изучение виртуальных следов преступлений.

Идя в ногу с развитием информационных технологий преступная деятельность динамично использует виртуальную площадку для подготовки, совершения и сокрытия своих противоправных деяний, что криминалистика, не всегда оперативно откликается на насущные потребности, необходимые для раскрытия и расследования преступлений, совершаемые посредством компьютерных и цифровых устройств.

На сегодняшний день наиболее распространенные виды преступлений в «виртуальном мире» это распространение вредоносных программ, взлом паролей, кража номеров банковских карт и других банковских реквизитов, распространение информации противоправного характера, то есть клевета, материалы порнографического характера, материалы, возбуждающих межнациональную и межрелигиозную вражду через интернет пространство, а также вредоносное вмешательство через компьютерные сети в работу различных систем. Это процессы, протекающие в «виртуальном» мире, создают следовую картину, следы преступных действий остаются в памяти электронных устройств. Это приводит к выводу, о необходимости модернизации криминалистического учения о следах: определения возникновения следов, их виды и классификации.

На данном этапе обнаружением, фиксацией и использованием таких следов занимается молодая отрасль криминалистики — цифровая криминалистика.Цифровая криминалистика — это отрасль криминалистики, изучающая обнаружение, фиксацию и дальнейшее использование в раскрытии и расследовании преступлений цифровых следов, образовавшихся в ходе преступных процессов, протекающих в «виртуальном» мире[1].

Цифровая криминалистика охватывает компьютерные аппаратные средства и их программное обеспечение, компьютерную информацию, сетевые технологии, мобильную связь, облачные технологии.

Для полного, качественного и своевременного раскрытия преступления необходимо обнаружить, зафиксировать, изъять его следы, которые впоследствии могут иметь доказательственное значение. У электронно-цифровых следов есть своя специфическая особенность, они как правило находятся на электронных носителях или передаются по проводным каналам связи, радиоканалам в виде электромагнитных сигналов.

Эта специфика цифровой информации обусловливает особенности ее поиска, обнаружения и изъятия посредством следственных действий. Цифровая информация имеет первичным носителем специальное техническое устройство — носитель цифровой информации. При получении вещественных доказательств часто возникает необходимость их экспертного исследования. Появление технических средств для этих целей обусловлено возможностями цифровых технологий.

Особую важность вопросу придает специфика данной категории преступлений, связанная с широким применением самых передовых достижений информационных технологий и телекоммуникаций. Лица, совершающие и организующие подобного характера преступления, отличаются высоким уровнем образования, креативным мышлением, теоретическими знаниями и практическими навыками в использовании компьютерной техники и радиотехнических средств. Конечно же, в складывающихся

условиях борьба с преступностью в сфере информационных и телекоммуникационных технологий требует нестандартных подходов и значительных изменений.

Опыт показывает, что человек, имеющий среднее общее, высшее образование (дознаватель, следователь, адвокат, судья и т. д.), должен не только иметь представление о базовых понятиях информатики и информационных технологий, но и умение правильно применять полученные знания в своей практической деятельности и повседневной жизни.

Изучение науки в сфере информационной технологии, можно отнести к специальным знаниям. Специальные знания в сфере цифровой криминалистики это система теоретических знаний и практических навыков в области информатики и информационно-телекоммуникационных технологий, а также знание криминалистических особенностей информационных систем и технико-криминалистических средств, приобретаемых путем специальной подготовки и профессионального опыта, необходимых для решения вопросов, возникающих в процессе уголовного, гражданского судопроизводства, производства по делам об административных правонарушениях[2].

Поэтому, на сегодняшний стоит остро вопрос о необходимости подготовки специалистов со специальными знаниями для проведения экспертиз, следственных действий практически с любой информационной системой, обладающий необходимыми знаниями относительно ее устройства и особенностей работы.

Теоретические знания информационных технологий, объектов компьютерной техники, специфики программных систем должны обязательно сопровождаться наличием практических навыков работы с конкретными технологиями и программно-техническими средствами. Специалист (эксперт), привлекаемый к проведению следственных или иных процессуальных действий в ходе расследования преступлений в сфере информационных или телекоммуникационных технологий должен иметь специальную подготовку по использованию специализированных аппаратных и программных средств исследования цифровых криминалистических средств. То есть, специалист должен обладать знаниями, навыками и умением использования инструмента проведения криминалистических исследований.

Важность этого требования, в первую очередь, связана с тем, что при формировании доказательств, основанных на цифровой информации следователь не может непосредственно воспринимать свойства окружающих объектов, наблюдать их изменения, произошедшие вследствие криминального события. При расследовании преступлений в сфере информационных и телекоммуникационных технологий все происходящее следователем воспринимается через призму цифровых криминалистических средств: специальных программ и аппаратных устройств, каждое из которых построено на основе определенных информационных, математических моделей. Свойства этих цифровых криминалистических средств существенно отличаются от их аналоговых предшественников[3].

Знание специфики работы цифровых криминалистических средств и умение использовать все их свойства является важнейшим условием качественного решения криминалистических задач, стоящих перед специалистом.

В связи с чем, необходимо подготовить высококвалифицированных и конкурентоспособных специалистов в области юриспруденции с умениями и навыками применения современных информационных технологий, направленных на обеспечение национальной безопасности государства криминалистическими методами и способами выявления, собирания, исследования, закрепления информационно-цифровых процессов.

---

[1] Криминалистика: Учебн. / Под ред. Т. А. Седовой, С. П. Кушниренко. — М., 2019.

[2] Махов В. Н. Использование специальных знаний сведущих лиц при расследовании преступлений. — М., 2000.

[3] Мещеряков В. А. Особенности специальных знаний, используемых в цифровой криминалистике. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/osobennosti-spetsialnyh-znaniy-ispolzuemyh-v-tsifrovoy-kriminalistike (дата обращения: 05.11.2021).

Умергалиев М. С.,
руководитель криминалистического управления
Агентства Республики Казахстан по финансовому мониторингу,
квалификационный класс 2 (подполковник)
(г. Нур-Султан)

Особенности криминалистической деятельности в службе экономических расследований

Современное развитие научных технологий способствует увеличению роли специальных знаний в расследовании преступлений.

Во многом это связано с тем, что развитие техники позволяет преступникам совершать традиционные правонарушения новыми способами. В процессе расследования практически любого уголовного дела следователь прибегает к помощи сведущих лиц. В ряде случаев использование таких сведений является условием для возбуждения уголовного дела.

Специалист оказывает содействие в сборе и исследовании доказательств на основе специальных знаний, научно-технических средств и методов.

В целях совершенствования методов и способов выявления, расследования финансовых правонарушений в 2015 г. при СЭР созданы криминалистические подразделения, штатная численность криминалистов составляет 54 единицы.

Для реализации указанных задач была утверждена нормативно-правовая база, проведена работа по оснащению криминалистическим и лабораторным оборудованием, принятые специалисты в СЭР имеют практический и профессиональный опыт работы в органах внутренних дел, судебной экспертизы, аудита, таможни, в сфере строительства.

СЭР приоритетной задачей является снижение теневой экономики.

Основой теневой экономики является выписка фиктивных счет-фактур. Именно через «обнальные фирмы» проводится легализация преступных доходов, совершается хищение бюджетных денежных средств, уклонение от уплаты налогов.

Для ее снижения СЭР проводятся оперативно-розыскные мероприятия, используются аналитические подразделения, осуществляющие дистанционный мониторинг базы данных государственных и частных организаций, по которым устанавливаются рисковые предприятия имеющие признаки правонарушений, также для выявления и расследования правонарушений используют научно-технические средства и специальные познания криминалистических подразделений.

В частности, в борьбе с теневой экономикой криминалисты обеспечивают оперативно-следственный состав СЭР доказательной базой по экономическим, компьютерно-техническим, техническим исследованиям документов, почерковедческим, дактилоскопическим, трасологическим, товароведческим, строительным и фонографическим исследованиям, принимают участие в следственных действиях и оперативно-розыскных мероприятиях.

Так, компьютерно-технические исследования проводятся с целью выявления цифровых следов правонарушений, в которых могут содержаться прямые/косвенные улики.

При исследованиях криминалисты используют современные аппаратно-программные комплексы «UFED», «Мобильный криминалист» и программное обеспечение «ENCASE» зарубежных производителей из Израиля, США, России.

Решают вопросы по извлечению и восстановлению удаленной информации с мобильных устройств (смартфонов, планшетов), компьютерной техники, облачных хранилищ, игорного оборудования на предмет установления, функционирования игровых приложений и наличия информации о денежных операциях, информационных систем, серверного оборудования и других объектов компьютерных технологий.

Отмечаем, что в Казахстане широко развивается деятельность по майнингу крипто валют (второе место по добыче в мире).

Злоумышленники организовывают крипто фермы на государственных предприятиях и по заниженным тарифам на электроэнергию занимаются добычей крипто валюты, что наносит большой ущерб государству.

В данном направлении криминалистами также нарабатывается практика исследования функциональных возможностей данного оборудования, на предмет его целевого назначения, а также поиска информации по объему добываемой цифровой валюты.

Для установления суммы ущерба по делам данной категории также привлекают криминалистов обладающие познаниями в сфере экономики. Экономические исследования испытывают влияние цифровизации, объектами исследования остаются все те же бухгалтерские, банковские и иные документы, но при этом они обретают новую форму существования.

Использование программных средств ведения бухгалтерского учета значительно изменяют объекты экономических исследований, вызывает необходимость исследовать не только традиционные объекты судебно-бухгалтерского, финансово-экономического исследования, а их трансформации, представленные в цифровом виде, изъятые с базы данных различных оборудований, информационных систем.

При производстве экономических исследований криминалисты используют программные продукты «1С Бухгалтерия» и программные приложения «Microsoft Excel», которые ускоряют процесс исследования.

С появлением новых цифровых объектов содержащие финансовые документы, криминалисты разрабатывают новые подходы к проведению экономических исследований.

Развитие современных технологий не обошло стороной и строительные исследования. Появление строительной программы «АВС – 4» и оборудований «Лазерный дальномер», «Электрический керноотборник» предназначенный для отбора кернов в асфальтовых и бетонных покрытиях, криминалистам существенно облегчает процесс выполнения строительных исследований. Использования криминалистами данных оборудований способствует за более короткий период устанавливать суммы ущербов по делам в сфере строительства, а также производить замеры, расчеты сметной документации, проводить отбора кернов с меньшим вложением трудозатрат.

Подделка денежных знаков в современном мире имеет транснациональный характер, который наносит ущерб нормальному экономическому развитию страны.

Из оборота территории страны в текущем году изъято 1 160 (2020 г. — 2 468, 2019 г. — 2 070) фальшивых банкнот.

Общая сумма изъятых фальшивых банкнот в текущем году составила свыше 17 млн тенге (в иностранной валюте около 40 тыс. $ США).

Использование специальных познаний криминалистов, а также высокотехнологичное оборудование позволяет проводить аналитическую и исследовательскую работу по формированию и ведению массивов (групп) фальшивых банкнот по номиналу, серии, номеру и способу изготовления.

Указанная работа позволила выявить и установить подпольные цеха на территории Республики Казахстан.

По оказанию содействия в сфере противодействия теневой экономике криминалистами также проводятся фонографические исследования с использованием высокотехнологичного оборудования «Икар II» производства России. По оперативным записям устанавливается принадлежность голоса и речи подозреваемых, свидетелей, дословные тексты разговоров фигурантов дела, осуществляется очистка записей от шумов и определяются признаки монтажа записей разговоров.

Кроме того, криминалистическим подразделением на постоянной основе проводится научно-методическая работа по улучшению качества, полноты заключений и совершенствованию, и созданию новых методов исследований.

С учетом потребности следственно-оперативной практики в сфере экономических правонарушений криминалистами разработаны методические рекомендации по экономическим, компьютерно-техническим, строительным и техническим исследованиям документов.

Также на постоянной основе криминалисты проходят курсы повышения квалификации на базе Академии правоохранительных органов при Генеральной прокуратуре и Центра судебных экспертиз Министерства юстиции.

В рамках технической модернизации криминалистической деятельности приобретаются современные технологические комплексы.

Наряду с проведением исследований назначаемых самим органом растет и количество направляемых постановлений с других правоохранительных органов МВД, КНБ и прокуратуры, также межведомственных следственно-оперативных групп.

Судебная практика показывает, что ежегодно число приговоров в сфере экономических преступлений растет, где одним из доказательств служат заключения специалистов СЭР.

Глобальная цифровизация в обществе затрагивает процессы работы криминалистической деятельности, возникает потребность постоянного совершенствования исследований, разработки новых методов и способов методик исследований позволяющие оперативно раскрывать преступления.

Для этих целей предлагаем участникам конференции:

- эффективное сотрудничество через усиление взаимодействия между странами путем обмена опытом в области криминалистики и экспертизы;
- совместно разрабатывать современные методики по видам проводимых исследований;
- организовывать повышение квалификации сотрудников криминалистических подразделений;
- обмениваться практикой использования высокотехнологичного оборудования, которое способствует установлению цифровых и иных следов преступлений;
- разработать меморандумы о сотрудничестве по вопросам научно-методического обеспечения, актуальным вопросам судебной криминалистики и экспертизы.

Усовский Б. А.,
старший преподаватель
кафедры судебных криминалистических экспертиз
(Институт повышения квалификации и переподготовки кадров
Государственного комитета судебных экспертиз
Республики Беларусь, г. Минск)

К ВОПРОСУ ОБ ИССЛЕДОВАНИИ ИДЕНТИФИКАЦИОННЫХ МАРКИРОВОЧНЫХ ОБОЗНАЧЕНИЙ ТРАНСПОРТНЫХ СРЕДСТВ

Экспертиза идентификационных маркировочных обозначений (ИМО) транспортных средств (ТС) на современном этапе развития интегрирует опыт из других областей научных знаний. Подобное объединение влечет за собой как трансформацию существующих объектов, методов, собственно предмета исследования, так и формирование новых.

В Республике Беларусь процесс дифференциации, который является следствием таких изменений, привел сначала к существенным различиям между исследованием идентификационных маркировочных обозначений транспортных средств и экспертизой по установлению уничтоженных (измененных) рельефных знаков, а затем и самостоятельному положению данного вида исследования в рамках экспертизы ИМО ТС.

Безусловно, всем этому способствовали современные достижения науки и техники, появление новых объектов и методов их исследования, а также уровень криминального изменения идентификационных маркировочных обозначений автомобилей.

По сути, с внедрением новых научных достижений в экспертную практику при исследовании объектов экспертизы ИМО на современном этапе применяются комплексы разнородных исследований.

Применение такого комплексного подхода с одной стороны, обусловлено экзогенным синтезом не только информационных знаний из многих наук: химии, физики, трасологии, технико-криминалистического исследования документов, компьютерно-технической экспертизы, но и сведений о технологиях производства и сборки кузовов транспортных средств, нанесения лакокрасочных покрытий и т. п.

Существующее положение вещей прежде всего, объясняется огромным количеством объектов, исследуемых в рамках экспертизы ИМО.

С другой стороны, наличие комплекса методов и способов, предназначенных для исследования соответствующих объектов, как уже имеющихся в арсенале эксперта, так и относительно недавно приобретших свое значение для исследования (например, метод технической диагностики электронных блоков управления автомобилей) также свидетельствует о разнородности проводимых исследований.

В результате расширения круга объектов исследования, начиная от элементов комплектации (например, коробка перемены передач определенного типа), маркировочного обозначения на кузове транспортного средства, заводских табличек, и заканчивая электронными блоками управления, затрагиваются не только собственно трасологические задачи, но и вопросы технико-криминалистического исследования документов, компьютерно-технической экспертизы, автотехнической экспертизы и т. д.

На практике, как отмечалось ранее, экспертиза идентификационных маркировочных обозначений транспортных средств безусловно, имеет наибольшую связь с трасологической экспертизой. Связано это с происходящим в настоящее время не только в экспертизе, но и в ряде областей знаний процессом интеграции, взаимопроникновения и обогащения друг друга новыми знаниями.

Прежде всего, это проявляется в анализе и оценке имеющегося комплекса признаков и характера повреждений маркируемой панели автомобиля.

Кроме этого, прослеживается и аналогия по объекту: исследование идентификационных маркировочных обозначений транспортных средств соотносится с таким подвидом трасологической экспертизы как исследование следов производственных механизмов.

Не менее тесная взаимосвязь по непосредственному объекту экспертизы ИМО транспортных средств имеется с технико-криминалистической экспертизой документов. В ряде случаев непосредственным объектом исследования выступают заводские таблички, имеющиеся на кузовных элементах, деталях и элементах комплектации салона автомобиля.

Заводские таблички могут представлять собой металлические пластины, бумажные наклейки, либо наклейки из полимерного материала любого конструктивного исполнения, на лицевой стороне которых каким-либо технологическим способом нанесены производственные обозначения узлов и агрегатов, в том числе, и идентификационный номер транспортного средства.

Среди большого количества объектов технико-криминалистического исследования документов выступают источники информации, изготовленные полиграфическим способом, либо с помощью средств оргтехники.

В результате можно наблюдать сходство двух видов экспертиз по объекту исследования, хотя следует отметить, что в рамках проведения экспертизы ИМО, исследование таких объектов является промежуточным этапом (подзадачей) при установлении первичного идентификационного номера транспортного средства.

В последние годы вызывает повышенный интерес и использование в качестве объекта исследования данных, имеющихся в электронных блоках управления автомобилей.

В памяти указанных электронных блоков управления хранится информация о состоянии систем автомобиля на текущий момент, и они призваны максимально облегчить техническую диагностику — сервисное обслуживание автомобиля.

Интегрировавшись в экспертизу, техническая диагностика оказывает помощь в решении задач, стоящих перед экспертом, но безусловно, в рамках данного вида исследования сервисное обслуживание транспортных средств не применяется, поскольку из всего комплекса информации, которую может получить эксперт, интерес представляют лишь данные об идентификационном номере автомобиля.

Получить информацию, которая находится в памяти электронных блоков, возможно посредством диагностического оборудования: диагностического сканера, либо, в отдельных случаях, путем реализации специальной комбинации органов управления на панели приборов автомобиля. Таким образом, техническая диагностика в экспертизе на современном этапе приобретает статус еще одного неразрушающего инструментального метода исследования.

Интеграция в экспертизу достижений из компьютерной области и автомобилестроения, является, на наш взгляд, одной из форм для формирования знаний о современном состоянии экспертизы идентификационных маркировочных обозначений транспортных средств.

Согласно методики, утвержденной Межведомственным научно-методическим советом в сфере судебно-экспертной деятельности при Государственном комитете судебных экспертиз Республики Беларусь, задачами экспертизы ИМО являются установление факта изменения маркировочных обозначений, способа изменения, а также установление их первоначального содержания.

Вышеуказанные задачи относятся к основным, однако, справедливо отметить, что пределы данного исследования являются более широкими. Помимо вышеперечисленных задач, экспертом может быть установлен факт замены отдельных деталей и агрегатов транспортного средства, произведен поиск дополнительных источников информации, позволяющих идентифицировать автомобиль.

Как показывает анализ экспертной практики, определение факта изменения маркировочных обозначений, чаще всего, не вызывает существенных затруднений. Однако, решая вопрос о содержании первичного идентификационного маркировочного обозначения, в большинстве случаев, применение традиционных физических и химических методов не всегда дает положительный результат.

В связи с этим, возникает необходимость использования новых методов и приемов исследования.

Исследование идентификационных маркировочных обозначений отличает расширенный подход. Он проявляется в том, что для установления первичного маркировочного обозначения, а по сути первичного идентификационного номера, исследуется комплекс объектов, которые составляют как непосредственно само транспортное средство, так и заимствуются из других источников информации об автомобиле, например, регистрационные документы транспортного средства, внутризаводские базы данных предприятий-изготовителей, информация НЦБ Интерпола.

Доступ к информации из производственных баз данных предприятий-изготовителей — это путь решения задачи, основанный на необходимости поиска информации на предоставленном автомобиле. Он может либо непосредственно свидетельствовать о содержании заводских маркировочных обозначений, либо содействовать в их установлении.

В свою очередь, методы исследования, применяемые в совокупности, составляют особенность методики проведения экспертизы идентификационных маркировочных обозначений транспортных средств.

Специфический подход к исследованию прослеживается и в разной сущности основополагающих понятий: «восстановление» и «установление».

Термин «восстановление» раскрывается в словаре С. И. Ожегова: «восстановить» — привести в прежнее нормальное состояние, соответственно, «восстановление» в экспертизе ИМО — приведение в прежнее нормальное состояние идентификационного маркировочного обозначения, позволяющее уяснить его содержание.

В свою очередь, «установление» — термин, составляющий понятие «определение».

Например, на исследуемом автомобиле, в месте должного расположения маркировки установлена панель с автомобиля-донора со знаками вторичной маркировки, либо безномерная пластина.

Очевидно, что результатом исследования будет вывод о том, что экспертным путем не представляется возможным установить содержание первичного идентификационного маркировочного обозначения, а, следовательно, не представляется возможным и установить заводской идентификационный номер, который был присвоен автомобилю на сборочном предприятии.

Применительно к исследованию маркировочных обозначений транспортных средств, к восстановлению эксперт прибегает в том случае, когда он уверен в наличии факта изменения первоначального маркировочного обозначения посредством изменения (перебивания) его знаков. Если же имеет место изменение идентификационной маркировки путем замены всей маркируемой панели или ее части (фрагмента), либо удаления маркируемой панели, то на этом исследование не заканчивается. В данной ситуации дальнейшие действия эксперта, специализирующегося на исследовании идентификационных маркировочных обозначений транспортных средств, направлены уже не на восстановление, а на установление заводского идентификационного номера, путем обращения к производственным базам данных предприятий-изготовителей, используя производственный номер или индивидуальные маркировки комплектующих элементов.

Использование при исследовании маркировочных обозначений транспортных средств современных достижений науки и техники, среди которых особую нишу занимает техническая диагностика, позволяет расширить возможности исследования его объекта с целью получения криминалистически значимой информации и увеличить количество и объем исследуемых признаков.

Таким образом, рассмотрев сущность экспертизы идентификационных маркировочных обозначений транспортных средств, можно с уверенностью сказать, что ее современное состояние соответствует всем законам формирования новых видов экспертных исследований.

Этому свидетельствует наличие целого комплекса исследуемых в ее рамках объектов, а также методов и технических средств, явившихся результатом технического прогресса и накопленных в той или иной области знаний.

Основанием самостоятельного положения данного вида исследования служит наличие собственных обязательных признаков: предмета, объекта, задач и методов исследования. Совокупность перечисленных аргументов, в свою очередь, дает основание для вывода о том, что исследование идентификационных маркировочных обозначений транспортных средств является самостоятельным видом экспертизы.

سونيا خليل عزتحماد.
نقيب مهندس ـ مختبر الأدلة الرقمية ـ دائرة الجرائم الإلكترونية ـ الشرطة الفلسطينية ـ فلسطين .
بكالوريوس هندسة أنظمة حاسوب.
محمد عبد الرحمن عبد الجليل مسعود.
نقيب مهندس ـ مختبر الأدلة الرقمية ـ دائرة الجرائم الإلكترونية ـ الشرطة الفلسطينية ـ فلسطين .
بكالوريوس هندسة أنظمة حاسوب.

" جمع الأدلة الرقمية "

جمع الأدلة الرقمية

❖ **ملخص البحث :-**

تناول هذا البحث الدليل الإلكتروني كوسيلة حديثة بالإثبات الجنائي واختلافه عن الأدلة التقليدية سواء أكان ذلك في قبول القاضي الجنائي له أو في تقديره ، وهذا الدليل عبارة عن معلومات يقبلها المنطق و العقل و يعتمدها العلم، حيث يتم الحصول عليها وتحليلها بإجراءات قانونية و باستخدام برامج وتطبيقات علمية خاصة عن طريق ترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي و ملحقاتها و شبكات الإتصال ، .و يمكن إستخدامها في أي مرحلة من مراحل التحقيق و المحاكمة لإثبات فعل أو شيء أو شخص له علاقة بالجريمة أو جانٍ او مجني عليه

❖ **المقدمة :-**

1- التعريف بموضوع البحث :-

شهد العالم ومنذ منتصف القرن الماضي ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية ، و ذلك اشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن فقد أمست قوة لا يستهان بها في أيدي الدول و الأفراد ، و كان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات و الاتصالات و الاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة ، حيث أبرزت ثورة المعلومات نظاماً جديداً أطلق عليه النظام المعلوماتي ، الذي أوجد بدوره المجتمع المعلوماتي الذي يعتمد على تقنية الاتصال بأنواعها كافة، و المعالجة الآلية للمعلومات خاصة ، و أصبح المتلقي يتعامل مع كم هائل من البيانات و المعلومات ، التي تجاوزت حدود المكان ، و اختزلت عنصر الزمان ، لقد أصبح العالم يتحدث عن شبكة اتصال عالمية لا تكتفي بنقل المواد المرسلة و استقبالها و إنما انتقال الإنسان بكامل حواسه و دون أن يبرح مكانه من أحد طرفي الأرض إلى الطرف الآخر ليتصل و يتفاعل مع نظيره من هذا الطرف الأقصى.

و هذا الانفجار المعلوماتي الذي نشهده الآن ما هو إلا ثمرة المزاوجة بين تكنولوجيا الاتصالات و تكنولوجيا الحاسب الآلي ، و تدار هذه المعلومات و البيانات من قبل مواقع حكومية أو شخصية تعنى بجميع الأمور الحياتية المختلفة و تقوم بتنظيم الأعمال و تحقيق التواصل و هذا هو الجانب الايجابي لثورة المعلومات و تقنية الاتصالات إلا أنه من الطبيعي أن يصاحب هذه الثورة المعلوماتية المفيدة وجه آخر يتمثل بالجانب السلبي من خلال استغلال المعلومات في ارتكاب جرائم لم تكن معهودة من قبل هي جرائم المعلوماتية أو الجرائم الإلكترونية التي أصبحت خطراً يهدد الأفراد و الدول في جميع المجالات.

و بظهور هذه الجرائم و استفحال خطرها ، و عدم فاعلية القوانين القائمة في مواجهة هذه الجرائم ذات الطبيعة المختلفة عن الجرائم التقليدية التي لها طبيعة محددة و أبعاد واضحة كان لزاماً على الدول البحث عن كيفية مواجهتها القانونية ، فبدأت بعض الدول بإصدار القوانين و عقد المعاهدات التي تهدف إلى مواجهة هذه الجرائم. ومن بينها فلسطين حيث تم الإقرار بقانون الجرائم الإلكترونية في عام 2017 وتم تعديله في بداية عام ال 2018. ومع اصدار القوانين ذات الطبيعة الموضوعية ، إلا أن التطبيق العملي لهذه القوانين يصطدم بتحديات إجرائية قانونية تعود إلى طبيعة الجريمة و مسرح الحادث و صعوبة تطبيق بعض الاجراءات الجنائية مثل المعاينة و التفتيش و الضبط و غيرها ، مما يشكل عائقاً كبيراً في مواكبة الاستفادة من الأدلة الرقمية التي ترتبط بأجهزة الحاسب الآلي و الشبكة العالمية .

2- أهمية موضوع البحث :-

تنبع أهمية البحث كون المجتمع أصبح مجتمعاً معلوماتياً يعتمد على قوة المعرفة و المعلومات ، و الاعتماد المتزايد على النظام المعلوماتي الالكتروني في شتى مجالات الحياة ، وما صاحبه من تنامي في ارتكاب جرائم الكترونية و الحاجة إلى مكافحتها و معاقبة مرتكبيها ، من خلال إجراءات سليمة تعتمد على جمع الأدلة الرقمية بشكل يساعد على إثبات الجريمة وفق نصوص القانون و بما يتناسب مع التحول الذي طرأ على الدليل الجنائي التقليدي و الحاجة إلى مواكبة التقدم التقني الذي أبرز الحاجة إلى جمع الأدلة الرقمية من بيئة رقمية معقدة تتميز بالتغيير و التطور المستمر .

3- صعوبة البحث:-

يعد موضوع الدليل الرقمي من حيث قبوله و تقديره في الاثبات الجنائي من الموضوعات الحديثة فهو يختلف عن الأدلة التقليدية و دورها في الاثبات حيث أن الأدلة التقليدية سبق و أن تم البحث فيها في حين أن الادلة العلمية الحديثة ومنها الدليل الرقمي من الموضوعات الجديدة التي لم يسبق البحث فيها بكثرة ووجه الصعوبة فيه لحداثته و شحة المراجع فيه .

و لأهمية مكافحة الجرائم الالكترونية و الحاجة إلى جمع الأدلة الرقمية وفق الضوابط الإجرائية القانونية و الأصول الفنية تبرز مشكلة البحث من خلال السؤال التالي : ما هي الطرق السليمة لجمع الأدلة الرقمية و أهميتها في الإثبات الجنائي ؟

المبحث الأول

ماهية الدليل الرقمي

يعد الدليل الرقمي النتيجة الطبيعية و المنطقية لظهور الجريمة الالكترونية ، باعتباره وسيلة إثبات هامة في المسائل الجنائية المتعلقة بالجريمة الالكترونية و التي ظهرت كنتيجة للثورة العلمية في مجال نظم المعلومات الالكترونية و الرقمية ، و بناءً على ذلك فإن للدليل الرقمي أهمية كبرى في إثبات الجريمة الرقمية و معرفة مرتكبها ، و يثير الدليل الرقمي الكثير من التساؤلات في مجال الإثبات الجنائي ، و ذلك لصعوبة الإثبات به و كيفية الحصول عليه ، و عليه سوف نتطرق في هذا المبحث بالتعرف على الجريمة الإلكترونية و الدليل الرقمي و خصائصه و الفرق بينه وبين الدليل التقليدي .

التعريف بالدليل الرقمي

- **أولاً :- الجريمة الإلكترونية :-**

قبل الخوض في دراسة ماهية الدليل الرقمي لا بد لنا من التعرض لمحل هذا الدليل ، وهي الجريمة الإلكترونية ، فلا يستقيم الحديث عن الدليل الرقمي إلا بعد الوقوف على أعتاب الجريمة الإلكترونية.و تعددت تعريفات الجريمة الالكترونية تبعاً لتعدد الزوايا التي ينظر من خلالها إلى هذه الجريمة ، فقد تم تعريفها من الناحية الفنية من جهة ، و من جهة أخرى تم التطرق لتعريفها من الناحية القانونية على النحو التالي :-

التعريف الفني للجريمة الإلكترونية :-

قام البعض بتعريف الجريمة الالكترونية من الناحية الفنية على أنها : " كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ العمل الإجرامي المقصود "[1].

و من وجهة نظر هذا الجانب من الفقه في أن تعريف الجريمة الإلكترونية و تصنيف صورها يتطلب تعريف المفردات المتعلقة بأركان جرائم الحاسب الآلي وهي[2] :-

1- الحاسب الآلي:- وهو الجهاز الذي يقبل أو يعالج أو يخزن أو يسترجع بيانات أو برنامج الحاسب الآلي.

2- برنامج الحاسب : هو سلسلة مشفرة من التعليمات أو النصوص يكون مقبولاً للحاسب الآلي بحيث يمكن معالجة البيانات و إعطاء نتائج تلك المعالجة .

3- البيانات : تعني تمثيل المعلومات أو النصوص بشكل يكون مقبولاً للحاسب الآلي بما في ذلك توثيق البرامج المعدة بطريقة منظمة أو مخزنة أو معالجة أو منقولة بواسطة الحاسب الآلي.

4- الممتلكات : هي عبارة عن دفعات الكترونية و معلومات خاصة وحقوق نشر محفوظة أو مسجلة و بيانات معالجة إلكترونياً و شفرات تعريف خاصة و ألاقام تسمح بالدخول على الحاسب الآلي ، و نظم قابلة للقراءة بواسطة الإنسان و الآلة و أي مواد أخرى ملموسة أو غير ملموسة تتعلق بالحاسب الآلي.

5- الدخول : يقصد به استعمال أو توجيه الاتصال.

6- الخدمات : يقصد بها معالجة البيانات أو الوظائف التخزينية .

7- العمليات الحيوية : يقصد بها تلك العمليات أو الخدمات المطلوبة لتشغيل أو حفظ أو إصلاح و توصيل شبكات نقل و توزيع من الحاسب الآلي ، و ذلك لضمان حماية الصحة العامة أو السلامة العامة .

التعريف القانوني للجريمة الإلكترونية :-

عرف جانباً آخر من الفقه الجريمة الإلكترونية بأنها : "سلوك غير مشروع معاقب عليه قانوناً ، صادر عن إرادة جرمية – مذنبة – ومحله معطيات الحاسب الآلي" [3].

فالسلوك الإجرامي يشمل الفعل و الامتناع عن الفعل ، و هذا السلوك غير مشروع باعتبار أن المشروعية تنفي عن الفعل صفة الجريمة ، و معاقب عليه قانوناً، لأن إسباغ الصفة الإجرامية لا يتحقق في مجال التشريع الجنائي إلا بإرادة المشرع و من خلال النص على ذلك حتى ولو كان هذا السلوك مخالفاً للأخلاق . و الحقيقة أن هذا الجانب من الفقه يرى أن محل جريمة الحاسب الآلي – دائماً- هي المعطيات بدلالتها الواسعة و التي تعني البيانات المدخلة و المخرجة و المخزنة و البرامج على أنواعها[4] .

- **ثانياً: الدليل الرقمي** :-

أدى ظهور الجريمة الإلكترونية و انتشارها – نتيجة التطور الإلكتروني الحاصل في المجتمع المعلوماتي – إلى عجز القوانين الإجرائية بصورة عامة و الدليل الجنائي العادي على وجه الخصوص في مواجهة هذه الجريمة الحديثة ، فكان لا بد من إيجاد وسيلة أخرى يتم من خلالها

إثبات هذهالجريمة و تقديم مرتكبيها إلى العدالة ، و كانت هذه الوسيلة هي الدليل الرقمي ، لما لهذا الدليل من أهمية كبرى في إثبات الجريمة و نسبتها إلى فاعلها. و الدليل الإلكتروني محور هذا البحث لا يخرج عن هذا المنهج، فالتساؤلات التي تدور حول التحقيق الجنائي الإلكتروني هي كيف يتم نشوء الدليل والأثر الإلكتروني؟ و كيف يتم إيجاده والتعرف عليه؟ و كيف يتم حفظه وعرضه أمام المحكمة؟

- **الدليل في الاصطلاح القانوني**:

الوسيلة التي يستعين بها القاضي للوصول للحقيقة التي ينشدها ، و المقصود بالحقيقة في هذا السياق هو كل ما يتعلق بالوقائع المعروضةعلى القاضي لإعمال حكم القانون عليها[5].

- **يمكن تعريف الدليل الرقمي بأنه** :

بيانات يمكن إعدادها او تراسلها او تخزينها رقمياً بحيث تمكن الحاسوب من تأدية مهمة ما[6]،أو أنه الدليل الذي يجد له الأساس في العالم الافتراضي و يقود إلى الواقعة غير المشروعة و مرتكبها[7].

و يعرف البعض الدليل الجنائي الرقمي بأنه ذلك الدليل الذي يشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد أرتكبت ، أو توجد علاقة بين الجريمة و الجاني أو توجد علاقة بين الجريمة و المتضرر منها ، و ما يقصد بالبيانات الرقمية في هذا التعريف بأنها مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة الرسومات ، الخرائط،و الصوت أو الصورة[8].

و بهذا يمكن القول بأن الأدلة الجنائية الرقمية هي معلومات يقبلها المنطق و العقل و يعتمدها العلم ، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي و ملحقاتها و شبكات الإتصال[9] ، و يمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات فعل أو شيء أو شخص له علاقة بجريمة أوجانٍ او مجني عليه [10].

- **ثالثاً: طبيعة الدليل الرقمي :-**

إن مسألة الطبيعة التي عليها الدليل الرقمي تثير في النقاش مسائل تتعلق بالتالي:-

1. الدليل الرقمي و الواقعة الافتراضية .
2. الدليل الرقمي و الواقعة المادية .

و كل من هذه المسائل تثير في البحث جدل واسع النقاش ، فهذه المسائل تمثل عصب البحث في طبيعة الدليل الرقمي و أداة التواصل بين سلطات الضبط القضائي و التحقيق، و أيضاً المحاكمة و بين الواقعة المعدة في القانون جريمة . حيث أنه يجب أن تكون العلاقة واضحة في القانون بين الدليل الرقمي و طبيعة الواقعة فيما إذا كانت إفتراضية أو مادية أو مزدوجة.

1- الدليل الرقمي و الواقعة الافتراضية :-

تعرف الواقعة الافتراضية الاجرامية بأنها تلك الواقعة التي تبدأ و تنتهي في إطار العالم الافتراضي ، فهذه الواقعة تشكل البناء الحقيقي للجريمة الافتراضية في صورتها المثالية[11].

و العلاقة بين الدليل الرقمي و الجريمة الافتراضية تظهر في أن كليهما يعد صورة للآخر، فالدليل الرقمي هو الواقعة الرقمية ذاتها ، و إن كانت التقنية تمثل وسيلة ضبط هذا الدليل، ذلك لا يعني أن التقنية في حد ذاتها هي التي تحدد صفة التجريم في الواقعة ، فالذي يحقق صفة التجريم و الواقعة الافتراضية هو قانون العقوبات فقط و تسري هذه الفاعلية التقليدية على التجريم عبر الانترنت[12].و تطبيقاً لهذا القول فإن جريمة الاختراق مثلاً ، يتبع في ارتكابها من ناحية و اكتشافها من ناحية أخرى ، التقنية ذاتها أي تكنولوجيا المعلومات ، حيث يقوم الهاكر بالاختراق باستخدام ذات التقنية التي يجب على جهات الضبط و التحقيق استخدامها لكشف واقعة الاختراق المذكورة.

2- الدليل الرقمي و الواقعة المادية :-

يحدث في بعض الأحيان بأن تتم واقعة مادية (جريمة) ، و يتم الاستعانة بالحوسبة و الرقمية من أجل الكشف عنها . و في هذه الحالة فإن الواقعة الرقمية تساهم بشكل فعّال في كشف الواقعة المادية ، بحيث يصبح الدليل الرقمي دليلاً له وجود في كشف الوقائع المادية.

فمثل هذه القضايا تعتمد على علاقات التخزين الرقمي في الواقع ، و لكي يتم الكشف عن الدليل الرقمي و يقدم للقضاء يجب الاعتماد على ضرورة القيام باتخاذ إجراءات ملائمة و مشروعة ، و إلا فقد الدليل مفهومه في القانون و أصبح واقعة مادية صرفة لا تصلح للتقاضي .كما هو الشأن في إتخاذ الاجراءات الملائمة لاستصدار اذن التفتيش أو القيام بأخذ موافقة المالك أو حائز الجهاز أو الشبكة كتابة و تصديق شهود على ذلك . و بهذا يصح القول بأنه كلما كان هناك واقعة مادية غير مشروعة ، فأنه من الممكن الاستعانة بإجراءات الكشف عن الدليل الرقمي للتدليل على حدوث الواقعة ، و يجب في مثل هذه الحالات التدقيق في الإجراءات ، (يجب أن يتضمن إذن التفتيش تخصيص بند فيه يسمح بتفتيش مخصص في الحواسيب و الشبكات و الأقراص و ... الخ) ، و التخصيص يعني تفصيل هذا البند بدقة متناهية حتى لا يكون إجراءالتفتيش باطلاً ، و بالتالي يتعرض الدليل الرقمي ذاته للدفع بالبطلان[13].

و هنا تظهر أهمية التمييز بين إجراءات الكشف عن الدليل الرقمي في الواقعة المادية ، حيث تبدأ إجراءات الكشف عن الدليل من إجراء استصدار إذن التفتيش مع ملاحظة فرق كبير بين تضمين إذن التفتيش بند يسمح بتفتيش الحواسيب و البحث فيها ، و بين التحفظ على المواد الحاسوبية و الرقمية لكي يتم نقلها إلى الحجرة المختصة بإجراء التفتيش و استخراج الدليل الرقمي و التحفظ عليه تمهيداً لتقديمه و عرضه على الجهات القضائية الفاصلة في النزاع ، فمثل هذه المسألة محل دفع أمام القضاء إذا لم يتم مراعاتها ، و الدفع فيها من الدفوع الموضوعية الجوهرية التي يجب على القضاء التعرض لها ، و إلا فقد الحكم تسبيبه الصحيح و أصبح عرضه للنقض[14].

- **رابعاً: خصائص الدليل الرقمي :-**

إن الدليل في العالم المادي الملموس عبارة عن مجموعة من الآثار التي يتركها المجرم أثناء إقترافه الجريمة، ويتم الكشف عنها بمختلف وسائل الإثبات. في حين إن الدليل الرقمي غير ذلك تماماً لوجوده ضمن البيئة الرقمية ، فمثلاً الصورة الموجودة على جهاز الكمبيوتر و شبكة الانترنت ليس لها وجود في العالم المادي إلا عن طريق طباعتها[15].

وتقوم خصائص الدليل الرقمي على مدى ارتباطه بالبيئة التي يحيا فيها، وهي البيئة الافتراضية والتي انعكست على طبيعة هذا الدليل فأصبح يتصف بعدة خصائص جعلته يتميز عن الدليل الجنائي التقليدي وهي :-

1. **دليل علمي :**

الدليل الرقمي هو الواقعة التي تنبئ عن وقوع جريمة أو عمل غير مشروع ، و هي واقعة مبناها علمي من حيث إن مبنى العالم الرقمي أو الافتراضي هو مبنى علمي شيده العلماء و التقنيين . و تفيد هذه الخصيصة أنه لا يمكن الحصول على الدليل الرقمي أو الاطلاع على فحواه سوى باستخدام الأساليب العلمية . وتفيد هذه الخصيصة أيضاً حين قيام رجال الضبط القضائي و الاستدلال أو سلطات التحقيق أو المحاكمة بالتعامل مع الدليل الرقمي سعياً وراء إثبات الحقيقة، حيث يجب أن تبني عملية البحث هنا على أسس علمية . فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقية كاملةً[16].

و إذا كان للدليل العلمي منطقه الذي يجب ألا يخرج عليه ، إذ يستبعد تعارضه مع القواعد العلمية السليمة فإن الدليل الرقمي له ذات الطبيعة ، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي و إلا فقد معناه [17].

2. **دليل تقني :**

تعرف التقنية بأنها ، المعدات و الأجهزة و المعادلات الفنية التي يمكنتوظيفها في تأدية مهمة أو وظيفة[18].

و هنا يقصد بالتقنية ، الأجهزة الخاصة بالإثبات للأدلة الجنائية ، و التي تتيح باستخدامها إنجاز أعمال و نتائج هامة في الإثبات الجنائي . و بهذا يمكن القول بأن الدليل الرقمي ليس مثل الدليل العادي ، فلا تنتج التقنية آلة (كالسكين) يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو مالاً في جريمة الرشوة و... الخ. و إنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها. و مثل هذا الامر يجعلنا ان نقرر أنه لا وجود للدليل الرقمي خارج بيئة التقنية أو الرقمية ، و انما يجب لكي يكون هناك دليل رقمي أن يكون مستوحى أو مستنبطاً أو حتى مستجلب من بيئته التي يعيش فيها ، و هي البيئة الرقمية . و هي في إطار جرائم الانترنت ممثلة في العالم الرقمي الذي يطلق عليها العالم الافتراضي ، و هو العالم الكامن في الحاسوب والخوادم و الملفات و الشبكات ، و يتم تداول الحركة فيه عبرها[19].

و نتيجة للطبيعة التقنية للدليل الرقمي فإنه أكتسب مميزات عدة عن الدليل المادي من حيث قابليته للنسخ ، بحيث يمكن إستخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل و لها نفس القيمة العلمية ، و هذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير ، بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله و ذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة[20].

3. **مفهوم يحتوي التنوع و التطور :**

و تعني هذه الخصيصة أنه على الرغم من ان الدليل الرقمي في أساسه متحد التكوينبلغة الحوسبة و الرقمية ، فأنه مع ذلك قد يتخذ أشكالاً عدة ، فمصطلح الدليل الرقمي يشمل كافة أشكال و أنواع البيانات الرقمية الممكن تداولها رقمياً ، بحيث يكون بينها و بين الجريمة رابطة من نوع ما ، تتصل بالضحية على النحو الذي يحقق هذهالرابطة بينها و بين الجاني[21].

و تتجلى خاصية التطور المستمر للدليل الرقمي في التطورات الحاصلة في مجال التقنية، حيث لم يكن في الإمكان الحصول على صور أو فيديو عن طريق الانترنت ، حيث كانت الخدمات مقتصرة على الرسائل النصية دون الصور ، في حين إلى حد الساعة يمكن الاتصال بالشبكة و ليس عن طريق خطوط الهاتف الثابت ، بل تعدت للهواتف اللاسلكية و النقالة و الأقمار الصناعية و الالياف البصرية[22].

أما من حيث التنوع فان الدليل الرقمي يمكن أن يظهر في هيئات مختلفة الشكل ، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل ، كما هو الشأن حال المراقبة عبر الشبكات و الملقمات أو الخوادم . و قد يكون الدليل الرقمي مفهوماً للبشر كما لو كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام ، كما من الممكن أن تكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي المرئي أو تكون مخزنة في نظام البريد الالكتروني[23].

4. **يصعب التخلص منه :**

و في إطار هذه الخصيصة يجب القول بأنه كلما حدث إتصال بتكنولوجيا المعلومات في معنى إدخال بيانات إلى ذلك العالم ، فأنه من الصعب التخلص منها ولو كان ذلك بإستخدام أدوات الإلغاء و الحذف[24] . فقد قضى بأنه عندما يتم حذف ملف حاسوبي فإن محتوى الملف يمكن إسترداده ، ذلك إن المساحة التي كان يشغلها الملف تظل كما هي متاحة ، و ما لم يتم شغلها من قبل ملف آخر فأن الملف الذي تم حذفه يمكن إسترداده باستخدام أداة إستردادية للملفات المحذوفة ، كذلك يمكن التعرف على تاريخ نشأة الملف و آخرتعديل عليه و آخر مرة تم فتحه فيها [25].

- **خامساً: الفرق بين الدليل الرقمي و الدليل التقليدي :-**

يمتاز الدليل الرقمي عن الدليل التقليدي المأخوذ من مسرح الجريمة المعتاد بما يلي :

1- طريقة نسخ الدليل الرقمي من أجهزة الكمبيوتر تقلل أو تعدم تقريبا مخاطر إتلاف الدليل الأصلي ، حيث تتطابق طريقة النسخ مع طريقة الإنشاء. باستخدام التطبيقات والبرامج الصحيحة ، يكون من السهولة تحديد ما إذا كان الدليل الرقمي ، قد تم العبث فيه أو تعديله وذلك لإمكانية مقارنته بالأصل.
2- الصعوبة النسبية لتحطيم أو محو الدليل ، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الكمبيوتر ، فيمكن للدليل الرقمي أن يعاد تظهيره من خلال وحدات التخزين الخاصة بالكمبيوتر .
3- نشاط الجاني لمحو الدليل ، يسجل كدليل أيضا ، حيث أن نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقاً لاستخدامها كدليل إدانة ضده.
4- الاتساع العالمي لمسرح الدليل الرقمي ، يمكّن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية ، وبمناطق مختلفة من العالم ، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبياً.
5- امتيازه بالسعة التخزينية العالية ، فآلة الفيديو الرقمية ، يمكنها تخزين مئات الصور ، وحدة تخزين صغير يمكنه تخزين مكتبة صغيرة وهكذا.
6- يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد ، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه ، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

المبحث الثاني

طرق جمع الأدلة الرقمية

بعد التعرف على مفهوم الدليل الرقمي في المبحث السابق واستكمالا لماهيته، وجب علينا التطرق في هذا المبحث إلى طرق استخلاص وتوثيق الأدلة الجنائية الرقمية، وذلك محاولة منا لعرض وفهم الطرق والأساليب المستخدمة في هذا الشأن ، حيث إن إجراءات التعامل مع الأدلّة الرقميّة هي عبارة عن عمليّة موحدة تتضمّن تحديد الأدلّة الرقميّة وجمعها واستحصالها ونقلها وتخزينها وتحليلها وإعداد التقارير بشأنها والتخلّص منها.وعلى هذا الأساس سنتعرض في هذا المبحث إلى مصادر الدليل الرقمي .

- **<u>أولاً: مصادر الدليل الرقمي :-</u>**

تتواجد الأجهزة الرقمية في كل مكان في عالمنا اليوم، مما يساعد الأشخاص على التواصل محليا وعالميا و بسهولة. معظم الناس يعتقدون على الفور ان أجهزة الكمبيوتر والهواتف المحمولة وشبكة الإنترنت هي المصدر الوحيد للأدلة الرقمية، ولكن بالحقيقة إن أي قطعة من التكنولوجيا تقوم بمعالجة المعلومات يمكن استخدامها بطريقة إجرامية. على سبيل المثال، فإن الألعاب المحمولة باليد يمكن أن تحمل رسائل مشفرة بين المجرمين وحتى احدث الأجهزة المنزلية، مثل الثلاجة و التلفاز، يمكن إستخدامها لتخزين وعرض وتبادل الصور غير القانونية . لذلك من المهم ان يكون المختصين قادرين من التعرف وإستغلال الأدلة الرقمية المحتملة بشكل صحيح.

إن مصادر الحصول على الدليل الرقمي تكمن في البيئة الرقمية التي إرتكبت فيها الجريمة (المعلوماتية و غير المعلوماتية) ، و تتمثل في أجهزة الحواسيب الخاصة بالجاني أو المجنيعليه و كذلك أجهزة مقدم الخدمة[26].و في الحقيقة إن مصادر الدليل الرقمي لها صلة وثيقة من حيث تقسيم الأدلة الرقمية إلى عدة أنواع و هذا يتم حسب أماكن تواجده ، و هي نفس الأماكن التي يمكن الحصول منها على الدليل الرقمي من أجل تعقب المجرم و تقديمه للمحاكمة[27] . و على ذلك يمكن تقسيم الأدلة الرقمية إلى:-

1. الأدلة الرقمية الخاصة بأجهزة الكمبيوتر و شبكاتها.
2. الأدلة الرقمية الخاصة بالانترنت.
3. الأدلة الرقمية الخاصة بالبروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
4. الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

و يجب القول بأن تنوع الدليل الرقمي يفيد إن هناك عدة طرق يمكن الحصول عليه ، ذلك لأن شبكة الانترنت شبكة معقدة ولكن على الرغم من ذلك فان الاتصال بها عملية سهلة خصوصاً مع وجود نوعين من خدمات الولوج إلى شبكة الانترنت (السلكي واللاسلكي) ، و بالتالي فأن الحصول على الدليل الرقمي يتطلب فحص نظم الاتصالات بالانترنت و مركبات الحاسب وملحقاتها و كل جهاز يمكن الولوج به إلى الانترنت.

- **<u>أولاً : نظم الاتصال بالشبكة:-</u>**

و يتمثل في نظام فحص مسار الانترنت و فحص بروتوكولات الانترنت ، و إن منطق التعرف على الحاسوب الذي تمت مباشرة إرتكاب الجريمة عبره من السهولة بمكان ، و هذا الامر يطلق عليه التعرف على بروتوكول الانترنت(IP)[28]، و هذا الامر طبيعي خصوصاً إذا تم الإبلاغ عن الجريمة أو كانت هناك عمليات مراقبة تقوم بها شرطة الانترنت ، كما أنه يمكن الحصول على (IP) عن طريق برمجيات معينة ، و في حالة اكتشاف الجريمة حيث يسهل الامر لو كانت الجريمة قد تمت عبر حاسوب شخصي ، يمكن لأجهزة الضبط ان تلاحق الجاني ، كما ممكن فحص الخادم الملقم و فحص النظام الأمني البرمجي ، و هذا للحصول على مزيدمن الأدلة الرقمية المتواجدة على مستواها[29].

- **<u>ثانياً : فحص مركبات الحاسوب :-</u>**

إن أهم مصادر الدليل الرقمي هي الحاسوب و كل مكوناته سواء المادية منها أو المعنوية، بالإضافة إلى مجموع الوسائل التي يمكن الولوج بها إلى شبكة الانترنت كالهواتف النقالة . و إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقق و بيان الطريقة التي قام بها هذا الاخير في إرتكاب جرائمه ، و مما لا شك فيه أن المجني عليه هو المصدر الكاشف و النتيجة التي يترتب عليها ما قام به الجاني من جرائم ، و بالتالي فإن فحص جهاز الحاسوبالخاص به يمكن المحقق من معرفة الدخول و تتبع مصدره[30].

و يمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال أجهزة الحاسوب سواء الخاصة بالجاني أو المجني عليه عن طريق البحث في أنظمة الحاسوب و ملحقاتها ، حيث تعد الحواسيب مصدراً غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بماثبة أرشفة سلوكية للأفراد ، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم ، وعملية حجز الحاسوب بقصد تفحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المعلوماتية بإعتبار أن هذا الجهاز هو وسيلة تنفيذها. و الحاسوب الآلي في ذاته يقوم على عنصرين أساسيين هما القرص الصلب(Hardware) و البرمجيات (Software) و عنصراً آخر يكون في ما بين هذين العنصرين و هو عنصر المعلوماتية ، لذلك فإن الأمر يستلزم أن يكون الفحص ماديا و معنويا للارتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل.

1- فحص القرص الصلب :

يعد القرص الصلب المحتوى الذي يضم في داخله مجموعة من البيانات الرقمية ذات الطابع الثنائي، و يتم فحص قرص الصلب إما كلياً أو جزئياً ، و هذا حسب نوع الجريمة و الآثار المترتبة عليها أي الاضرار الناجمة عنها.

و يتم الفحص الجزئي للقرص الصلب عن طريق استرداد المعلومات الموجودة على مستواه الموجود في سلعة التفتيش أو المعاينة أو التي تم حذفها ، و المثال التقليدي المستخدم هنا هو حالة البحث في الملفات و النسخ الإضافية التي تحتويها نظم التشغيل مثل النوافذ و الملفات المؤقتة ، حيث أنه بمجرد الولوج إلى شبكة الانترنت فإن هذه الملفات تحتفظ بنسخ ، كما يمكن فحص الملفات الخاصة بالتحميل[31].

و للتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم فيها ضبط الحاسوب و مهارة الشخص القائم بإستخلاص البيانات دون العبث بمحتوياتها .و إن من الأمور التي تظهر بعد عملية فحص أي قرص صلب لأي جهاز تلك البيانات التي كان يستخدمها الجاني ، و كذلك الصور المخزنة فيه و مخابئ صفحات الأنترنت ، و من خلالها يمكن التوصل لصفحات وعناوين مواقع الأنترنت و كذلك رسائل البريد الإلكتروني بالإضافة إلى رؤوس الصفحات المرسلة و المتلقاة و مجموعة البرامج الجاهزة المتخصصة التي إستخدمها (المشتبه فيه) و منها يمكن تحديد أصدقاء (المشتبه فيه) و كذلك تحديد ما يتحاورون فيه[32].

2- فحص البرمجيات :

و هي المكون المعنوي للحاسوب ، و يثار هنا ما إذا كانت البرمجيات معطوبة أي بها خلل في حد ذاتها ، ذلك أن برمجية الحاسوب يمكن أن تؤثر في الحاسوب فتجعله محل شك يمكن أن يهز قيمتها كدليل [33].و هذا القصور له أثره في عملية تقييم الدليل المستمد من البرمجية ذاتها ، فمثلاً إن استمداد أدلة حين فحص برمجية معينة كبرمجية البريد الالكتروني أو برمجية تحصيل أموال المخدرات و ... الخ ، و التي تكون مركبة على الحاسوب ، فإن مجرد كون هذه البرمجية معطوبة ليست من الأسباب التي تجعلها قاصرة عن إستمداد دليل يحمل الإدانة ، حتى و إن أمكن إستخدام برمجيات عالية الكفاءة لتنقيتها من الشوائب ، إذ يظل حالها محل شك على مستوى الاستدلال و ليست دليلاً كاملاً[34].

3- فحص النظام المعلوماتي :

إن نظام المعلومات يحتوي على بيانات في هيئة رقمية متبادلة ، كما يمكن فحص نظام ذاكرة التخزين ، و الذي يمكن تعريفه بأنه قدرة الحاسوب الآلية على الاحتفاظ في ذاكرة بنسخة كاملة مما أطلع عليه عضو الانترنت إثناء إبحاره عبر العالم الافتراضي[35].

حيث إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب ، و تعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات يمكن إسترجاعها عبره تكون مخزنة في ملفات على أي شاكلة يمكن أن تكون عليها الحركة الإسترادادية ما دام موضوعها يشكل جريمة[36].

4- الملحقات :

أصبح التطور يطال كل الأجزاء التي تكون متصلة بالحاسب الآلي و منها الطابعة ، التي أصبحت تتميز بميزة تخزين منطقية لمجموع الصفحات التي تم استخراجها من الحاسوب ، و حتى في الحالة التي يتم فيها إلغاءها و في الواقع هناك برمجيات متطورة تقوم بإسترجاع مخرجات الطابعة ، فمثل هذه البرمجيات تساعد في معرفة ما إذا كان الشخص قد قام بطباعة صفحات تتضمن صور داعرة و خليعة من الانترنت و تاريخ قيامه بذلك و ساعته بدقة غريبة ، و يراعى ان تقدير ما إذا كان مالك الحاسوب أو الهوية عبر الانترنت هو مرتكب الجريمة عبر الانترنت ، و إنما تم تخريجه بالطباعة منسوب إليه يظل خاضعاً لتقدير محكمة الموضوع في كل الأحوال [37] . كما يمكن فحص لوحة المفاتيح ، حيث أن عمل مجرم الانترنت قد يصل إلى أن يتحكم في لوحة المفاتيح و من ثم يمكن الاعتماد عليها في استمداد الدليل[38].

- **ثالثاً: الأجهزة الذكية المحمولة :-**

سابقاً كانت تستخدم الأجهزة الخليوية للاتصالات الصوتية فقط، اما اليوم اصبحت تستخدم أيضا لالتقاط الصور الرقمية والأفلام، وإرسال الرسائل الفورية، وتصفح شبكة الإنترنت، وتنفيذ العديد من المهام كجهاز كمبيوتر تماماً. إن الأجهزة المحمولة تسمح للمجرمين المشاركة في مجموعة متنوعة و متزايدة من الأنشطة كما وتمكن من تتبع كل خطوة وكل رسالة. لذلك فإن خاصية التتبع تحول الأجهزة المحمولة إلى أدلة رئيسة في كثير من الحالات.

و يمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال الأجهزة الذكية المحمولة سواء الخاصة بالجاني أو المجني عليه عن طريق البحث في كافة البيانات الموجودة عليها من تطبيقات و رسائل نصية وصوتية وصور ومقاطع فيديو و مكالمات.

- **رابعاً: المتصلون بشبكة الانترنت :-**

إن إرتكاب جريمة الانترنت و الجريمة المعلوماتية يجمع في الغالب أكثر من طرفين ، أي الجاني و المجنى عليه و مقدم خدمة الانترنت أي مزودها ، لذا فأن أول الخطوات التي يجبالقيام بها من طرف الأجهزة المختصة بالبحث هي التفتيش عند[39]:-

1- المشتبه به :

و هي عملية فحص أجهزة الحاسوب والأجهزة الذكية لديه خصوصاً إذا ما تمت الجريمة من خلالها ، و يتم فحص جهاز الكمبيوتر بكل ما يحتويه من وحدة تخزين دائمة و الوحدات الفرعية الملحقة ، و التي تشمل القرص المرن و أقراص الليزر و وحدات التخزين الأخرى ، و التي يمكن إستخدامها كالقرص القابل للإزالة.

2- المجنى عليه :

و هذا قد يكون شخص طبيعي أو معنوي ، فيمكن للأجهزة المختصة بالتحري و الاستدلال أن تقوم بعملية تتبع بعض الآثار المتبقية التي يمكن أن يتركها الجاني ، و هذا يتم بتفتيش الأنظمة و معاينة مسرح الافتراضي ، و إتخاذ جميع التدابير اللازمة من أجل الحفاظ على الدليل الرقمي.

3- مزود الخدمة (مقدم خدمة الانترنت) :

حيث يمكن الاستعانة به لاكتشاف الأدلة المتوافرة لدى مقدم الخدمات الدولية على سبيل المثال (Google،YouTube ،Facebook) و المحلية ، حيث يتم تسجيل و حفظ البيانات الخاصة بالمشتركين على شبكة الانترنت و كيفية استخدامهم للخدمات المقدمة من قبل هذه الشركات.

ثانياً:عملية ضبط الأجهزة الرقمية:-

الضبط هي العملية التي تتم فيها نقل الأدلة الرقمية المحتملة والمعرّفة من موقعها الأصلي إلى بيئة أخرى لاستحصالها لاحقاً وتحليلها[40]. قد تكون الأجهزة المستهدفة في احدى الوضعيات التالية والتي تحدد النهج المتبع في عملية الضبط والأدوات المطلوبة:

- جهاز يحتوي على الأدلة الرقمية المحتملة في وضعية التشغيل.
- جهاز يحتوي على الأدلة الرقمية المحتملة مغلق.

تشمل عملية الضبط الخطوات العامة التالية[41]:

- توثيق النهج والأسلوب المتبع في عملية الضبط وتسلسل العهدة/ حفظ الأدلة باستخدام النماذج.
- تسمية الأجهزة لتمييزها بوضوح.
- ضبط الأدلة الرقمية المحتملة بحسب الأولوية التي تم وضعها أثناء عملية التعريف.
- تحديد ما إذا يمكن تجميع الأدلة الرقمية المحتملة عبر مزود خدمة الانترنت أو شركة الاتصالات الخلوية من خلال ارسال طلب بذلك.
- الانتباه إلى المتطلبات الخاصة لعملية الضبط والتي تعتمد على وضعية الجهاز.
- تغليف الأجهزة قبل النقل.
- تجميع الأدلة غير الرقمية أو المواد التي لها علاقة بالأدلة الرقمية المحتملة مثل الملاحظات التي تشمل كلمات المرور أو مفاتيح التشفير أو قاعدة تثبيت الجهاز أو وصلة الكهرباء.
- مقابلة الأفراد في مسرح الجريمة أو مكان التفتيش لضبط المعلومات التي قد يكون لها علاقة للاحتمالية المطروحة.
- ضبط الأدلة الرقمية المحتملة بحسب الإجراءات من خلال تقديم مذكرة التفتيش والضبط للهدف.
- يجب معرفة وضعية الجهاز المستهدف خلال عملية الضبط لتقليل الضرر الذي قد يقع على الأدلة الرقمية المحتملة.

- **كيف يتم جمع الأجهزة الرقمية:-**

المعلومات المخزنة رقمياًداخل الأجهزة الرقمية حساسة للغاية ويمكن فقدانها بسهولة. لذلك تم تحديد بعض الإجراءات التي يجب اتباعها لضبط الاجهزة والحواسيب بشكل صحيح. فبمجرد ان يتم تأمين مسرح الجريمة وإعطاء السلطة القانونية الإذن لإستخدام الأدلة يمكن جمع الأجهزة. وينبغي ان تؤخذ كلمات السر و الرموز من الأفراد المعنيين إن أمكن، بالإضافة الى الشواحن والكوابل والاجهزة الطرفية وأيأدلة ارشادية مرتبطة بها.

ان المستخدم الأول بحاجة الى الاعتناء بالأجهزة الرقمية بشكل خاص بالإضافة إلى الإجراءات المعتادة لجمع الأدلة وذلك لمنع التعرض لأشياء مثل درجات الحرارة القصوى، الكهرباء الساكنة والرطوبة.

- **جمع الأجهزة المحمولة :-**

ينبغي إيقاف تشغيل الأجهزة على الفور وازالة البطاريات ، إذا كان ذلك ممكنا. إيقاف تشغيل الهاتف يحافظ على معلومات مواقع تنقل الهاتف وعلى سجلات المكالمات، ويوقف عملية استغلال الهاتف، والتي يمكن أن تغيير البيانات الموجودة على الهاتف. بالإضافة الى أنه إذا كان الجهاز مضبوطا على أمر التدمير عن بعد يمكن استخدامه دون معرفة المحقق بذلك . فبعض الهواتف لديها نسق تلقائي لتشغيل الهاتف للحصول على التحديثات، وهذا من شأنه أن يضر البيانات، وبالتالي إزالة البطارية هو الحل الأمثل.

إذا كان لا يمكن إيقاف تشغيل الجهاز، يجب عزله عن برج الإرسال من خلال وضعه في bag Faraday أو اي مادة عازلة اخرى، وتعين وضع الطيران، أو القيام بتعطيل خاصية ال WI-FI ، وتقنية ال Bluetooth أو أي نظام إتصالات أخر . يجب وضع الأجهزة الرقمية في اكياس مقاومة للكهرباء الساكنة مثل أكياس الورق أو مغلفات البطاقات البريدية و الورق المقوى. وينبغي تجنب الاكياس البلاستيكية لأنها يمكن أن تنقل الكهرباء الساكنة، أو تسمح بحدوث التكاثف أو تسرب الرطوبة.

في حالات الطوارئ أو الحالات التي تهدد الحياة، فإن معلومات الهاتف يمكن ازالتها وحفظها في مكان الحادث، ولكن يجب توخي الحذر الشديد في وثائق العمل والحفاظ على البيانات.

عند إرسال الأجهزة الرقمية إلى المختبر، يجب على المحقق أن يشير إلى نوع المعلومات المطلوبة ، على سبيل المثال أرقام الهواتف و سجلات المكالمات من الهاتف الخليوي، أو البريد الإلكتروني و الوثائق و رسائل الكمبيوتر و الصور التي على الأقراص[42].

- **<u>جمع أجهزة الكمبيوتر والمعدات :-</u>**

لمنع تغيير الأدلة الرقمية خلال عملية الجمع يجب على فريق الإستجابة توثيق أي نشاط على جهاز الكمبيوتر أوالمكوناتو الأجهزة عن طريق إلتقاط صور وتسجيل أية معلومات على الشاشة. يمكن للمختص تحريك الفأرة(Mouse) دون الضغط على الأزرار لتحديد إذا كان هناك شيء على الشاشة. إذا كان الكمبيوتر في وضع التشغيل، فينصح وبشدة استدعاء خبير بالجنايات الإلكترونية حيث انه يمكن فقدان الإتصال بالنشاط الإجرامي اذا تم إيقاف تشغيل جهاز الكمبيوتر. إذا كان الكمبيوتر في وضع التشغيل ولكنه بدأ بتشغيل برنامج تخريبي (لتنسيق او حذف او إزالة و محو المعلومات)، فيجب فصل الطاقة الكهربائية عن جهاز الكمبيوتر على الفور للحفاظ على ما تبقى على الجهاز.

البيئات المكتبية تجعل عملية جمع الادلة أصعب وذلك بسبب الشبكات، واحتمال فقدان الأدلة والمطلوبات خارج وكالة التحقيق الإجرامي. على سبيل المثال، إذا تم ايقاف تشغيل الخادم فان العملاء في الخارج لن يتمكنوا من استخدام الخدمات المقدمة لهم، وفقدان الخدمة للعميل قد يكون مضرا للغاية. وبالإضافة إلى ذلك، ينبغي جمع المعدات المكتبية التي يمكن أن تحتوي على أدلة مثل آلات النسخ، والماسحات الضوئية والكاميرات الأمنية وأجهزة الفاكس وأجهزة الاستدعاء و وحدات هوية المتصل.

قد تجمع أجهزة الكمبيوتر المغلقة ايضا كأدلة وفقا لإجراءات المعتادة للأدلة الرقمية[43].

- **<u>إعادة بناء الدليل الرقميDigital Evidence Reconstruction توجد ثلاثة أنواع من إعادة بناء الأدلة الرقمية و هي :-</u>**

1- الأدلة الرقمية الصحيحة.
2- الأدلة الرقمية التي تم العبث فيها أو محوها.
3- وهناك نوع ثالث يطلق عليه الأدلة الرقمية الهامشية.

ويلاحظ أنه من الضروري لإعادة بناء الدليل الرقمي أن تتم الاستعانة بهذه الأنواع الثلاثة فالأدلة الرقمية الصحيحة يتم من خلالها استخلاص المعلومات المتعلقة بالجريمة والمجرم من خلال البحث فيها ، كما أن الأدلة الرقمية التي تم محوها أو العبث فيها ، تتم إعادة بنائها باستخدام برامج خاصة معروفة لهذا الأمر والأدلة الرقمية المهمشة ، وهي أدلة رقمية تلعب دوراً حاسماً في إعادة ترميم الأدلة الممحوة أو التي تم العبث فيها ، كما أنها تكمل أوجه النقص في الأدلة الرقمية المستخلصة من الأدلة الرقمية الصحيحة عن علاقة المجرم بالجريمة المرتكبة.

- **<u>ثالثاً: صعوبات جمع الأدلة الرقمية:-</u>**

تبدو الأهمية العملية للحديث عن كيفية إستخلاص الدليل الرقمي من خلال صعوبة استخلاصه، التي قد يكون سببها أمور تتعلق بالدليل ذاته ، بإعتبار ان الجريمة المعلوماتية في الأغلب لا تترك آثاراً . كما أن وسائل المعاينة و طرقها التقليدية لا تفلح غالباً في إثبات دليلهذه الجريمة التي تنفرد بطبيعة خاصة.

و كذلك قد تظهر مشكلات استخلاص الدليل الرقمي لصعوبات تتعلق بحجم و كم البيانات المتعلقة بهذه الجريمة ، من حيث ضخامتها و سهولة تدميرها ، إذ يكفي أن يقوم شخص بضغط زر واحد لمحو كم هائل من البيانات التي قد تنطوي على جريمة معلوماتية ، أو تلك البيانات التي تتعلق بجريمة غير معلوماتية ولكن تسهل إثبات إرتكابها و من ارتكبها.

- **<u>رابعاً: توثيق الدليل الإلكتروني وتأمينه :-</u>**

يعتبر التوثيق من المراحل الدقيقة والمهمة في كل خطوة من خطوات جمع الدليل وتحليله، و هناك طرق عدة للقيام بالتوثيق، لعل من أهمها وأنجحها الطريقة التقليدية باستخدام الورق والقلم، حيث أنه يصعب تزويرها كما هو الحال في الملفات الالكترونية. و هناك بعض البرمجيات الخاصة التي تساعد في عملية التوثيق، لكن من الضروري توثيق استخدامها أيضا ، كما يتم استخدام التصوير وتسجيلات الفيديو في عملية التوثيق.

يمكن الجمع بين الوسائل السابقة، و لكن لا بد من التوقيع على كل صفحة وملف، اعطاء أرقام تسلسلية لها أثناء عملية التوثيق من أجل ضمان المصداقية، و يشترط البعض وجود شهود أثناء عملية التوثيق هذه، وضرورة توقيع الشهود عليها جميعها.

و تنبعث أهمية التوثيق لكل مرحلة من ضرورة فهم الآخرين لما تم أثناء عملية جمع الدليل ومعالجته، إضافة إلى بيان وعرض كيف يمكن إنتاج هذه المستخلصات مرة أخرى، و بالعادة يتم وضع بروتوكول يمكن الخبراء الذين سيعاينون النتائج لاحقاً من متابعة الخطوات المدونة به والنتائج المتوقعة لكل خطوة.

تبدأ هنا مرحلة التحضير لعملية الجمع، حيث توضع الأهداف لما يراد جمعه ودراسته، ويتم وصف عملية الجمع بشكل دقيق، بحيث الا يتم إهمال أو ضياع عنصر من عناصر الدليل، كذلك يتم التركيز على موضوع الخصوصية للبيانات التي يتم جمعها، حيث لا بد من مراعاة القوانين والإجراءات المتعلقة بخصوصيات الأفراد، ولا سيما تلك التي ليس لها مكان في التحقيق الالكتروني .

إن عدم اتباع هذه المعايير في هذه المرحلة يجعل الدليل بأكمله في موضع شك. و يتم بعد ذلك حفظ الدليل من خلال سلسلة من الخطوات المعيارية، يتم التأكد من خلالها أن الدليل لا يمكن تغييره بعد الآن. وكذلك يتم حفظ وحماية البيئة التي تحتضن الدليل لمنع الدخول إليه أو الاتصال به من خلال حماية فيزيائية، باستخدام القاصة ، كذلك استخدام أدوات حماية الشبكات التي تمنع الوصول لهذه الأجهزة و الأدلة ، و تتم هنا تعبئة نماذج خاصة بكل دليل ومكان وجوده، كما يتم كذلك التفريق بين الدليل الذي يتم حفظه في حالة أن الأجهزة كانت في حالة عمل أو كانت مغلقة.

- **<u>خامساً : مراحل استخلاص الدليل الرقمي:-</u>**

إن التطور التقني الذي لحق نظم المعالجة الآلية فضلاً عن الطبيعة الخاصة للدليل الرقمي ، سيؤدي حتما ودون أي شك إلى تغيير كثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها ، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم لمنهج بعض الإجراءات التقليدية في قانون أصول المحاكمات الجزائية ، فضلا عن إستحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية . فتطوير الإثبات و وسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الإجرام.

حيث تبدأ عملية البحث و التحري للحصول على الدليل الرقمي ، من طرف مصالح الضبطية القضائية ، من خلال تنقل الفرق المختصصة إلى مسرح الجريمة لمعاينة محل الجريمة، و جمع و حفظ الأدلة و إرسالها إلى المخبر العلمي لترجمة التحاليل بغرض تهيئة المحضر و تقديم الخبرة ، و تتبع هذه المصالح قواعد مرتبطة بحماية الأدلة من خلال : -

- حفظها بإستخدام نسخ خلال مرحلة التحليل المختبري .
- إعداد تقرير عن كل عملية تمت بالتدقيق حتى نهاية التحليل .
- تنصيب سلسلة ، و هي تثبيت الموجودات التي أفضى عنها التحليل في كل مرحلة للوصول إلى الدليل .

كما تتبع أيضاً قواعد مرتبطة بصلاحية الطرق المستعملة لارتكاب الجريمة من خلال:-

- البحث في ما إذا كانت هذه التقنية قد جربت من قبل ، و هل من الممكن تجريبها مرة أخرى .
- البحث في ما إذا كانت التقنية قد نشرت أو أخضعت للتقييم من طرف مخابر مختصة .
- البحث عن نسبة الخطا الذي يمكن أن تتضمنه التقنية ، و كذلك مختلف أشكال الرقابة الضرورية الملائمة.

و تجدر الإشارة إلى أهمية تكوين المصالح الضبطية القضائية في هذا المجال لمواكبة التطورات الراهنة و الخروج من قوقعة التعامل مع الجرائم التقليدية ، حيث تتطلب الجرائم الماماً كبيراً بتقنيات حديثة من أجل إثبات الجريمة و قمعها . كذلك من الممكن استشارة الخبراء المختصين في هذا المجال كلما دعت الحاجة إلى ذلك .

- **<u>سادساً: تحليل الدليل الالكتروني :-</u>**

من الضروري في هذه المرحلة بدء العمل على نسخة طبق الأصل من الدليل، وليس النسخة الأصلية التي تبقى للمراجعة فيما بعد، حيث تبدأ هذه المرحلة بفصل البيانات غير الضرورية لعملية التفتيش، وذلك لوجود أعداد ضخمة من المواد في الأجهزة المتحفظ عليها، التي تحتاج دراستها واحدة تلو الأخرى إلى عشرات السنين إن فحصت جميعها. و يتم في البداية فصل ما هو ضروري عما هو غير ضروري للقضية موضع البحث، كذلك يتم الفصل حسب أماكن تواجد الأدلة تبعا لطبيعة القضية قيد البحث، فمثال إن كان البحث يقتضي إيجاد صور تحتوي على مواد ممنوعة يتم التركيز فقط على الملفات من نوع صورة، ويتم استثناء غيرها.

- **<u>سابعاً: عرض الدليل الإلكتروني :</u>**

مرحلة العرض هي المرحلة النهائية في الإثبات أو النفي للأدلة الإلكترونية التي تمت معالجتها في مراحل التحقيق. و يتوقف نجاح هذه المرحلة بالدرجة الأولى على مصداقية الخبير الذي قام بهذه العملية في كيفية عرضه للأدلة وثقته بما يعرض وعدم وجود تناقض أو غموض في شهادته، كذلك ، حيث يتم فحص مدى التزامه بالمهنية والدقة . يلعب ملف التوثيق الذي قام بإعداده دوراً كبيراً بالإجراءات المعروفة والمتفق عليها في هذا المجال. ولا بد من التركيز حين عرض الأدلة على الدقة ومخاطبة الآخرين حسب درجة معرفتهم التقنية، فمثال يتم تحضير وعرض دليل مفصل للخبراء التقنيين ومن يهتم بذلك، أما أمام القضاء واالدعاء، فلا بد من عرض النتائج والملخصات وسلسلة الإجراءات التي تمت في تحليل الدليل دون التعمق في التفاصيل الجزئية.

وعليه، يتضح أن الصعوبات التي تواجه الشاهد الخبير هو عدم وجود الخبرة التقنية للجمهور في المحكمة، على عكس ما تم توثيقه من أدلة تقنية تفصيلية، وكذلك إمكانية فحص عمله من قبل خبراء تقنيين آخرين يمكن أن يطعنوا في بعض الإجراءات التي قام بها أو أهمل بعضها.

1_ د. عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دراسة متعمقة في جرائم الحاسب الآلي والانترنت ، دار الكتب القانونية ، مصر ، 2002 ، ص34 .

2- د. محمد الامين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت ، دولة الامارات العربية المتحدة، ص6 .
3- د. عبد الفتاح بيومي حجازي ، التزوير في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، مصر ، المحلة الكبرى ، 2008، ص 26.
4- د. نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في التشريع الاردني ،كلية الشريعة والقانون ، جامعة الامارات ، 2000 ،ص 3.
5- أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1981 ، ص 418.
6- و هو التعريف الذي أخذ به التقرير الأمريكي المقدم إلى ندوة الانتربول العلمية حول الدليل الرقمي عام 2001 ، عمر محمد بن يونس ، الدليل الرقمي ، 2007- 2008، ص 25 .
7- عمر محمد بن يونس ، الجرائم الناشئة عن الانترنت ، دار النهضة العربية ، مصر،2004، ص975 .
8- مرنيز فاطمة ، الإعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت ، أطروحة دكتوراه ، جامعة أبوبكر بلقايد ، تلمسان ، الجزائر ، 2013 ، ص 256 .
9- شلاب بن منصور البقمي ، دور الأساليبالعلمية الحديثة في تحديد مرتكبي التفجيرات الإرهابية ، أطروحة دكتوراه في فلسفة العلوم الأمنية ،قسم العلوم الشرطية ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2007 ، ص 219 و 220 .
10- محمد أمين البشري ، التحقيق في الجرائم المستحدثة ، المجلة العربية للدراسات الأمنية و التدريب ، اكاديمية نايف للعلوم الأمنية ، الرياض، 2008 ، ص 219
11- مولاي ملياني دلال ، الإثبات في جرائم الانترنت ، رسالة ماجستير ، جامعة بشار ، كلية الحقوق و العلوم السياسية ، سورية ، 2008- 2009 ،
12 - مرنيز فاطمة ، مرجع سابق ، ص259.
13- مرنيز فاطمة ، مرجع سابق ، ص 260
14- مولاي ملياني دلال ، الإثبات في جرائم الانترنت ، رسالة ماجستير ، جامعة بشار ، كليةالحقوق و العلوم السياسية ، سورية ،2008- 2009، ص 34.
15- مولاي ملياني دلال، مرجع سابق ، ص75 .
16- عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص42 .
17- سعيداني نعيم ، أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالةماجستير ، جامعة الحاج لخضر باتنة ، كلية الحقوق والعلوم السياسية ، 2012- 2013 ، ص123.
18- فيصل مساعد العنزي ، أثر الإثبات بوسائل التقنية الحديثة على حقوق الانسان ، رسالةماجستير، قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الامنية ، الرياض ، 2007، ص 10و11 .
19- عمر محمد بن يونس ، الجرائم الناشئة عن الانترنت ، مرجع سابق ، ص 979.
20- سعيداني نعيم ، مرجع سابق ، ص 123 .
21- عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص 45 .
22 - مولاي ملياني دلال ، مرجع سابق ، ص76 .
23- عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص46 .
24- سعيداني نعيم ، مرجع سابق ، ص124.
25عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص47.
26سعيداني نعيم ، مرجع سابق ، ص 130 .
27- مرنيز فاطمة ، مرجع سابق ، ص 268 .
28محمد أمين الشوابكة ، جرائم الحاسوب و الانترنت - الجريمة المعلوماتية - ، عمان ، 2006 ، ص16 .
29- مرنيز فاطمة ، مرجع سابق ، ص 269 .
30- سعيداني نعيم ، مرجع سابق ، ص 130 .
31- عمر محمد بن يونس ، الجرائم الناشئة عن إستخدام الانترنت ، مرجع سابق ، ص 1011 و 1012.
32- سعيداني نعيم ، مرجع سابق ، ص 132 .
33- مولاي ملياني دلال ، مرجع سابق ، ص 45 .
34مرنيز فاطمة ، مرجع سابق ، ص 270 .
35عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، مرجع سابق ، ص 1017.
36سعيداني نعيم ، مرجع سابق ، ص 134.
37- مولاي ملياني دلال ، مرجع سابق ، ص. 46.
38- مرنيز فاطمة ، مرجع سابق ، ص 271.
39المرجع السابق ، ص 271 و 272 .
40- المعيار الدولي 27037، ISO/IEC، 2012.
41- المصدر السابق.
42المصدر السابق.
43- المصدر السابق.

Харисова З. И.,
доцент кафедры криминалистики, кандидат технических наук
(Уфимский юридический институт МВД России)

О ВОЗМОЖНОСТИ ИНТЕГРАЦИИ ДАННЫХ OSINT-РАЗВЕДКИ В НЕЙРОСЕТЕВОЙ КРИМИНАЛИСТИЧЕСКИЙ КЛАСТЕР

На сегодняшний день информация, являясь одним из наиболее ценных продуктов для мирового сообщества, часто становится объектом преступного посягательства, при этом информационные технологии служат орудием такого рода злонамерений. Зародившаяся еще в годы Второй мировой войны OSINT-разведка (с англ. — opensourceintelligence) в настоящее время является действенным средством получения колоссального количества данных, что становится особенно важно с учетом глобальной цифровизации общества[1]. В результате значительного роста обрабатываемых средствами массовой информации, интернет-сервисами и веб-приложениями данных по всему миру, можно отметить наличие возможности использования структурированных объемов информации в целях формирования международного информационно-аналитического кластера криминалистических данных[2].

В основе сетевой разведки лежит принцип поиска и анализа информации из открытых источников данных, в основном, в сети интернет. Причинами популяризации сбора данных средствами OSINT в настоящее время являются:

- минимальные риски раскрытия информации о лице, который занимается разведывательной деятельностью;
- бюджетность исследований (затрат, связанных только в свете получения доступа к базам данных интересующих серверов);
- простота и географическая независимость проведения разведки;
- корреляция большого количества критериев информации в сети (начиная с построения карты перемещений пользователя, заканчивая извлечением EXIF-информации на фото).

Таким образом, возможность успешной сетевой разведки обусловлена наличием значительного количества информации в общем доступе, на основе которой можно построить модель хранилища криминалистически значимой информации с функцией нейросетевого анализа данных[3; 4].

Предлагаемая концепция системы на основе общедоступной информации (общеизвестные сведения либо информация, доступ к которой не ограничен и используемые любыми лицами по их усмотрению при условии соблюдения установленных нормативными правовыми актами ограничений в отношении распространения такой информации[5]), аналогично криминалистическим учетам в цифровом виде, определила бы возможность гибкой настройки по выдаче отчетов по интересующим следователя направлениям.

Так, в Российской Федерации возможно формирование базы путем парсинга данных официальных сайтов государственных органов, т.е. сбором информации представляемой Федеральной налоговой службой, Федеральной службой судебных приставов, Федеральной службой исполнения наказаний, МВД России, Судебным департаментом, Нотариальной палатой, Росфинмониторингом, Министерством образования и пр., а также специализированными сервисами, например, такими как: «Прозрачный бизнес», «Электронное правосудие», «Scholar.google», «Focus.kontur», «SocialSearcher», «SocialMention», «FindFace», «VIN01», «AVinfo», «Blockchain.info», поисковые Telegram-боты и множеством иных каналов информации, размещенных в глобальной сети интернет.

Необходимость поддержания инфраструктуры предлагаемой системы заключается в плановом и своевременном обновлении сформированных каталогов и инструментов для поиска данных, а также обеспечения соблюдения требований по обработке лишь общедоступных источников, а также грамотного переобучения системы после обновления баз данных[6; 7].

При этом, главной проблемой по формированию интеллектуального нейросетевого криминалистического кластера является отсутствие единых стандартов в подходе к охраняемой информации, в частности — персональных данных граждан различных стран. По этой причине актуальной задачей на этапе зарождения проекта являлось бы формирование рассматриваемой информационной системы в рамках реализации для одного государства (национального кластера) либо возможностью создания массива кластеров данных при условии их обезличивания (прием введения условных идентификаторов объектов множества кластеров)[8].

Таким образом, достоинством формирования интеллектуальной системы на основе OSINT-парсинга глобальной сети является повышение эффективности поиска необходимой для раскрытия или расследования информации, удобство обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети, снижение трудозатрат и ресурсов поиска криминалистически значимой информации.

---

[1] Официальный сайт компании ESET ADEON SK [Электронный ресурс] — Информационный портал, Республика Словения, 2021, Исследование на основе открытых источников OSINT — Режим доступа: https://eset.ua/ru/blog/view/117/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost (дата обращения: 01.10.2021).

[2] Харисова З. И., Файзулова Р. Р., Дюсьмекеева Д. С. Современные угрозы информационной безопасности в условиях глобализации информационного пространства // Актуальные проблемы кибербезопасности в сети Интернет. — 2020. — № 1. — С. 163 – 165.

[3] Антонов В. В., Калимуллин Н. Р., Харисова З. И., Герфанова М. Р. Проблемы правового регулирования сферы искусственного интеллекта // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020): Тр. VIII Всеросс. науч. конф. (с приглашением зарубежных ученых). В 2-х томах. — Уфа, 2020. С. 10 – 14.

[4] Харисова З. И., Филиппов О. А., Федоров Д. А. Искусственный интеллект в государственном управлении // Информационные технологии интеллектуальной поддержки принятия решений (ITTDS'2020): Тр. VIII Всеросс. науч. конф. (с приглашением зарубежных ученых). В 2-х т. — Уфа, 2020. С. 26 – 29.

[5] Антонов В. В., Харисова З. И., Колесников В. А. Международно-правовые аспекты обеспечения информационной безопасности в сети интернет: Учеб. пос. — Уфа, 2021.

[6] Харисова З. И. Система для экспрессного определения гранулометрического состава суспензий на основе видеотехнических средств и искусственной нейросети, дообучаемой в процессе работы // Приборы и системы. Управление, контроль, диагностика. — 2017. — № 2. — С. 57 – 64.

[7] Fetisov V. S., Kharisova Z. I., Dmitriyev O. A., Melnichuk O. V. Rapid particle size analysis of suspensions based on video technology and artificial neural network with additional training during operation // International Journal of Applied Engineering Research. — 2017. — Т. 12. — № 7. — С. 1271 – 1278.

[8] Антонов В. В., Куликов Г. Г., Харисова З. И. Теоретико-множественный подход к построению дуальной системной модели ПАК для исследуемой области деятельности со смешанными реальными и виртуальными объектами // Вестн. Южно-Уральск. гос. ун-та. 2019. Т. 20. № 1. С. 5 – 15.

Хусанов А. Д.,
начальник кафедры криминалистических экспертиз,
доктор философии (PhD) по юридическим наукам
(Академия Министерства внутренних дел
Республики Узбекистан, г. Ташкент)

Инновационные технологии в судебно-экспертной деятельности в процессе доказывания по преступлениям, связанным с нарушением правил безопасности движения

В Республике Узбекистан, как и в других странах, количество автотранспортных средств растет, что, в свою очередь, ведет к росту дорожно-транспортных происшествий, которые в силу их общественной опасности могут приобретать статус преступлений. Государственными органами принимаются соответствующие меры по пресечению, предупреждению, раскрытию и расследованию преступлений в сфере дорожно-транспортного происшествия (ДТП). Одной из действенных мер в этом отношении является эффективный уголовно-процессуальный порядок сбора доказательств посредством экспертно-криминалистической деятельности по преступлениям, связанным с нарушением правил безопасности движения или эксплуатации транспортных средств.

Данная экспертно-криминалистическая деятельность направлена на разработку, совершенствование и внедрение соответствующих научно-технических средств и методов в быстрое и качественное расследование преступлений, предусмотренных действующим уголовным законодательством Республики Узбекистан. В целях раскрытия и расследования преступлений, связанных с нарушением правил безопасности движения или эксплуатации транспортных средств, экспертно-криминалистическая служба интегрирует в себе последние достижения науки и техники. Для этого она должна осуществлять «инновационную» деятельность: успешно разрабатывать, внедрять и использовать новейшие наукоемкие технологии, обеспечивать разработку научно обоснованных методов, приемов и средств раскрытия преступлений и предварительного расследования, проводить судебные экспертизы, помогать в техническом оснащении оперативно-розыскных мероприятий.

Проведенный анализ норм уголовно-процессуального законодательства, имеющих отношение к сбору доказательств в расследовании преступлений, связанных с нарушением правил безопасности движения или эксплуатации транспортных средств, показал, что данный процесс материализуется посредством криминалистических средств и способов установления объективной истины в расследуемом уголовном деле. В научных исследованиях, посвященных расследованию ДТП, отмечается, что «повышение эффективности и качества расследования преступлений неразрывно связано с активным внедрением в деятельность правоохранительных органов достижений науки и техники»[1, 3], и, следовательно, доказательная информация основывается на возможностях науки в автотехнической сфере. Для этого органы, ответственные за расследование, обязаны привлечь соответствующих специалистов, экспертов и обеспечить своевременную, оптимальную, качественную, основанную на научно-техническом прогрессе фиксацию доказательственной информации о происшедшем ДТП.

В ст. 91 действующего УПК РУз была внесена дефиниция, связанная с определением термина «фиксация»: «фиксация процессуальных действий в виде осмотра места происшествия по особо тяжким преступлениям, обыска, проверки показаний на месте события, следственного эксперимента с использованием средств видеозаписи является обязательной»[2]. Законодатель данной новеллой дал

понять, какое значение уделяется процессуальному закреплению, то есть фиксации доказательственной информации.

Научно-теоретический анализ содержания рассматриваемого термина показывает, что оно соответствует понятию удостоверения факта совершения ДТП, который позволяет обеспечить доказательственную базу в раскрытии и расследовании данного вида преступлений.

Доказывание в уголовном процессе не ограничивается только субъективным уяснением обстоятельств дела самим дознавателем, следователем или специалистом-криминалистом. Согласно ст. 85 УПК РУз, «доказывание состоит в собирании, проверке и оценке доказательств с целью установления истины об обстоятельствах, имеющих значение для законного, обоснованного и справедливого разрешения дела». Также под доказыванием понимаются источники доказательственной информации, которые не всегда возможно приобщить к материалам уголовного дела. Поэтому уголовно-процессуальный закон предоставляет основания для их документальной или технической фиксации. На этом основании В.В. Лысенко пришел к выводу, что собирание, проверка и оценка сведений о временных характеристиках дорожно-транспортного преступления является одной из основных проблем, которые необходимо исследовать[3]. Следует иметь в виду, что доказательство, связанное с ДТП, не всегда можно легко обнаружить и зафиксировать. Поэтому следователь, дознаватель или должностное лицо, осуществляющее доследственную проверку, привлекает специалистов (экспертов), которые оказывают помощь в обнаружении и фиксации необходимых обстоятельств. При этом последние могут применять специальные криминалистические, технические средства и приборы.

Наглядным примером непосредственного применения инновационных технологий при производстве судебных экспертиз является использование приборов и оборудования, созданных на основе интеграции их и традиционных технологий. Традиционные возможности таких устройств многократно усилены современными цифровыми технологиями. Одним из таких приборов, сочетающих в себе функции оптического микроскопа и широкие возможности, присущие лазерному профилометру, является микроскоп Leica DVM6 и (производитель LeicaMicrosystems, Германия) с функцией 3D-моделирования. Являясь высокоскоростным лазерным сканирующим 3D-микроскопом, Leica DVM6 и он нужен для точных и достоверных измерений, а также для построения пространственных изображений. Изображение в микроскопе формируется в масштабе реального времени за счет использования быстродействующего оптического сканирующего модуля, а также программных алгоритмов обработки сигналов. Оптическая система микроскопа имеет максимальное увеличение, соответствующее 400х, три способа освещения (кольцевой, сегментный и коаксиальный), причем все эти способы могут быть использованы во всем диапазоне увеличений. Указанные возможности позволяют полностью решить проблему нехватки глубины резкости при больших увеличениях и проводить измерения не только в плоскости, но и по глубине[4].

Научный анализ содержания ст. 85 УПК РУз показывает, посредством какой деятельности и какого источника доказательственной информации он обнаружен. Наиболее эффективным способом создания доказательственной базы по делам, связанным с ДТП, являются предусмотренные УПК следственные действия и особенно осмотр места происшествия и назначения автотехнической экспертизы. При их проведении составляется протокол или выносится заключение эксперта, в которых фиксируются обстоятельства происшедшего ДТП. В частности, в ст. 90 УПК РУз указано, что «сведения и предметы могут быть использованы в качестве доказательств только после того, как они зафиксированы в протоколах следственных действий».

Научно-теоретический анализ обеспечения фиксации дорожно-транспортного происшествия в раскрытии и расследовании преступлений показывает, что данный технологический процесс выражается в использовании оптимального механизма использования криминалистических тактики, методики и техники, направленной на получение необходимой доказательственной информации. При этом под фиксацией в криминалистике понимаются определенные тактические действия, направленные на обнаружение и собирание доказательной базы для раскрытия и расследования преступлений.

Теоретические и тактико-методические аспекты инновационных технологий в судебно-экспертной деятельности в процессе доказывания по преступлениям, связанным с нарушением правил безопасности движения в процессе доказывания, затронул в своих исследованиях Р. Ю. Ачмиз[5].

Но он придерживается классического механизма получения доказательственной информации, а мы являемся сторонниками более широкого применения инновационных технологий в криминалистической фиксации ДТП.

В этом отношении можно согласиться с мнением В. А. Городокина, который является сторонником использования специальных автотехнических знаний при расследовании преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств[6], но при этом, на наш взгляд, необходимо шире использовать последние достижения научно-технического прогресса. В частности, видеофиксацию на дорогах и перекрестках, использование bodycamer у сотрудников дорожно-патрульной службы, которые предоставляют возможность установления фактов нарушения прав человека. Следует признать, что на современном этапе без применения самых современных технологий невозможно реально обеспечить права личности при расследовании ДТП.

Таким образом, в целях решения проблем, связанных с инновационными технологиями в судебно-экспертной деятельности в процессе доказывания по преступлениям, связанным с нарушение правил безопасности движения или эксплуатации транспортных средств, в процессе доказывания, необходимо широко применять достижения научно-технического прогресса и инновационных технологий. Для этого, по нашему мнению, следует привлекать специалистов в научно-технической сфере, психологов и иных специалистов, которые обладают соответствующими знаниями в этой области, и они как эксперты или специалисты могут оказать действенную помощь как в обнаружении и фиксировании доказательственной информации, так и в обеспечении прав личности.

---

[1] Ким О. Д. Проблемы и пути совершенствования расследования дорожно-транспортных происшествий на основе научных знаний: на материалах следственной и экспертной практики Кыргызстана: Автореф. дис. … д-раюрид. наук. — Воронеж,1998.

[2] Ст. 91 Законом Республики Узбекистан от 4 апреля 2018 года № ЗРУ-470дополнена частью четвертой // Национальная база данных законодательства, 05.04.2018 г., № 03/18/470/1005.

[3] Лысенко В. В. Собирание, проверка и оценка сведений о временных характеристиках дорожно-транспортного преступления: Автореф. дис. … канд. юрид. наук. — М., 2002.

[4] Spagnolo G. S. Potentiality of 3D laser profilometry to determine the sequenceof homogenous crossing lines on questioned documents // Forensic Science International. — 2006. — № 164.

[5] Ачмиз Р. Ю. Расследование дорожно-транспортных преступлений: Теоретические и тактико-методические аспекты: Автореф. дис. … канд. юрид. наук. — Волгоград, 1999.

[6] Городокин В. А. Использование специальных автотехнических знаний при расследовании преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств: Автореф. дис. … канд. юрид. наук. — Екатеринбург, 2009.

Черданцев А. Ю.,
следователь по особо важным делам первого отдела по расследованию особо важных дел Восточного межрегионального следственного управления на транспорте Следственного комитета Российской Федерации, аспирант кафедры криминалистики факультета подготовки научных инаучно-педагогических кадров, капитан юстиции (Московская академия Следственного комитета Российской Федерации)

ОБЛАЧНЫЕ СИСТЕМЫ ХРАНЕНИЯ ЦИФРОВЫХ ДАННЫХ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

По мере развития и повсеместного внедрения различных облачных технологий возрастает и важность подготовки к работе с ними в следственной и иной правоохранительной практике. Исходя из данных, полученных в ходе проведенного опроса действующих сотрудников правоохранительных органов показал, что лишь 45 % респондентов осведомлены об облачных технологиях и имеют некоторое представление о механизме функционирования такового, около 15 % условно понимают техническую составляющую удаленного хранения данных.

Из этого следует вывод, что фактически 85 % действующих правоохранителей из целевой группы не имеют представления о том, как в настоящее время можно получить цифровые доказательства и использовать их в уголовном процессе, осуществляя взаимодействие с облачными хранилищами больших объемов данных.

Вместе с тем облачное хранение данных представляется наиболее перспективным и динамично развивающимся направлением цифровизации общества, которая без преувеличения стала одной из самых прорывных за последние два десятилетия. Для сравнения уже в 2015 г. около 20 % ведущих

цифровых корпораций перешли на облачное хранение данных, за последние 6 лет их доля увеличилась в несколько раз[1].

При этом, как мы понимаем, быстрый рост и внедрение облачных технологий хранения данных создает большие проблемы для органов предварительного расследования в части противодействия различным преступным посягательствам и получения доказательственной информации об уже совершенных преступных деяниях. Кроме того, представляется нестандартной системой хранения информации, которую традиционная криминалистика ранее не имела возможности изучить.

Полагаем, что сотрудники экспертно-криминалистических подразделений согласятся с нашим мнением относительно того, что в настоящее время отсутствует, как законодательная база регулирующая процесс получения доказательств из различных облачных хранилищ, так и унифицированные криминалистическо-методические подходы для работы с ними.

Не вдаваясь в технические особенности формирования облачного хранилища отметим, что общепринято выделять следующие типы:

- объектное хранилище (хранят свойства и объекты в виде метаданных);

- файловое хранилище (хранят резервные копии программ, совместно используемых файлов и т. д., в т. ч. медиафайлы);

- блочное хранилище (в большинстве случаев используются предприятиями для функционирования рабочего процесса и высокой производительности)[2].

Для органов предварительного расследования наиболее интересным является второй тип облачного хранилища, так как большая часть рядовых пользователей использует именно их в повседневной деятельности (например, резервное копирование системы IOS, Android, облако Mail.ru, Dropbox, Google Диск, Mega, Яндекс.Диск, OneDrive, iCloud, Box, и др.)

При этом необходимо понимать, что хоть и существует формальное разделение возможности администрирования данного хранилища в части личных данных конкретного пользователя, но в большинстве случаев поставщик облачных услуг имеет полный административный контроль над данными пользователя и полный контроль над программным обеспечением процедуры облачного хранения, а также фактически может в определенной части администрировать устройство, подключенное к облачному хранилищу (например, удаленно деинсталлировать приложения на смартфоне пользователя, удалять данные, нарушающие политику использования программного обеспечения или устройства в целом).

Доступ к цифровой криминалистически значимой информации в облачных хранилищах станет возможен при понимании некоторых принципиальных положений, связанных с процессом его администрирования.

Так, основополагающим принципом поставщиков данного рода услуг выступает то, что они обеспечивают максимальную конфиденциальность и всеми возможными в настоящее время способами защищают предоставленными им данные своих пользователей.

Для этого осуществляется шифрование данных, зачастую не дающих возможность, даже в случае их санкционированного получения оперативно понять вид и содержание файлов, процесс расшифровки даже при наличии ключей шифрования может занять достаточно продолжительное время.

При этом сложно отрицать, что органы предварительного расследования, должны иметь своей основной целью именно получение ключей шифрования данных от администратора облачного хранилища.

Сложно переоценить значимость получения данных из облачных хранилищ по причине того, что в облачной среде данные автоматически загружаются в несколько хранилищ (зеркальное хранение), в связи с чем доказательства, утерянные или уничтоженные в одном устройстве, могут быть найдены в иных устройствах.

При этом необходимо понимать, что физическое расположение запрашиваемых данных может находиться вне юрисдикции Российской Федерации.

В качестве резонансного примера можно привести судебную практику против компании Google LLC, когда 29 июля 2021 г. мировой судья судебного участка № 422 Таганского района Москвы оштрафовал Google на 3 млн рублей за отказ локализовать данные пользователей в России[3].

За аналогичное правонарушение к административной ответственности привлекли Twitter и Facebook. Они получили штрафы по 4 млн руб.

В связи с этим, в настоящее время необходимо предусмотреть законодательное закрепление оснований, процедуры взаимодействия правоохранительных органов и получения ключей для зашифрованных данных в облачных хранилищах данных.

Относительно локализации хранения данных в юрисдикции Российской Федерации, следует отметить его принципиальность исполнения в связи с тем, что потеря контроля над средствами хранения облачных данных приведет в большинстве случаев к полной утрате возможности их получения (за исключением случаев, когда в ходе предварительного расследования будет получено устройство-пользователя, имеющего доступ и право администрировать данное облачное хранилище).

*Приведем пример из практики СО по г. Н*** СУ по Н*** области СК России, где в ходе обысков были изъят мобильный телефон IphoneXS, в ходе осмотра которого установлено наличие биометрической блокировки (FaceID) и цифрового восьмизначного пароля пользователя.*

В ходе неоднократных попыток получить доступ к устройству, в том числе с использованием автоматизированных программных комплексов UFED, мобильный криминалист иных средств доступ к устройству получен не был.

При проведении оперативно-разыскных мероприятий установлен числовой пароль пользователя, благодаря которому был разблокирован телефон и получен доступ к устройству. При осмотре устройства из облачного хранилища iCloud были получены фотоизображения (ранее удаленные с устройства), на которых был запечатлен фигурант уголовного дела, банковские карты, на которые перечислялись денежные средства, скриншоты части переписки в мессенджере WhatsApp с взяткополучателем, где было указано время и адрес места встречи.

В дальнейшем оперативными сотрудниками с близлежащих камер наружного наблюдения были изъяты видеозаписи обстановки, благодаря изучению которых за искомую дату были обнаружены лица, причастные к совершению данного преступления, их автомашины, что подтвердило факт встречи последних и косвенно доказало событие преступления.

В ходе осмотра контактов не были обнаружены искомые номера фигурантов, однако при осмотре мессенджера Telegram обнаружены ранее синхронизированные на сервер данного мессенджера контакты с номерами телефонов и именами, ранее удаленные из записной книжки телефона.

Полученные сведения доказали факт знакомства фигурантов и осведомленности о номерах для связи. Помимо этого, в истории звонков были обнаружены исходящие вызовы со временем соединения и его продолжительностью в даты совершения преступления, что в совокупности дало основания полагать, что событие преступления имело место быть.

Примеры положительного использования данного метода работы также в своем исследовании наглядно продемонстрировал А. А. Бессонов, справедливо отметив, что в целях решения задач, поставленных перед органами предварительного расследования изучается вся информация, содержащаяся в принадлежащих совершившему преступление лицу и потерпевшему (в некоторых случаях — свидетелям) компьютерах, ноутбуках, нетбуках, планшетах и т. п., из которой можно получить сведения: о лицах из круга их общения и содержании переписки с ними; файлах фотографий, содержащих сведения о месте и времени осуществления съемки; других используемых такими лицами электронных устройствах, сопряженных и синхронизируемых с изучаемым компьютером и т. п., которые возможно непосредственно использовать для установления обстоятельств расследуемого события и места нахождения скрывающегося преступника[4].

Необходимо отметить, что например сервисы GoogleLLC вообще по умолчанию собирают и хранят на серверах геоданные пользователя (рис. 1), в том числе о маршрутах его передвижения и избранных местоположениях (рис. 2), при получении доступа к этим данным их можно использовать для доказывания в уголовном процессе[5].

Взаимодействие с поставщиками услуг по облачному хранению данных в значительной степени будет зависеть от конкретного вида и типа хранилища, а также о сведениях, интересующих органы предварительного расследования, но в большинстве случаев фактически извлечение необходимой информации будет производиться самими сотрудниками поставщика услуг под контролем сотрудников, осуществляющих предварительное расследование[6, 10].

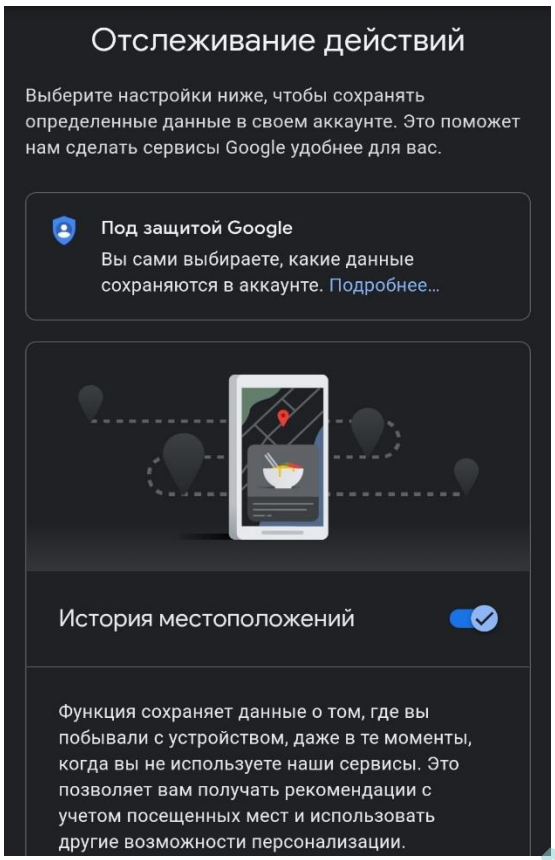


Рисунок 1

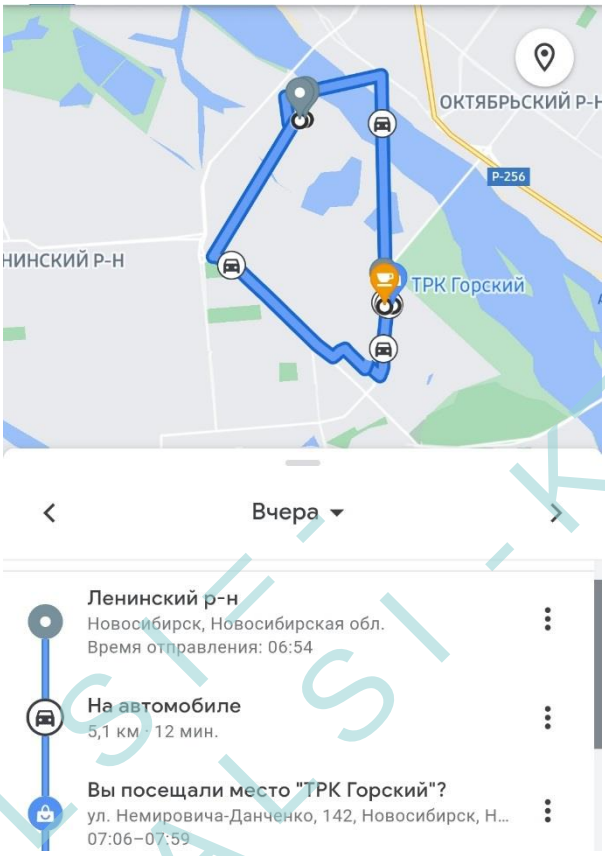


Рисунок 2

Проводя аналогию с уже имеющейся практикой, можно сказать, что в настоящее время, получая информацию о соединениях между абонентами и (или) абонентскими устройствами (с серверов поставщика телекоммуникационных услуг, при этом на российском рынке операторы сотовой связи уже начали осуществлять услуги по облачному хранению данных и управлению инфраструктурой пользователя), уже реализуется примерный механизм получения данных из облачных хранилищ в юрисдикции Российской Федерации, в связи с чем законодательное закрепление данной процедуры не трудозатратно и требует скорее доработки путем внесения изменений в законодательство, чем принципиально новых законодательных решений.

Поскольку необходимость получения криминалистически значимой информации из облачных систем хранения данных возрастает с каждым днем крайне важно, чтобы поставщики данных услуг, законодатель и сотрудники правоохранительных органов работали в тесном взаимодействии, обеспечивая, как защиту прав граждан-пользователей сервисов, так и граждан, пострадавших от преступных посягательств, нуждающихся в государственной защите, достичь которую можно, в том числе путем правомерного использования полученных цифровых доказательств из облачных систем хранения данных.

---

[1] Облачный рынок вышел на уровень 100 млрд рублей. [Электронный ресурс]. — Режим доступа: https://www.iksmedia.ru/articles/5712782-Oblachnyj-rynok-vyshel-na-uroven.html (дата обращения: 02.10.2021).

[2] Что такое облачное объектное хранилище? [Электронный ресурс]. — Режим доступа: https://aws.amazon.com/ru/what-is-cloud-object-storage/ (дата обращения: 02.10.2021).

[3] Официальный телеграм-канал столичных судов общей юрисдикции. [Электронный ресурс]. — Режим доступа: Telegram: Contact @moscowcourts(дата обращения: 02.10.2021).

[4] Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестн. Ун-та им. О. Е. Кутафина. 2018. № 3. С. 46 – 52.

[5] Как управлять историей местоположений? [Электронный ресурс]. — Режим доступа: https://support.google.com/accounts/answer/3118687?hl=ru (дата обращения: 02.10.2021).

[6] Багмет А. М., Скобелин С. Ю. Актуальные вопросы применения криминалистической техники для получения информации, содержащейся в мобильных электронных устройствах // Вестник криминалистики. — 2013. — № 4 (48).

Шеховцова Л. С.,
старший преподаватель кафедры криминалистики,
кандидат юридических наук, подполковник полиции
(Московский университет МВД России им. В. Я. Кикотя)

НАЗНАЧЕНИЕ ЛИНГВИСТИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАССЛЕДОВАНИИ ВЫМОГАТЕЛЬСТВА

Судебно-лингвистическая (далее по тексту «лингвистическая») экспертиза зародилась в конце 90-х годов прошлого века. Специалисты утверждают, что причины ее возникновения непосредственно связаны с развитием права на свободу слова[1], а, следовательно, и увеличением количества публичных высказываний социально патологичных крайних взглядов, экстремистского характера. Необходимость правильной юридической оценки таких высказываний, в свою очередь, дало толчок к развитию юридической лингвистики и становлению нового вида судебной экспертизы.

Лингвистическая экспертиза получила нормативное закрепление в отечественном законодательстве в 2005 г.[2] Первоначально ее основной направленностью был анализ текстового материала экстремистского характера, но, со временем, с развитием информационных технологий и увеличением цифрового пространства необходимость использования специальных познаний в области смыслового понимания текста стала возникать и при расследовании иных категорий уголовных дел, в том числе, вымогательств.

Анализ отечественной судебной практики последних пяти лет свидетельствует, что назначение лингвистической экспертизы при расследовании вымогательства в подавляющем большинстве случаев направлено на определение лингвистической формы речевого действия «угроза».

Статья 163 УК РФ говорит о требовании передачи чужого имущества или права на имущество, или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого. При этом юридический термин: «угроза» никак в законе не определяется. Действительно, в ряде случаев установление факта наличия или отсутствия угрозы применения насилия, уничтожения или повреждения чужого имущества не требует применение специальных знаний, поскольку они не двусмысленны и очевидны для обывателя. При этом анализ судебной практики свидетельствует, о наличии и иных случаев, когда определение лингвистической формы речевого действия «угроза» требует привлечения специалиста в области смыслового понимания текста.

К таким спорным случаям можно, в частности, отнести:

- выражение угрозы в форме обрывочных речевых фрагментов, частично доступных для смыслового понимания;
- наличие в тексте ошибок в использовании вербальных и паравербальных[3] средств русского языка, главным образом, лексических, затрудняющих, но не исключающие смысловое понимание текста;
- наличие в тексте лексических средств, толкование которых требует использования дополнительной литературы (ненормативной или специальной лексики);
- маскировка содержательных элементов текста.

Выражением угрозы в форме обрывочных речевых фрагментов может служить текст, состоящий из незаконченных непоследовательных частей, лишенных очевидной связи. Так, при экспертном исследовании файла с аудиозаписью телефонного разговора гр. С. с потерпевшим гр. М. гр. С. произносит, в том числе, фразы: «Знаешь, че я тебе сейчас сделаю, а? … у тебя зубы нижние выпадут, ты понял?», «Ты понял, куда попал?» … «Расклад быстренько», «Ты вообще не вкупаешься, куда попал?», «Хоть куда жалуйся, на меня жалоб по восемь штук в неделю приходят», «Как будем разговаривать?»[4]. Содержание разговора и даже его тематика требовала проведения лингвистического анализа, он же позволил выявить признаки адресной вербальной агрессии в форме угрозы.

Нередко в судебной практике встречаются вымогательства, совершенные с использованием замаскированной угрозы. Примером могут служить слова гр. М., владельца печатного издания, который вымогал денежную сумму под угрозой публикации материалов негативного характера о компании гр. Ш.: «Ну, я говорю, если вы не хотите дружить вдолгую, давайте дружить, или начнем хотя бы дружить, вкороткую… Я говорю, если мне кто-то закроет этот миллион двести, который я сейчас имею… Я выдохну и скажу: слава Богу, и пошлю на … этот самый, как его с компанией со всеми де-

лами. Принципиальная позиция предельно простая: вам нужно, чтобы все было спокойно, нормально, тихо. Мы делаем свои добрые дела»[5].

В результате лингвистического исследования текста разговора было установлено наличие со стороны гр. М. высказываний, содержащих вербально выраженные признаки угрозы.

В ходе лингвистической экспертизы, назначаемой по делам о вымогательстве, на разрешение эксперта лингвиста в том числе ставятся следующие вопросы:

1) Имеются ли в высказывании лингвистические признаки угрозы применения насилия (угрозы уничтожения или повреждения чужого имущества, распространения сведений, позорящих потерпевшего или его близких, иных сведений, которые могут причинить вред потерпевшему или его близким)?

2) Кто является субъектом побуждения и адресатом?

3) Имеются ли в тексте признаки маскировки его содержательных элементов?

4) Если да, то можно ли определить значение скрытых элементов текста либо их характеристики?

Для разрешения этих вопросов эксперту необходимо установить наличие или отсутствие следующих обстоятельств:

1. Коммуникативную цель, выражающую негативные намерения говорящего в будущем. Исходя из контекста, анализируя речевую ситуацию, манеру и темп разговора, используемые сторонами, идиоматические выражения эксперт устанавливает носят ли высказывания угрожающий характер непосредственно в момент их выражения или в будущем.

2. Адресность этого намерения. Эксперт определяет направленность выражения, того, к кому оно обращено, у кого должна вызвать негативный эффект.

3. Конкретное содержание негативного действия и (или) последствия. Речевое деяние описывается в основном через определенные смысловые компоненты, которые, его характеризуют. Речевая форма выражения должна содержать признаки вербальной агрессии и проявляться во вспышках гнева, крике, унижении, сообщение о применении физической силы, лишении жизни, высказанной в адрес оппонента.

3. Реальность выполнения обещания негативных последствий. То есть упоминание говорящим о специальной боевой и физической подготовки, определенном должностном положении и других возможностях, дающих основания опасаться осуществления угрозы[6].

Лингвистическая экспертиза часто назначается в комплексе с психологической экспертизой. Объясняется это тем, что установление смыслового содержания текста тесно связано с оценкой эмоциональной составляющей текста, определением скрытого смысла сообщения, а также психологической оценкой лица, выражающего вербальную агрессию.

Текст, содержащий признаки вербальной агрессии в форме угрозы может иметь форму аудиозаписи, то есть быть зафиксирован на аудионосителе. Учитывая, что криминалистическим исследованием звуковой и речевой информации занимается фоноскопическая экспертиза, в ряде сложных случаев связанных, например, с проведением акустического анализа речевых сигналов, при нарушении звукопроизношения, наличии диалектических, акцентных и иных особенностей говорящего целесообразно назначить комплексную лингвистическо-фоноскопическую экспертизу.

Проведение смыслового исследования текста в рамках лингвистической экспертизы при расследовании вымогательства позволяет расширить возможности доказывания в ситуациях, когда текст, содержащий требование передачи чужого имущества или права на имущество, или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества не очевиден для обывателя и вызывает сомнения у правоприменителя.

---

[1] Сысенко А. Р. Место лингвистической экспертизы в системе судебных экспертиз // Закон и право. — 2021. — № 3. — С. 164 – 166.

[2] Приказ МВД РФ «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с Инструкцией по организации производства судебных экспертиз в экспертных подразделениях органов внутренних дел Российской Федерации, Перечнем Родов (видов) Судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации) от 29 мая 2005 г. № 511 // Российская газета. 2005. № 191.

[3] Паравербальные средства — совокупность звуковых сигналов, сопровождающих устную речь, привнося в нее дополнительные значения.

[4] Уголовное дело № 1-4/2018 Верхнекаместкий районный суд Томской области.

[5] Уголовное дело 1-114/2018 Ленинградский районный суд г. Калининграда.

[6] Лингвистическая экспертиза. Типовая методика судебной лингвистической экспертизы: Методические рекомендации/ Под ред. В. Ф. Статкуса: — М., 2009.

Ширчин Номин-Эрдэнэ,
научный сотрудник Научно-исследовательского института,
магистр психологических наук, адъюнкт
(Университет внутренних дел Монголии, г. Улан-Батор)

ПСИХОЛОГИЧЕСКОЕ ПОРТРЕТИРОВАНИЕ ПРЕСТУПНИКА КАК ОДИН ИЗ НЕТРАДИЦИОННЫХ ПСИХОЛОГИЧЕСКИХ МЕТОДОВ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Использование нетрадиционных методов в борьбе с преступностью на современном этапе открывает новые возможности для ценной оперативно-значимой информации, профилактики и пресечения преступных действий[1, 48]. В качестве рабочей гипотезы, в заложенной в концепции применения нетрадиционных методов, лежат широко известные научные факты о том, что противоправные действия совершаются человеком, находящимся в «особом» психическом состоянии, на фоне выраженного эмоционального и нервно-психического напряжения, которое в свою очередь обуславливает его поведенческие реакции. Изучение этих «особых» психических состояний, их систематизация, поиск взаимозависимости и взаимообусловленности с факторами внешней среды и функциональным статусом, криминалистически значимых признаков преступления на практике позволяют существенно сузить круг подозреваемых и с большей эффективностью использовать имеющиеся силы и средства при розыске преступника[2, 101].

Основными научно-практическими направлениями в рассматриваемом нами в аспекте являются:

1. Использование регистраторов психологического стресса (образцов почерка, полиграфов и др.)

2. Анализ преступного поведения и построение информационной модели преступника при раскрытии серийных особо тяжких преступлений против личности.

3. Гипнорепродукция как действенный способ активизации памяти свидетелей и потерпевших.

4. Использование экстраординарных (экстрасенсорных) способностей человека для раскрытия преступлений.

5. Аудиовизуальная экспресс-оценка психологических особенностей личности в коммуникативном процессе[2, 196].

Каждое из указанных направлений имеет под собой достаточно прочную теоретическую базу, разработанную и нашедшую свое подтверждение в научных трудах академика А. К. Анохина, Л. П. Гримака, А. Р. Лурия (психофизиология), Б. Ф. Ломова, Ю. Б. Гиппенрейтера(психология) и др.

Нетрадиционные методы юридической психологии не противопоставляются традиционным, а служит дополнением к ним. Полученная с их помощью информация имеет не доказательственный, а ориентирующий характер и может быть использована в процессе проведения следственных действий и оперативно-розыскных мероприятий для формирования и выдвежения следственных и оперативно-розыскных версий[3, 107].

В практике оперативно-розыскной и следственной деятельности расследования преступлений применяются многочисленные психологические методы, но ограничиваясь объемом доклада мы затронули лишь одну из них, который, на наш взгляд, является наиболее важным и перспективным для решения оперативно-розыскных и следственных задач. Это метод психологического портретирования неизвестного преступника, которую, мы рассмотрели в рамках некоторых подходов.

*Подход составления психологического портрета по следам, обнаруженным непосредственно на месте происшествия.*Ученые и специалисты считают, что необходимость в разработке психологического портрета преступника актуальна при расследовании определенной категории преступлений, совершенные не устанновленным лицом, характеризующихся существенным или полным отсутствием сведений о конкретном виновном лице: убийств на сексуальной почве с признаками садистского истязания жертвы; убийств с посмертными колотыми и резаными ранениями; убийств, содержащих признаки манипуляций преступника с трупом жертвы; «безмотивных» поджогов и взрывов; изнасилований и др. В этом случае поиск признаков преступника осуществляется зачастую только исходя из следов и обстоятельств преступления. Их психологический анализ в рамках методики составления пси-

хологического портрета преступника способен инициировать продуктивные версии о его признаках, которые позволяют сужать круг розыска, а также выявлять виновного среди лиц, попавших в поле зрения следствия[4, 68]. С учетом этих требований в портрет преступника специалисты рекомендуют включать следующие данные:

1) общую характеристику личности и преобладающую мотивацию преступлений;
2) индивидуальные признаки личности — привычки, склонности, навыки и пр.;
3) возраст;
4) район места жительства;
5) район места работы, службы, учебы;
6) частные характеристики места вероятного обитания;
7) уровень образования и профессиональной квалификации;
8) род занятий;
9) особенности происхождения (родительской семьи) и личной истории жизни;
10) семейное положение;
11) наличие детей;
12) отношение к отдельным видам деятельности — к службе в армии, спорту, медицине, работе с людьми и пр.;
13) наличие прошлой судимости;
14) наличие психической, а также иной патологии;
15) антропологические и динамические характеристики лица (тип внешности, телосложение, пантомимика и др.).

Концептуально психологический портрет преступника строится на основе теоретического положения о личностной детерминированности всякого поведения. При этом имеют место два подхода к установлению связи между признаками преступления и преступника[5, 81].

Следующий *статистическийподход*, который основывается на существующей статистике сопряжений признаков преступника с признаками криминалистической характеристики преступления (в их совокупности), выявленной по аналогичной категории раскрытых дел. Он активно используется в практике следственно-розыскной деятельности полиции США, Англии, Голландии и некоторых других стран. Недостаток данного подхода — отсутствие содержательных суждений по поводу выводимых признаков преступника. В то же время по конкретному делу наименее статистически определенный признак может оказаться наиболее достоверным и информативным.

Далее*аналитико-психологический подход,* которыйнацелен на вскрытие субъективно-личностного содержания действий преступника, основываясь на котором выдвигается аргументированная версия о его признаках. Иначе говоря, связь признаков лица с признаками поведения здесь опосредована их психологической, смысловой взаимосвязью. В данном контексте мы рассмотрели теоретические основания, принципы и алгоритм реализации данного подхода на практике.

Также, в теории и практике психологии, исследование психических явлений исходит из конкретных действий и поступков человека, из его объективного поведения. При этом, опираясь на существование общей для внешней и внутренней деятельности макроструктуры, можно судить о способности «идеального образа», который способен оставлять свой «отпечаток» в материальной среде в виде «комплексного, личностно-регуляционного следа».

В основу разработки психологического портрета преступника положены следующие частные психологические принципыанализа происшествия:

1. Элементы криминалистической характеристики рассматриваются как результаты поведения, реализованного лицом в условиях свободного выбора, для детерминированного системой как осознаваемых, так и неосознаваемых побуждений и направленного на достижение субъективно желаемой цели.

2. Элементы криминалистической характеристики преступления рассматриваются как единая система, системообразующим принципом которой выступает личность преступника в ее субъективном отношении к другим составляющим криминалистическую характеристику элементам.

Таким образом, преступное событие как психолого-криминалистическая система включает в себя его элементы (время, место, орудие, жертву и др.) по признаку «материализованного в них идеального (психологического)», а именно субъективного отношения преступника к качественному содержанию каждого из них и в их совокупности, что и предопределяет сделанные преступником выборы[6, 123].

Данное, личностно окрашенное отношение находит внешнее проявление в «индивидуальном действии», которое трактуется по Х. Хекхаузену как действие, детерминированное индивидуальной особенностью личности.

В отличие от многофункционального словесного портрета психологический портрет отражает внутренние, психологические, а также поведенческие признаки человека. Его основная функция — быть средством поиска, выявления преступника, личность которого не установлена. Психологический портрет формируется не на основе достоверных знаний об отражаемых в нем признаках, а на базе знаний вероятностного характера. Существенно и то, что этот метод «работает» далеко не в каждом случае раскрытия преступления. Полем его применения являются лишь некоторые группы дел, и прежде всего те, что связаны с раскрытием тяжких преступлений против личности. В тех случаях, когда убийство совершено с целью ограбления, а жертва — лишь средство в достижении этой цели, применение метода психологического профиля в США считается нецелесообразным.

Для составления «психологического портрета преступника» используют следующие материалы:

- фотоснимки,фиксирующие местосовершения преступления, следы на различных участках тела-потерпевшего (ран, шрам, родинок и др.) положение трупа, сделанные с разных позиций и под разными углами;

- с помощью обширной фотодокументации криминально-технической службы, а также используя карты, планы, схемы, в комплексе анализируется все информации,непосредственно собранные сотрудниками полиции на месте преступления и вокруг него. При этом максимум внимания уделяется каждой видимой на фотографии детали, каждому зафиксированному на снимках портрету или положению, в котором было найдено тело, определяется логическая связь объектов с предполагаемым ходом преступления. Случается, что полицейские, проводившие первичный осмотр места преступления, вносят в него какие-либо изменения. Такие изменения, если они неизбежны, следует тщательно документировать и сообщать о них, иначе возникает опасность сделать позднее ложные выводы о механизме преступления. Хорошо продуманное ограждение места преступления и ловко проложенные пешеходные дорожки являются при исследовании тяжкого преступления важными предпосылками для успеха в работе на месте. Наряду с сохранением следов на месте происшествия задача криминально-технической службы состоит в создании обширной и подробной фотодокументации. При этом в каждом случае используется цветная пленка[7, 55].

Ни при каких обстоятельствах не следует экономить на фотоснимках. Важно, чтобы как близкие, так и удаленные от места происшествия окрестности были представлены достаточным количеством фотографий. Так, при совершении убийства внутри здания нужно фиксировать, не только помещение, где было найдено тело потерпевшего, но и другие помещения дома и его окрестности. Наряду с обзорными снимками желательны также фотографии деталей, зафиксированных с различных направлений и под разными углами. Фотодокументирование места преступления и его окрестностей — необходимое условие для создания психологического портрета преступника.

Материалы вскрытия трупа и исследования их результатов. При вскрытии трупа должен присутствовать сотрудник криминально-технической службы. Егозадача, с помощью фотографического метода зафиксировать весь процесс вскрытия и исследования трупа. Анализ вскрытия ориентирован на получение ответов на следующие вопросы: каким орудием, где, в какой последовательности и с какой силой были нанесены повреждения, явившиеся причиной смерти. Точная локализация повреждений на теле жертвы позволяет сделать предположение о том, была ли жертва застигнута убийцей врасплох или убийству предшествовала борьба. Интерес представляет также количество повреждений, были ли и какие повреждения нанесены посмертно, были ли ранения нанесены сквозь одежду или в область неприкрытой кожи тела. Общая картина повреждений позволяет сделать вывод о душевном состоянии убийцы в момент преступления и о том, существовали ли между ним и жертвой какие-либо отношения.

План перемещений потерпевшего до наступления смерти: место работы, место жительства, где последний раз видели жертву перед тем, как она была обнаружена на месте преступления[8, 286].

Документы с информацией о личности жертвы. В методе психологического профиля изучению жертвы придается столь же важное значение, как и изучению преступника. Для получения психологического профиля преступника необходимо иметь психологический портрет преступника жертвы. На выполнение этой работы выделяются дополнительные сотрудники, специализирующиеся в области криминалистической виктимологии. Эти сотрудники занимаются исключительно жертвой столько

времени, сколько необходимо для того, чтобы получить «точную картину жертвы», которая, на наш взгляд, должна основываться на следующих признаках: возраст; пол; физические особенности;одежда во время инцидента; семейный статус; социальная адаптированность; интеллект; успеваемость в школе; взаимоотношения в школе; стиль жизни и недавние изменения в стиле жизни; особенности личности и темперамента; манера поведения; место жительства (прежнее и настоящее); взаимосвязь места жительства и места преступления; сексуальная адаптированность; род занятий (прежний и настоящий); репутация в доме и на работе; история болезни (физические и психические особенности); личностные привычки (употребление алкоголя, наркотиков); социальные привычки; увлечения; пристрастия; друзья и враги; полицейское досье и др.

Информация о полной картине преступления и реконструкция механизма содеянного (сведения о месте, времени и дате события, показания свидетелей, род оружия, которым было совершено преступление и т. д.). С помощью характеристики жертвы, анализа места преступления, характера ран и повреждений на теле жертвы можно реконструировать предположительно последовательность событий преступления. Это часто помогает выяснению, почему преступник выбрал тот или иной способ действий. Реконструкция механизма содеянного позволяет диагностировать психологическое состояние преступника в момент совершения преступления, составить представление об уровнях природной интеллигентности и образованности преступника. Особый интерес представляет поведение преступника в так называемой ситуации после убийства (спрятал ли тело жертвы, уничтожил ли другие вещественные доказательства или в панике покинул место преступления, оставив различные следы и т. д.).

Также необходимоучесть, что существует риск получения искаженных результатов при анализе деликта методом «портретатирования». Возможные причины этого во многом кроется в отдаваемых следователем предпочтениях привычным, стереотипным суждениям, предвзятой направленности расследования. «Первоначально возникающие установки могут порождать тенденциозность в интерпретации воспринимаемых явлений». Исходя из анализа материалов уголовного дела,объективность выводов о признаках личности преступника в психологическом портрете, обеспечивается рядом общих правил, таких как:

1. Отказом от преждевременных обобщений и выводов.

*2. Вариативностью предположений.*Е. И. Регирер, изучая развитие способностей исследователя, отметил, что он «… должен держать свое воображение «на привязи», постепенно охлаждая себя суждениями о возможности и степени вероятности. Не сбрасывая с себя этой узды, необходимо почаще рассматривать всякие предположения: «если бы», «допустим, что» и всевозможные предполагаемые ситуации, связанные с некоторым риском мысли».

3. *Многократностью наблюдений*(повторяемостью) проявлений особенностей личности в других обстоятельствах и действиях. Данное требование предполагает учитывать то, что «… одна и та же форма поведения является, с одной стороны, реализацией многих индивидуально-личностных тенденций и особенностей, с другой — имеет различные объективные отражения-следы. Поэтому сделать заключение о той или иной особенности личности предполагаемого преступника можно лишь на основе анализа многих форм его поведения, отраженных в разных криминалистических элементах преступления».

4. *Контролем с помощью других методов исследования*(например, специально организованного эксперимента).

5. *Выявлением противоречий в логике действий преступника,* обстоятельствах происшествия и их между собой, ища им объяснения, не исключая возможность инсценировки.

6. *Системностью.* Отдельные объекты объединяются в системы, комплексы, обусловленные сущностью изучаемых явлений, с соблюдением такого порядка «наблюдения», чтобы ни один существенный для расследования объект не остался вне поля внимания. При этом оценивается значение одного факта в системе других фактов. Новое знание — вывод сопоставляется с известным и другими выводными знаниями. При альтернативных гипотезах о личности предпочтение отдается той, которая находит большие основания в совокупности обстоятельств преступления[9, 48]. «Реконструкция тем успешнее, чем больше информации о взаимосвязях между всеми элементами события».

Таким образом, наличие сведений, о которых говорилось выше, позволяет ответить на вопросы: что произошло на месте преступления и почему это произошло? Основная предпосылка, на которой базируется метод психологического профиля, состоит в том, что ответ на первые два вопроса подво-

дит к ответу на третий — кто мог совершить данное деяние, то есть к составлению психологического портрета преступника, отражающего существенные признаки, позволяющие судить о личных качествах и поведениях убийцы. С помощью данного метода преступник может быть описан так, как будто речь идет о хорошо знакомом и известномчеловеке. Однако,метод психологического портретирования преступника «не называет» конкретных имен. Поэтому содержащиеся в нем сведения одинаково применимы к большому количеству людей определенной категории.

Несмотря на то, что психология расследования преступлений, на сегодняшний день, считается одним из наиболее разработанных разделов юридических психологии, она подлежить дальнейшему комплексному исследованию. Обусловлено это тем, что, с одной стороны, сопровождающие общественную жизнь процессы социально-экономических и политических преобразований влияют на динамики и роста преступности, приводя к повсеместному распространению определенных видов преступлений (взяточничества, мошенничества, заказных убийств и т. д.), что в свою очередь, влечет необходимость изучения различных, в том числе и психологических аспектов их расследования. С другой стороны, повышение уровня профессионализма и организованности преступных формирований, предопределяет возникновение новых психологических особенностей труда следователя и, таким образом, вызывает необходимость определения дополнительных требований, предъявляемых данным видом деятельности к его профессионально значимым психологическим качествам.

Использование нетрадиционных методов в борьбе с преступностью на современном этапе открывает новые возможности для ценной оперативно-значимой информации, профилактики и пресечения преступных действий. Таким образом, мы рассмотрели общие психологические проблемы следствия и психологические аспекты отдельных следственных действий. В практике в следственной деятельности ни одно следственное действие не имеет самодовлеющего значения. Общие, стратегические задачи расследования преступлений обеспечиваются комплексом следственной действий.

Необходимость в разработке психологического портрета преступника актуальна при расследовании определенной категории неочевидных преступлений, характеризующихся существенным или полным отсутствием сведений о конкретном виновном лице. Основная предпосылка, на которой базируется метод психологического профиля, состоит в том, чтобыответить на вопрос«что произошло на самом деле?»(событие, фактические обстоятельства), с помощью которого решаетсяконкретный вопрос: кто совершилпреступление.Таким образом, к составлению психологического профиля, отражаются существенные характеристики и признаки преступника, указывающие на его личные качества. Данный профиль описывает психологические особенности преступника, с помощью которых можно судить об его личном качестве. Однако профиль «не называет» конкретных имен. Поэтому содержащиеся в нем сведения могут быть использованы в отношение людейопределенной категории.

Имея не только важное научное, но и практическое значение, психология расследования преступлений нуждается в постоянном обновлении имеющихся знаний и проведениии новых исследований, результаты которых, могут быть использованы в следственной деятельности, способствуют достижению целей уголовного процесса.

---

[1] Алексеева Л. В. Психологическая характеристика субъекта преступлений: Дис. … канд. психол. наук. — М., 2004.

[2] Аминов И. И. Юридическая психология: Учебн. для вузов. — М., 2011.

[3] Антонян Ю. М., Еникеев М. И., Эминов В. Е. Психология преступника и расследования преступлений: Учеб. пос. — М., 2000.

[4] Анфиногенов А. И. Психологический портрет преступника, его разработка в процессе расследования преступлений: Дис. … канд. психол. наук. — СПб., 2003.

[5] Баронин А. С. Психологический профиль убийц: Пособие по криминальной психологии и криминалистике. — Киев, 2001.

[6] Бегунова Л. А. Проблемы разработки и использования психолого-криминалистического портрета подозреваемого при раскрытии изнасилований и убийств, сопряженных с действиями сексуального характера: Дис. … канд.юрид. наук. — М., 2002.

[7] Дьячкова Ю. Е. Психологический прогноз поведения участников следственных действий при расследовании преступлений: Дис. … канд. психол. наук. — М., 2004.

[8] Еникеев М. И., Образцов В. А., Эминов В. Е. Следственные действия: психология, тактика, технология. — М., 2011.

[9] Кузьмин Р. М. Психология предварительного расследования преступлений, совершаемых осужденными в исправительных учреждениях: Дис. … канд. психол. наук. — СПб, 2003.

Югай Л. Ю.,
докторант факультета послевузовского образования,
доктор философии (PhD) по юридическим наукам
(Академия МВД Республики Узбекистан, г. Ташкент)

ТЕХНОЛОГИЯ DEEPFAKE: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Цифровая трансформация общества обусловливает внедрение информационных технологий во все сферы социальной жизни, ускорение информационных процессов в системе государственного управления, получение различного спектра услуг населением в удаленном режиме, минимизацию коррупционных составляющих и многие другие позитивные изменения.

Постановление Президента Республики Узбекистан № ПП-4996 «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» от 17 февраля 2021 г. предусматривает разработку Стратегии развития искусственного интеллекта, а также проекты по внедрению биометрических технологий, каких как систем распознания лиц (Face-ID) и голосовой верификации личности, Единой биометрической системы (далее по тексту — ЕБС) и многие другие инновационные проекты.

Кроме того, Постановлением правления Центрального Банка Республики Узбекистан № 20/5 «Об утверждении Положения о порядке цифровой идентификации клиентов» от 6 сентября 2021 г. внедряется процедура проверки и подтверждения личности клиента в автоматическом порядке.

Достаточно широкий сегмент охвата биометрическими технологиями сфер жизнедеятельности общества создает определенные риски и угрозы при недостаточно ответственном отношении к сохранности указанных персональных данных.

В 2016 г. в Гане были похищены биометрические данные избирателей. В 2017 г. были украдены биометрические данные (отпечатки пальцев) филиппинских избирателей; похищены отпечатки пальцев покупателей американской компании AvantiMarkets; кроме того, в Индии была зарегистрирована утечка из всеобщей биометрической системы Aadhaar, которая используется для аутентификации в банках и при получении государственных услуг. В 2018 г. В Зимбабве похитили отпечатки пальцев и фотографии избирателей. В 2019 г. в открытый доступ попала многомиллионная дактилоскопическая база южнокорейской компании Suprema[1].

4 и 8 октября 2021 г. наблюдался глобальный сбой Facebook и Instagram, а также мессенджера WhatsApp. При этом, в конце сентября 2021 г. на платформе хакерского форума DarkNet представлены на продажу персональные данные более 1,5 млрд пользователей Facebook[2]. После данного инцидента особую актуальность приобрел вопрос безопасности биометрических данных лиц, при этом мнения специалистов по данной проблеме разделяются[3]; [4].

На сегодняшний день биометрические параметры человека не только похищаются, но и создаются при помощи нейронных сетей и технологии машинного обучения. Одним из данных продуктов искусственного интеллекта являются дипфейки.

Дипфейки (DeepFake — «глубокая подделка») — это технология создания искусственным интеллектом цифрового двойника реальной личности. Данный цифровой двойник может иметь лицо и голос реального человека. Нейросеть изучает тысячи фотографий отдельного лица и создает видео. На сегодняшний день виртуальное пространство наполнено видео- и фотоизображениями простых людей, блогеров, артистов, политиков и других медийных людей, что, несомненно, расширяет возможности преступников.

И. Н. Подволоцкий отмечает, что цифровые технологии фиксации и хранения портретной информации требуют адаптации имеющихся приемов к оценке качественных и количественных характеристик изображений, представляемых на исследование. При сохранении признаков, присущих как фото-, так и видеоизображениям, есть много новых, свойственных только для цифровых документов (количественные и качественные параметры форматов записей, алгоритмы архивирования видеоинформации, средств визуализации, обработки, перекопирования, а возможно и умышленного воздействия на первоначальное содержание данных)[5]. При проведении судебных экспертиз данных материалов необходим комплексный подход с использованием соответствующего программно-технического ресурса. Данная ситуация осложняется еще тем, что нейронные сети постоянно совершенствуются, и фальсификацию цифровых видеоматериалов выявить становится все сложнее.

В 2019 г. Facebook совместно с Microsoft, Массачусетским технологическим институтом, Калифорнийским университетом в Беркли и Оксфордским университетом объявил конкурс по созданию и технологиям выявления дипфейков (DeepFakeDetectionChallenge)[6; 7].

Кроме того, Агентство перспективных оборонных исследовательских проектов при Министерстве обороны США работает с несколькими крупнейшими исследовательскими учреждениями страны, чтобы выявлять дипфейки[8].

При этом, в 2021 г. МВД России заключило контракт с АО «Научно-промышленная компания «Высокие технологии и стратегические системы» на разработку программного обеспечения под шифром «Верблюд» для выявления видеофейков[9]. Кроме того, Самарский университет им. С. П. Королева работает над сканером дипфейков, предназначенным для определения подлинности видеоматериалов.

На сегодняшний день участились случаи использования дипфейков в криминальных целях. К примеру, в Великобритании в марте 2019 г. после телефонного звонка руководителю крупной британской энергетической компании якобы от вышестоящего руководителя на счет мошенников было переведено 220 тыс. евро. Сгенерированный нейросетями голос имел даже присущий указанному лицу немецкий акцент и особенности интонации[10].

В январе 2021 г. Народная прокуратура Шанхая обвинила двух жителей Китая, которые при помощи дипфейков с 2018 г. обманывали налоговую службу и подделали накладные на сумму $ 76,2 млн. Они покупали фотографии людей на «черном онлайн-рынке», «оживляли» с помощью дипфейк-приложений и проходили проверку систем распознавания[11].

В начале сентября 2021 г. в социальных сетях появилось видео с участием человека, похожего на Олега Тинькова, который предлагает 50 %-ный бонус к любой сумме вложения. При переходе по ссылкам рядом с дипфейком, пользователи должны были внести свои персональные данные. Авторы подделки смогли создать «моргание» у фейкового Тинькова[12]. В 2020 г. отсутствие моргания считалось одним из признаков, позволяющих выявить deepfake.

Для противодействия данным технологиям в Калифорнии, Великобритании и Канаде запретили использовать различные голосовые, текстовые и визуальные фейки в предвыборной гонке[13]. Применение технологии DeepFake сейчас запрещается крупнейшими сайтами, включая Reddit, Twitter и Facebook.

В Китае с 1 января 2020 г. уже законодательно запрещена публикация дипфейков без специальной и различимой пометки.

Использование технологии дипфейк обязательно должно регулироваться по всему миру. М. А. Желудков считает, что необходимо создание особой системы цифровых и правовых форм защиты от технологии дипфейк[14].

С. В. Баженовым, В. Е. Дивольдом, А. А. Морозовым, Д. В. Поповым, Д. М. Сафроновым, А. В. Серовым была разработана Концепция национальной системы биометрической идентификации личности, которая определяет принципы Национальной системы биометрической идентификации личности, вопросы информационной безопасности и защиты персональных данных[15].

На сегодняшний день специалисты выделяют следующие признаки Deepfake, так называемые цифровые артефакты: отсутствие моргания у лица; неестественная частота моргания; несоответствующая и несинхронизированная мимика; неестественная подвижность головы, жестикуляции; необычный оттенок глаз, разный цвет глаз; нечеткое отображение зубов в виде белого пятна и т. д.

Киберпреступники заинтересованы в разработке, постоянном совершенствовании и внедрении инновационных высокотехнологичных подходов для осуществления своей деятельности. Если дипфейки первого поколения выявляются с вероятностью 100 %, то в случае второго поколения данные показатели составляют от 15 до 30 %. Специалисты признают, что на данный момент обнаружение DeepFake чрезвычайно сложно и все еще остается нерешенной проблемой.

Ущерб от данной категории преступлений более существенный по сравнению с традиционными видами преступлений. Последствия от них могут быть экономическими, политическими, репутационными, моральными и т. д. Кроме того, дипфейки в судебной практике влекут за собой вопрос допустимости аудио- и видеоматериалов доказательной базы (диктофонных записей, файлов видеорегистраторов и т. п.).

В связи с этим, решениями по недопущению «подделки цифровой личности» являются следующие: при осуществлении удаленной идентификации при получении банковских или государственных услуг биометрический идентификатор не должен быть в качестве основного, он должен быть альтер-

нативным; государственное финансирование и проведение и масштабных научных исследований по выявлению Deepfake; соблюдение информационной гигиены пользователями систем; организационные и технические меры безопасности; совершенствование нормативно-правовой базы в сфере оборота биометрических данных и соблюдение регламента обеспечения их безопасности.

Подводя итог, необходимо отметить, что динамичное развитие искусственного интеллекта, несомненно, позволяет поднять на новый уровень получение государственных и банковских услуг гражданами, ускорить процесс идентификации и верификации личности и многое другое. Однако при этом преступность также уходит в «цифру», возникают новые виды и способы совершения преступлений и соответственно традиционные методы борьбы с ней не всегда эффективны. В данном аспекте, основной задачей правоохранительных органов является постоянное совершенствование и внедрение инновационных программно-технических методов и средств в деятельность по раскрытию расследованию и предупреждению преступности.

---

[1] Как защитить биометрические данные пользователей от криминального использования. [Электронный ресурс]. — Режим доступа: https://sk.ru/news/kak-zaschitit-biometricheskie-dannye-polzovateley-ot-kriminalnogo-ispolzovaniya/ (дата обращения: 08.10.2021).

[2] Miklos Zoltan. Web Scrapers Claim to Possess and Sell Personal Data on 1.5 Billion Facebook Users on a Hacker Forum. [Электронный ресурс]. — Режим доступа: https://www.privacyaffairs.com/facebook-data-sold-on-hacker-forum/ (дата обращения: 08.10.2021).

[3] Россиянам рассказали про технологии защиты биометрии. [Электронный ресурс]. — Режим доступа: https://lenta.ru/news/2021/10/07/biometr/ (дата обращения: 08.10.2021).

[4] Россиянам посоветовали не пользоваться биометрическими данными[Электронный ресурс]. — Режим доступа: https://lenta.ru/news/2021/10/06/biometr/ (дата обращения: 08.10.2021).

[5] Подволоцкий И. Н. Портретные видеоизображения как объекты комплексного исследования // Вопросы экспертной практики. — 2019. — № S1. — С. 535 – 540.

[6] Brian Dolhanski, Joanna Bitton, Ben Pflaum, Jikuo Lu, Russ Howes, Menglin Wong,Cristian Canton Ferrer. The DeepFake Detection Challenge (DFDC) Dataset. [Электронныйресурс]. — Режимдоступа: https://arxiv.org/abs/2006.07397 (датаобращения: 08.10.2021).

[7] Роман Илющенко. Не верь глазам своим. [Электронный ресурс]. — Режим доступа: https://mvdmedia.ru/publications/shield-and-sword/aktualno/ne-ver-glazam-svoim/ (дата обращения: 08.10.2021).

[8] Роман Илющенко. Не верь глазам своим. [Электронный ресурс]. — Режим доступа: https://mvdmedia.ru/publications/shield-and-sword/aktualno/ne-ver-glazam-svoim/ (дата обращения: 08.10.2021).

[9] МВД заказало научную разработку по выявлению дипфейков. [Электронный ресурс]. — Режим доступа: https://www.computerworld.ru/news/MVD-zakazalo-nauchnuyu-razrabotku-po-vyyavleniyu-dipfeykov (дата обращения: 08.10.2021).

[10] Мошенничество с deepfake: темная сторона искусственного интеллекта. [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/blog/company/ PandaSecurityRus/347085.php (дата обращения: 08.10.2021).

[11] Липанова Л. Мошенники в Китае с помощью дипфейков обманули госсистему распознавания лиц на $76,2 млн. [Электронный ресурс]. — Режим доступа: https://vc.ru/legal/228953-moshenniki-v-kitae-s-pomoshchyu-dipfeykov-obmanuli-gossistemu-raspoznavaniya-lic-na-76-2-mln (дата обращения: 08.10.2021).

[12] Мошенники создали дипфейк Тинькова с обещанием бонусов[Электронный ресурс]. — Режим доступа: https://secretmag.ru/news/moshenniki-sozdali-dipfeik-tinkova-s-obeshaniem-bonusov-06-09-2021.htm (дата обращения: 08.10.2021).

[13] Желудков М. А., Бетина А. Ю. Противодействие дипфейкам при расследовании корыстных преступлений // Следственная деятельность: наука, образование, практика: тезисы докладов Международной научно-практической конференции (Минск, 24 июня 2021 г.) / Ред. кол. С. Я. Аземша (председатель) и др. — Минск, 2021. — С. 245 – 248.

[14] Желудков М. А. Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология DeepFake) // Развитие наук антикриминального цикла в свете глобальных современных вызовов обществу: Сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием (Саратов, 16 октября 2020 г.) / Под общ. ред. А. Г. Блинова, Е. В. Кобзевой. — Саратов, 2021. С. 262 – 270.

[15] Баженов С. В., Дивольд В. Е., Морозов А. А., Попов Д. В., Сафронов Д. М., Серов А. В. Создание Концепции национальной системы биометрической идентификации личности // Тр. Акад.управл. МВД России. 2020. № 2 (54). С. 41 – 53.

Янгаева М. О.,
доцент кафедры криминалистики, кандидат юридических наук
(Барнаульский юридический институт МВД России)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ (НА ПРИМЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА)

Повсеместное наступление цифрового мира неминуемо. Отличительной чертой нашего времени является стирание границ и различий между реальностью и виртуальностью[1].

Одним из наиболее ярких представителей научно-технического прогресса стал искусственный интеллект (далее — ИИ).

В 2019 г. Президентом Российской Федерации В. В. Путиным была утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 г.[2] Изначально в России ИИ рассматривался всего лишь как сквозная технология, затем в 2020 г. был создан федеральный проект «Искусственный интеллект», который стал седьмым федеральным проектом национальной программы «Цифровая экономика».

Первоначальная идея «машины, которая думает» принадлежит ученым Древней Греции. Однако, одними из родоначальников ИИ считают Алана Тьюринга, который в 1950 г. издал научную статью «Вычислительные машины и интеллект», и Джона Маккарти, который 1956 г. ввел термин «искусственный интеллект» на первой в истории конференции по искусственному интеллекту в Дартмутском колледже.

Искусственный интеллект — это технологии, позволяющие имитировать когнитивные, то есть самые сложные, функции человеческого мозга (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека[2].

Сегодня выделяют два типа ИИ —«слабый» и «сильный».

«Слабый ИИ» (или узкий ИИ) — это ИИ, обученный и ориентированный на выполнение определенных задач и моделирование определенных функций, например распознавание образов, синтез речи (голосовые помощники Siri, Алиса и т. д). «Слабый ИИ» управляет большей частью ИИ, который нас окружает сегодня.

«Сильный ИИ» (или общий ИИ) — это форма ИИ, в которой машина (компьютер) будет иметь интеллект, равный человеческому; у него будет самосознание, способное решать проблемы, учиться и планировать будущее. На сегодняшний день «сильный ИИ» является только теоретической моделью, практических примеров его использования в мире еще нет.

ИИ предусматривает алгоритмы и подходы, которые позволяют компьютерным системам имитировать работу человеческого мозга и принимать нестандартные, но эффективные решения. Считается, что нейротехнологии и ИИ могут выполнять любые, даже творческие задания, например рисовать картины или писать музыку. До появления ИИ компьютеры могли только «мыслить» логически и следовать набору инструкций, заданных человеком.

Спектр применения ИИ широк — от систем интеллектуального перевода до аналитики и прогнозов, от распознавания речи до серьезных систем безопасности (рис. 1).

В последние годы ИИ стал важным аспектом работы полиции во всем мире. Рассмотрим некоторые направления работы полиции России, в которых применяется искусственный интеллект.

Распознавание лиц.

Полицейские используют технологию распознавание лиц для поиска без вести пропавших лиц, идентификации лиц, находящихся в розыске за совершение преступления. Фото- и видеоизображения с уличных камер довольно низкого качества. Просмотр этих изображений для получения значимой информации является трудным и трудоемким. Многие территориальные органы МВД России не имеют достаточного количества специалистов для обработки большого объема изображений и их анализа. ИИ с большой точностью идентифицирует разыскиваемых людей, тем самым экономит время сотрудников полиции. ИИ может использовать параметры для идентификации лиц, которые не распознаются людьми.

Так, в Москве в 2019 г. заработал глобальный розыск преступников с городских камер с помощью технологии FindFace российской компании NtechLab. Технология считается одной из лучшей в мире по тестам, она показала свои возможности на практике: во время Чемпионата мира по футболу 2018 г. полиция с ее помощью задержала 180 подозреваемых.

В марте 2021 г. МВД России сообщило, что использование системы распознавания лиц позволило выявить и задержать в Москве свыше 260 граждан, находящихся в федеральном розыске. Реализация госпрограммы Москвы «Безопасный город» в 2020 г. способствовала раскрытию более 5 тыс. преступлений. Эффективность применения систем видеонаблюдения в раскрытии преступлений имеет ежегодный рост на 15 – 16 процентов[3].

Рисунок 1

Камеры видеонаблюдения

ИИ может не только применять технологию распознавания лиц по фото- и видеоизображениям, но также определять объекты (например, транспортные средства, оружие и т. д.) и действия (например, ДТП, массовое скопление агрессивно настроенных людей и т. д.). Часто полицейские полагаются на работу ИИ для предотвращения преступлений.

Идентификация объектов ИИ особенна важна для полицейских при проведении крупных массовых мероприятий. Так, ИИ выявляя предмет, похожий на оружие подает сигнал оператору, тот направляет патрульные наряды для проверки достоверности данной информации.

Анализируя изображения с камер уличного видеонаблюдения, ИИ может идентифицировать транспортное средство по заданным характеристикам. Например, ИИ найдет каждый черный седан, который проезжал через заданный перекресток за час. Полученные данные помогают полицейским искать похищенные транспортные средства, а также искать преступников, передвигающихся на автомобилях.

Правоохранительные органы также работают с камерами дронов, которые позволяют им исследовать большую площадь территории и быстрее участвовать в поисково-спасательных операциях. Такие дроны, оснащены функциями искусственного интеллекта для распознавания лиц и объектов.

В системе АПК «Безопасный город» проходит апробацию так называемый ИИ-Интрубот. Интрубот способен анализировать видеоизображение, параметры моторной активности, оценивать психическое состояние человека (страх, агрессию, тревогу) и прогнозировать его поведение. Благодаря этому чудо-техника бесконтактно определяет потенциально опасных людей при массовом скоплении по параметрам вибрации. Программные модули сигнализируют оператору, наблюдающему за сотнями камер: необходимо обратить внимание на этот объект! Причем, он может запоминать цели, покинувшие его поле зрения. Внедрение данной программы в обзорные скоростные видеокамеры в аэропортах, торговых центрах, на вокзалах и площадях позволит выявлять террористов, зачинщиков массовых беспорядков и даже наркокурьеров[4].

В 2020 г. МВД России представило проект по использованию искусственного интеллекта для составления фотороботов и выявления признаков серийных преступлений.

Сейчас вероятные связи между преступлениями специалисты ищут вручную. ИИ будет автоматически сравнивать детали происшествий, находить совпадения в свидетельских показаниях и документах по различным делам. Кроме того, ИИ поможет выявлять внешние особенности преступников на основе биоматериала, полученного с места преступления. Система должна выйти в эксплуатацию в 2024 г.[5]

Также Министерство внутренних дел России намерено при помощи искусственного интеллекта определять преступников по голосу. ИИ должен помогать криминалистам в обработке голосовых файлов, и безошибочно определять принадлежность записанного голоса тому или иному человеку.

Автоматизированное рабочее место «Эксперт-фоно» будет предназначено для решения задач идентификации лиц по фонограммам речи, а также технического исследования фонограмм при производстве фоноскопических экспертиз и исследований в экспертно-криминалистических подразделениях МВД России[6].

В мае 2021 г. МВД России были подведены итоги первого в истории ведомства хакатона«Искусственный интеллект на службе полиции», организатором которого выступило федеральное казенное учреждение «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации».

Благодаря усовершенствованным технологиям обработки изображений, распознаванию лиц и объектов ИИ снижает потребность в трудоемких задачах, освобождая сотрудников правоохранительных органов для выполнения более сложных задач. Неизвестно, как эти новые технологии в дальнейшем изменят роль сотрудника полиции и принесут пользу общественной безопасности. Одно можно сказать наверняка: результаты, вероятно, окажут большое влияние на всех.

---

[1] Жданов Ю. Н., Овчинский В. С. Киберполиция XXI века. Международный опыт / Под ред. С. К. Кузнецова. — М., 2020.

[2] Национальная стратегия развития искусственного интеллекта на период до 2030 года [Электронный ресурс]: Указ Президента Российской Федерации от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Искусственный интеллект на службе полиции[Электронный ресурс]. — Режим доступа: http://vestnik-glonass.ru/news/intro/iskusstvennyy-intellekt-na-sluzhbe-politsii/ (дата обращения: 05.11.2021).

[4] Хохлов Е. Е. Эффективность использования и перспективы развития аппаратно-программного комплекса «Безопасный город» в раскрытии преступлений в сфере незаконного оборота наркотиков // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сб. ст. международ. науч.-практ.конф.— М., 2019. С. 242 – 247.

[5] МВД внедрит ИИ для составления фотороботов и выявления серийных преступлений[Электронный ресурс]. — Режим доступа: https://habr.com/ru/news/t/528212/ (дата обращения: 05.11.2021).

[6] Искусственный интеллект на службе полиции.[Электронный ресурс]. — Режим доступа: http://vestnik-glonass.ru/news/intro/iskusstvennyy-intellekt-na-sluzhbe-politsii/ (дата обращения: 05.11.2021).

«Криминалистикадағы инновациялық технологиялар» атты халықаралық ғылыми-практикалық конференция бойынша
ҰСЫНЫМДАР

1. Криминалистикаға цифрлық технологияларды интеграциялау қандай да бір жаңа цифрлық криминалистиканы құру жолымен емес, жаңа криминалистикалық теорияны — криминалистиканың жалпы теориясының жаңа бөлігі болып табылатын криминалистикалық қызметті ақпараттық — компьютерлік қамтамасыз ету теориясын құру арқылы жүзеге асырылады.

2. Құжаттық информатика және информатика, математика, кибернетиканың басқа да салаларының шеңберінде жасалған мүмкіндіктерді пайдалануға мүмкіндік беретін құқық қорғау органдары мен құқық қолдану органдарының жаңа тілі — алгоритмдік құқықтық тілінің негізін құру қажет. Қазіргі заманғы криминалистиканың теориялық негіздерінің дамуы тұрғысынан құқықтық информатика мен компьютерлік криминалистика негіздерін құруға бағытталған бірқатар әзірлемелерге назар аудару керек, оларды тек ғалымдар ғана жүргізіп қоймайды, сонымен қатар нормативтік құқықтық актілерде де жариялауға болады. Осыған байланысты қылмыстық іс жүргізуді ақпараттық қоғам мен білім экономикасының барлық субъектілерін тиімді қылмыстық-құқықтық қорғауды қамтамасыз етуге мүмкіндік беретін, қазіргі заманғы құралдармен жарақтандыру үшін қылмыстық-құқықтық блоктың, экономиканың, информатиканың және ғылыми білімнің басқа салаларының барлық ғылымдары жүйесіндегі криминалистиканың барған сайын өсіп келе жатқан интеграциялық рөлін атап өту қажет.

3. Адамның сөз бостандығы мен пікірлердің плюрализмі, зиянды және криминогендік ақпараттан қорғау құқығының тепе-теңдігін сақтау мақсатында интернет-ортаны реттеу үшін құқықтық шеңберін анықтауға мүмкіндік беретін цифрлық ортада медиақауіпсіздікті криминалистикалық қамтамасыз етуге кешенді заң-лингвистикалық тәсілді қолдануды ұсынамыз.

4. «Цифрлық дәлелдеме» ұғымын Қазақстан Республикасының қылмыстық процесстік құқығында қолдануды ұсынамыз. Атап айтқанда, Қазақстан Республикасының 04.07.2014 жылғы №231-V ҚРЗ қылмыстық процестік кодексіне өзгерістер енгізуді ұсынамыз.

Алынған сәттен бастап электронды ақпарат тасығыштар деректерінің тұтастығы мен өзгермейтіндігін куәландыру үшін Америка Құрама Штаттарының мысалында хабарламалар табылған және алынған сәттен бастап өзгертілген-өзгертілмегенін анықтау үшін қолдануға болатын «қауіпсіз хэштау стандартын» анықтауды ұсынамыз.

Шетелдік Қызмет Провайдерлерінен электрондық дәлелдемелерді алу үшін қылмыстық құдалау органдарына, прокурорлар мен соттарға «Басқа елдерден электрондық дәлелдемелерді сұрату тәртібі жөніндегі практикалық нұсқаулықты» жұмыста пайдалану үшін ұсынылады. БҰҰ 2019 жылдың қаңтарында шығарылған.

5. Қылмыстарды жеткілікті ашу және тергеу мақсатында криминалистикалық техниканың пәндік саласына технологияларды одан әрі бекіту және зерттеу мүмкіндігімен ақпаратты берудің цифрлық құралдарын бейімдеу арқылы дамыту және енгізу толығымен негізделген.

6. Құқық қорғау және арнайы органдар бөліністерінің жедел, тергеу және сараптама қызметінің қызметкерлеріне міндетті түрде рұқсат бере отырып, бағдарламалық өнім немесе мобильді қосымша форматында техникалық құралдардың интеграцияланған тізбесі (ақпараттық бюллетень, ведомость, жіберілім) құрылымында ғылыми-техникалық құралдардың жекелеген түрлерінің тактикалық-техникалық сипаттамалары мен қолдану алгоритмдерін жүйелі түрде жариялауды ұсынамыз.

7. Сыбайлас жемқорлыққа қарсы іс-қимылдың құралдары мен механизмдерін үкіметтің электрондық басқару саласындағы практикасына енгізуді қарастыру, бұл саяси шешімдерді жақсартуға әкеледі, қабылданатын шешімдердің ашықтығының жоғары дәрежесін қамтамасыз ету және мемлекеттік басқаруда есеп беруді арттыру бойынша мемлекет қойған міндеттерді тиімді іске асыруға ықпал ететін болады. Мобильді технологиялар мен қосымшаларда сапалы, қолжетімді, өзекті деректерді жинауды қамтамасыз ету оларды сыбайлас жемқорлыққа қарсы күресте табысты пайдалануға мүмкіндік береді.

8. Ресей тәжірибесін қолдану және жол картасына заманауи криминалистиканы дамыту бойынша келесідей ұсыныстарды енгізу:

- цифрлық криминалистика саласындағы ғылыми зерттеулерді қолдау;

- қылмыстарды тергеу мақсатында жасанды интеллект технологияларын пайдаланатын бағдарламалық қамтамасыз етуді әзірлеу және дамыту;

- алдын ала тергеу міндеттерін шешу үшін қажетті аппараттық және бағдарламалық қамтамасыз етудің қол жетімділігін арттыру;

- құқық қорғау органдарын жасанды интеллект технологияларымен, білікті кадрлармен ақпараттандыру және қамтамасыз ету деңгейін арттыру;

- жасанды интеллект технологияларын дамыту мен пайдалану деңгейін ескеретін құқық қорғау және сараптама органдары арасындағы өзара іс-қимылдың кешенді жүйесін құру.

9. «Цифрлық тұлғаны жалған жасау» туралы алдын алу үшін келесілерді сақтау қажет:

- банктік немесе мемлекеттік қызметтерді алу кезінде қашықтықтан сәйкестендіруді жүзеге асыру кезінде биометриялық сәйкестендіргіш негізгі емес, балама болуы тиіс;

- Deepfake анықтау бойынша мемлекеттік қаржыландыруды және ауқымды ғылыми зерттеулер жүргізуді көздеу;

- жүйе пайдаланушыларының ақпараттық гигиенаны сақтауы;

- ұйымдастырушылық және техникалық қауіпсіздік шараларын сақтау;

- биометриялық деректер айналымы саласындағы нормативтік құқықтық базаны жетілдіру және олардың қауіпсіздігін қамтамасыз ету регламентін сақтау.

10. Көздің түсіне арналған IrisPlex бет әлпетінің фенотипін болжау жүйелерімен, көздің және шаштың түсіне арналған HIrisPlex, сондай-ақ көздің, шаштың және терінің түсіне арналған Hirisplex-S бет әлпетінің фенотипін болжау жүйесінің кеңейтілген нұсқасымен жұмыс істеуді жалғастыру. Жүйені қазақ популяциясына тән бет әлпетінің фенотипін қалыптастыруға жауапты гендердің полиморфты сайттарымен толықтыру, осылайша болжамның дұрыстығын арттыру. Бұл жүйелерді отандық практикаға криминалистика саласынан басқа, медицина (пигментация патологиясы), физикалық антропология және археология саласы (ежелгі ДНҚ бойынша сыртқы келбетті қайта жаңарту) үшін енгізу. Қазақтар популяциясындағы сыртқы келбет фенотиптері әртүрлілігінің генетикалық негіздерін зерделеу үшін жасалған алғышарттар аралас ғылымдарға тартылатын болады.

11. Сот сараптамасы мен криминалистикада практикалық қолдану үшін, зерттеу барысында алынған 23 аутосомды STR-локус аллельдерінің пайда болу жиілігін қамтитын нәтижелерді пайдалану. Генетикалық сәйкестендіру және биологиялық туыстықты орнату кезіндегі ДНҚ-ны зерттеу нәтижелері сенімді, маңызды болып табылады.

12. «SVX-3Ki» сараптамалық жарық көздерін байқаудан алынған нәтижелерді оқиға орындарын тергеу барысында жұмыс істеу кезінде де, зерттеу жүргізу кезінде зертханалық жағдайларда да көрінбейтін және нашар көрінетін іздерді табу үшін енгізу.

13. Полиграфологиялық тестілеу нәтижелерін Қазақстан Республикасының Қылмыстық сот ісін жүргізуде ЖІҚ шеңберінде сұрау нысанында және ҚР ҚПК 80-бабына сәйкес қылмыстық процеске маманның қатысуы нысанында пайдалануға кеңес береміз.

Әртүрлі тремор датчиктарын қолдану бағытында полиграфологиялық жабдықты жетілдіру. «AQI-QAT» полиграфында тремордың бес датчигі пайдаланылуы мүмкін, бұл полиграфиялық тексерудің дәлдігі мен сенімділігін едәуір арттыруға мүмкіндік береді. Бұл датчиктер: мата қаптамасындағы мотор белсенділігі; металл плиталары бар мотор белсенділігі; әмбебап пьезоплетизмограммалар және бет мимикасы; динамикалық қарсылықты анықтайтын екі компонентті модульдер; шайнау бұлшықетінің треморын бекітетін — «жақ сенсоры».

14. Оқиғалардың детальдарын автоматты түрде салыстыру, куәгерлік айғақтарда және әртүрлі істер бойынша құжаттарда сәйкестіктерді табу, оқиға орнынан алынған биоматериал негізінде қылмыскерлердің сыртқы ерекшеліктерін анықтау үшін жасанды интеллект (ЖИ) пайдалануды ұсынамыз. ЖИ криминалисттарға дауыстық файлдарды өңдеуге көмектеседі және жазылған дауыстың белгілі бір адамға тиесілігін дәл анықтайды.

15. Ақпаратты ашу немесе тергеу үшін қажетті іздеу тиімділігін арттыру, желінің бір сегментіндегі кілт сөздер мен сүзгілерді қолдана отырып, көптеген деректерді өңдеудің ыңғайлылығы және криминалистикалық маңызды ақпаратты іздеудің еңбек шығындары мен ресурстарын азайту үшін ғаламдық желінің OSINT-парсингіне негізделген зияткерлік жүйені қолдануды ұсынамыз.

16. Қазіргі уақытта қолданылатын АДИС ПАПИЛОН – 7-ні ПАПИЛОН – 9-ға ауыстыруды ұсынамыз, өйткені жаңа нұсқадағы нейрондық желі түрінде «жасанды интеллектті» қолдану арқылы қамтамасыз етілетін артықшылықтар «күрделі», аз ақпараттандырылған іздерді анықтау, сондай-ақ автомат-

ты түрде құрылған ұсыныс тізімдерінде қашықтағы позицияларды иеленетін кандидаттар арасында шынайы сәйкестіктерді анықтау мүмкіндігі болып табылады, бұл олардың көру тереңдігін түбегейлі арттыруға мүмкіндік береді, ал нақты оператордың үлесі қысқартылған ұсыныс тізімдерінің жазбаларын қарау болып қалады.

17. Смартфондарда, графикалық планшеттерде және т.б. стилус қаламының көмегімен жасалған қолжазба мен қолтаңбаны зерттеу әдістемесін әзірлеу қажет.

18. Қылмысқа қатысы бар адамдарды анықтау және іздестіру мәселелеріне, сондай-ақ сыртқы келбеті реконструктивті немесе пластикалық хирургия арқылы өзгертілген адамдарды анықтау процесіне кешенді пәнаралық тәсілді қолдану қажет деп санаймыз. Мұндай жағдайларда реконструктивті немесе пластикалық хирургия саласындағы тиісті мамандарды кеңес беру үшін де, сыртқы түрі өзгеруі мүмкін адамдарды медициналық куәландыру кезінде де тартқан жөн.

19. Адамдарды сканерлеу арқылы жедел сәйкестендіру жүйесін жетілдіру, бұл адамның сыртқы келбетін кез келген жағдайда, кез келген ерекше жағдайсыз (жарықтандыру, беттің орналасуы және т. б.) фотографиялық дәл көшіруге мүмкіндік береді. 3D сканерлеуді келесі бағыттар бойынша пайдалану: біріншіден, субъективті портретті қайта құру және бет әлпетті реконструкциялау; екіншіден, өзара әрекеттесуді, фото және видео есептердің мәліметтер базасы арасындағы интеграцияны біріктіру және реттеу, есепке алу кезінде жасанды интеллектке негізделген радиалды базистық функциясы бар (RBF — Radial Basis Function Network) нейрондық желінің мүмкіндіктерімен 3D сканерлеуді пайдалану, бұл адамның сыртқы келбетін әртүрлі бұрыштан алынған бейнесуреттер арқылы тексеруге және сәйкестендіруге нақты мүмкіндік береді.

20. 3D сканерлеу, МоСари және қайталанатын нейрондық желі (DCNN) негізінде 3D модельдерінің көмегімен, адамның жүрісін тану әдісін қолдана отырып, бағдарламалық жасақтаманы құрастыру. Бұл нейрондық желі кеңістіктік аймақтағы кіріс сигналдарын жинақтайды және суреттер сияқты жаппай сигналдарды өңдеуге бағытталған. Сыртқы деректерді талдау DCNN бағдарламасын пайдалану негізінде, адамның моделін қолдана отырып, осы нұсқаулықтарды алдын-ала анықтау арқылы жүру ерекшеліктерін алу үшін белгіленген нұсқауларға сәйкес жүзеге асырылады. Болашақта адамның сыртқы келбетіне негізделген модель келе жатқан силуэттердің тізбегін алу арқылы жұмыс істейді. Соңғы кезең қайталанатын нейрондық желі арқылы жүру туралы ақпаратты беру, содан кейін тіркелген тұлғаның 3D моделіне қабаттасу және бейімделу болады.

21. Алдын ала зерттеу кезеңінен бастап зерттеу нәтижелерін бағалауға және тұжырым жасауға дейін портреттік сараптамалар/зерттеулер жүргізу үшін отандық мамандандырылған бағдарламалық қамтамасыз етуді әзірлеу. Болашақ автоматтандырылған жүйе нейрондық желі (жасанды интеллект) негізінде суреттерді өңдеуге мүмкіндік беруі керек. Бұл автоматтандырылған жүйе көп платформалы болуы керек, кез келген заманауи операциялық жүйелерде, Windows, Lenux немесе Ubuntu жүйелеерінде дұрыс жұмыс істеуі керек. Бағдарлама техникалық жағынан меңгерілуі бойынша қарапайым болуы және компьютерлік бағдарламалық жасақтамамен жұмыс істеу туралы білімі жоқ адамдарда да жұмыс істеуге қиындық туғызбауы тиіс.

22. Бәсекелестік сараптамалық ортаның жоқтығын ескере отырып, заң шығарушы алдында сарапшы мәртебесін ІІО криминалист — мамандарына қайтару туралы мәселеге бастамашылық жасау. ІІО-да тиісті мамандарды даярлау және оларды криминалистикалық зерттеулердің тиісті ғылыми негізделген әдістемелеріне оқыту мүмкіндігі бар. Бұл кейіннен ІІО-ның ССО-да сараптама жүргізуге жұмсаған орасан зор қаржылық шығындарын қысқартады. Қазіргі уақытта сарапшының мәртебесі маманнан гөрі жоғары деп санауға ешқандай іс жүргізу негіздері жоқ, ал сарапшының қорытындысы маманның қорытындысына қатысты үлкен дәлелге ие.

23. Еңбек жағдайлары зиянды жұмыстармен айналысатын адамдар санатына маман-криминалист мамандығын енгізу туралы мәселесін қарастыру.

24. Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясында киберқылмысқа қарсы іс-қимыл жөніндегі цифрлық хаб (оқу және ғылыми-зерттеу құрылымдарының кешені, оның ішінде цифрлық полигонның) құрылсын, оның базасында ақпараттық жүйелерді пайдалана отырып жасалатын қылмыстық құқық бұзушылықтарға қарсы іс-қимыл (алдын-алу, анықтау, жолын кесу, ашу, тергеу) негіздері бойынша ІІО қызметкерлерін даярлау, сондай-ақ осы саладағы криминалистикалық зерттеулер ұйымдастырылсын.

РЕКОМЕНДАЦИИ
МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ»

1. Интеграция в криминалистику цифровых технологий идет по пути не создания новой — цифровой — криминалистики, а создания новой криминалистической теории — теории информационно-компьютерного обеспечения криминалистической деятельности, которая является частью общей теории криминалистики.

2. Создать основы для нового языка правоохранителей и правоприменителей — алгоритмического юридического языка, позволяющего использовать возможности, которые уже имеются для этого в рамках документальной информатики и других отраслей информатики, математики и кибернетики. С точки зрения развития теоретических основ современной криминалистики обратить внимание на ряд разработок, нацеленных на создание основ правовой информатики и компьютерной криминалистики, которые не только ведутся учеными, но и постулируются в нормативных правовых актах. В этой связи необходимо отметить и все возрастающую интегрирующую роль криминалистики в системе всех наук уголовно-правового блока, экономики, информатики и других отраслей научного знания, для оснащения уголовного судопроизводства современным инструментарием, позволяющим обеспечить эффективную уголовно-правовую защиту всех субъектов информационного общества и экономики знаний.

3. Применять комплексный юридико-лингвистический подход к криминалистическому обеспечению медиабезопасности в цифровой среде, что позволит определить правовые рамки для регламентации интернет-среды в целях соблюдения баланса права человека на свободу слова, плюрализма мнений и защиты от вредоносной и криминогенной информации.

4. Ввести понятие «цифровое доказательство» в уголовно-процессуальное право Республики Казахстан, в частности, внести соответствующие изменения в Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК.

Для удостоверения целостности и неизменности данных электронных носителей информации с момента изъятия на примере Соединенных Штатов Америки определить «стандарт безопасного хеширования», который может использоваться для определения, были ли сообщения изменены с момента их обнаружения и изъятия.

Для получения электронных доказательств у зарубежных провайдеров услуг органам уголовного преследования, прокурорам и судам использовать в работе «Практическое руководство по порядку запроса электронных доказательств из других стран», выпущенное ООН в январе 2019 г.

5. В целях успешного раскрытия и расследования преступлений развивать и внедрять технологии в предметную область криминалистической техники путем адаптации цифровых средств передачи информации с возможностью ее дальнейшей фиксации и исследования.

6. Систематически освещать тактико-технические характеристики и алгоритмы применения отдельных разновидностей научно-технических средств в структуре интегрированного реестра (информационного бюллетеня, ведомости, рассылки) технических средств, в формате программного продукта или мобильного приложения, с обязательным предоставлением доступа сотрудникам оперативных, следственных и экспертных подразделений правоохранительных и специальных органов.

7. Рассмотреть вопрос внедрения инструментов и механизмов противодействия коррупции в практику правительства в области электронного управления, что приведет к улучшению политических решений, будет способствовать эффективной реализации поставленных государством задач по обеспечению высокой степени прозрачности принимаемых решений и повышению подотчетности в государственном управлении. Обеспечение сбора качественных, доступных, актуальных данных в мобильных технологиях и приложениях позволит успешно использовать их в борьбе с коррупцией.

8. Применить опыт России и включить в Дорожную карту развития современной криминалистики следующие предложения:

- поддержка научных исследований в области цифровой криминалистики;
- разработка и развитие программного обеспечения, в котором используются технологии искусственного интеллекта для целей расследования преступлений;

- повышение доступности аппаратного и программного обеспечения, необходимого для решения задач предварительного расследования;

- повышение уровня информированности и обеспечения правоохранительных органов технологиями искусственного интеллекта, квалифицированными кадрами;

- создание комплексной системы взаимодействия между правоохранительными и экспертными органами, учитывающей уровень развития и использования технологий искусственного интеллекта.

9. Для предупреждения «подделки цифровой личности» соблюдать следующее:

- при осуществлении удаленной идентификации при получении банковских или государственных услуг биометрический идентификатор должен быть не основным, а альтернативным;

- предусмотреть государственное финансирование и проведение масштабных научных исследований по выявлению Deepfake;

- соблюдать пользователями систем информационную гигиену;

- соблюдать организационные и технические меры безопасности;

- совершенствовать нормативно-правовые базы в сфере оборота биометрических данных и соблюдать регламент обеспечения их безопасности.

10. Продолжить работу над системами прогнозирования фенотипа внешности лица IrisPlex — для цвета глаз, HIrisPlex — для цвета глаз и волос, а также над расширенной версией системы прогнозирования фенотипа внешности лица HIrisPlex-S — для цвета глаз, волос и кожи. Дополнить систему полиморфными сайтами генов, ответственных за формирование фенотипа внешности лиц, специфичных для казахской популяции, таким образом повысить достоверность прогнозирования. Внедрить эти системы в отечественную практику не только в сфере криминалистики, но и в сфере медицины (патология пигментации), физической антропологии и археологии (реконструкция внешности по древней ДНК). Созданные предпосылки для изучения генетических основ разнообразия фенотипов внешности в популяции казахов будут задействованы в смежных науках.

11. Использовать полученные в ходе исследования результаты, содержащие частоты встречаемости аллелей 23-х аутосомных STR-локусов, для практического применения в судебной экспертизе и криминалистике. Результаты исследования ДНК при генетической идентификации и установлении биологического родства являются достоверными, актуальными значимыми.

12. Внедрить результаты апробации источников экспертного света «SVX-3Ki» для обнаружения невидимых и слабовидимых следов как в ходе осмотров мест происшествия, так и в лабораторных условиях при проведении исследований.

13. Использовать результаты полиграфологического тестирования в уголовном судопроизводстве Республики Казахстан в форме опроса в рамках ОРД и в форме участия специалиста — в уголовном процессе, в соответствии со ст. 80 УПК РК.

Усовершенствовать полиграфологическое оборудование в части применения разнообразных датчиков тремора. В полиграфе «AQIQAT» может быть использовано пять датчиков тремора, что позволяет значительно повысить точность и надежность полиграфной проверки. Это датчики: двигательной активности в тканевом чехле; двигательной активности с металлическими пластинами; универсальные пьезоплетизмограммы и мимики лица; двухкомпонентные модули выявления динамического противодействия; «датчик челюстей», фиксирующий тремор жевательной мышцы.

14. Использовать искусственный интеллект (ИИ) для автоматического сравнения деталей происшествий, нахождения совпадений в свидетельских показаниях и документах по различным делам, выявлении внешних особенностей преступников на основе биоматериала, полученного с мест происшествий. ИИ помогает криминалистам в обработке голосовых файлов и безошибочно определяет принадлежность записанного голоса тому или иному лицу.

15. Использовать интеллектуальную систему на основе OSINT-парсинга глобальной сети для повышения эффективности поиска необходимой для раскрытия или расследования информации, удобства обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети и снижения трудозатрат и ресурсов поиска криминалистически значимой информации.

16. Заменить используемые в настоящее время АДИС ПАПИЛОН – 7 на ПАПИЛОН – 9, поскольку преимущества, обеспечиваемые применением искусственного интеллекта в форме нейросети в новой версии заключаются в возможности идентифицировать «сложные», малоинформативные следы, а также обнаруживать истинные совпадения среди кандидатов, занимающих удаленные позиции в ав-

томатически сформированных рекомендательных списках, что позволяет радикально увеличить глубину их просмотра, при том что на долю настоящего оператора останется просмотр записей усеченных рекомендательных списков.

17. Разработать методику проведения исследования почерка и подписи, выполненных с помощью стилус-ручки на смартфонах, графических планшетах и т. п.

18. Применять комплексный междисциплинарный подход к вопросам установления и розыска лиц, причастных к совершению преступления, а также к процессу отождествления лиц, внешний облик которых был предположительно изменен посредством реконструктивной либо пластической хирургии. В таких случаях целесообразно привлекать соответствующих специалистов в области реконструктивной либо пластической хирургии как для дачи консультации, так и для проведения медицинского освидетельствования лиц, внешность которых предположительно могла быть изменена.

19. Усовершенствовать системы оперативного отождествления с помощью сканирования лиц, что даст возможность фотографически точно воспроизводить по цифровой копии внешний вид лица человека в любом положении, без каких-либо специальных условий (освещение, положение лица и т. п.). Использовать 3D-сканирование по следующим направлениям: во-первых, реконструкция внешности и воссоздание субъективного портрета; во-вторых, интегрировать и наладить взаимодействие, интегрирование между базами данных фото- и видеоучетов, использовать при постановке на учет 3D-сканирование, с возможностями нейронной сети, имеющей в своем интерфейсе радиальную базисную функцию (RBF — Radial Basis Function Network), основанную на искусственном интеллекте, что даст реальную возможность верификации и идентификации внешности человека по видеоизображениям, полученным с различным ракурсом.

20. Разработать программное обеспечение с использованием метода распознавания походки человека с помощью 3D-моделей, на основе 3D-сканирования, MoCap и рекуррентной нейронной сети (DCNN). Данная нейронная сеть свертывает входные сигналы в пространственной области и направлена на обработку массивных сигналов, например, изображений. Анализ внешних данных осуществляется на основе использования программы DCNN, по фиксированным ориентирам для извлечения особенностей походки, путем предварительного определения этих ориентиров с помощью модели человека. В дальнейшем модель на основе внешнего облика человека функционирует путем извлечения последовательностей силуэтов идущего. Заключительным этапом будет передача информации о походке через рекуррентную нейронную сеть с последующим наложением и адаптацией регистрируемого лица на 3D-модель.

21. Разработать отечественное специализированное программное обеспечение для проведения портретных экспертиз/исследований от стадии предварительного исследования до оценки результатов исследования и формулирования выводов. Будущая автоматизированная система должна позволять производить обработку изображений на основе нейронной сети (искусственного интеллекта), обладать мультиплатформенностью, исправно работать на любых современных операционных системах поколения Windows, Linux или Ubuntu. Технически программа должна быть проста в освоении даже людьми с недостатком знаний по работе с компьютерным программным обеспечением.

22. Учитывая отсутствие конкурентной экспертной среды, инициировать перед законодателем вопрос о возвращении статуса эксперта специалистам-криминалистам ОВД. В ОВД имеются возможности подготовки необходимых специалистов и обучения их соответствующим научно обоснованным методикам криминалистических исследований. Это в дальнейшем сократит огромные финансовые затраты ОВД на производство экспертиз в ЦСЭ. В настоящее время какие-либо процессуальные основания считать, что эксперт выше по статусу, чем специалист, а заключение эксперта обладает большей доказательственной способностью, по отношению к заключению специалиста, отсутствуют.

23. Рассмотреть вопрос о включении специалиста-криминалиста в категорию лиц, занятых на работах с вредными условиями труда.

24. Создать в Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова цифровой хаб (комплекс учебных и научно-исследовательских структур, в том числе цифровой полигон) по противодействию киберпреступности, на базе которого организовать подготовку сотрудников ОВД по основам противодействия (профилактики, выявления, пресечения, раскрытия, расследования) уголовным правонарушенениям, совершаемым с использованием информационных систем, а также проведение криминалистических исследований в данной области.

МАЗМҰНЫ • СОДЕРЖАНИЕ

ПРИВЕТСТВЕННЫЕ СЛОВА

ДОКЛАДЫ НА ПЛЕНАРНОМ И СЕССИОННОМ ЗАСЕДАНИЯХ

КРИМИНАЛИСТИКАДАҒЫ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

Халықаралық ғылыми-практикалық конференциясының материалдары

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Материалы международной научно-практической конференции

INNOVATIVE TECHNOLOGIES IN CRIMINALISM

Materials of the international scientific and practical conference

2021 жылғы 29 қазан

29 октября 2021 г.

October 29, 2021

Авторлық редакцияда жарияланады.

Публикуется в авторской редакции.

Published in the author's edition.

Жиналымға 27.09.2021 жіберілді. 08.10.2021 басылымға қол қойылды. Форматы 60×841/16.
Офсеттік басылым. Офсеттік қағаз.
Шартты баспа табақ 27,75.
Тиражы 100 дана. Тапсырыс № 609

Сдано в набор 27.09.2021 г. Подписано в печать 08.10.2021 г. Формат 60×841/16.
Печать офсетная.
Бумага офсетная. Усл. печ. л. 27,75.
Тираж 100 экз. Заказ № 609

Handed over to the set 09/27/2021. Signed to print on 08.10.2021. Format 60×841/16.
Offset printing. Offset paper.
Conditional printed sheets 27.75.
Circulation 100 copies. Order № 609

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының ғылыми-зерттеу және редакциялық баспа жұмысын ұйымдастыру бөлімі

Отдел организации научно-исследовательской и редакционно-издательской работы Карагандинской академии МВД РК им. Б. Бейсенова

Department of the organization of research and editorial and publishing work of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenova

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының баспаханасында басылып шығарылды.
Қарағанды қ., Ермеков көш., 124

Отпечатано в типографии Карагандинской академии МВД РК им. Б. Бейсенова.
г. Караганда, ул. Ермекова, 124

Printed in the printing house of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after B. Beisenov. Karaganda, st. Ermekova, 124