Костанайская академия Министерства внутренних дел Республики Казахстан
им. Ш. Кабылбаева

УДК 343.985.7

На правах рукописи

ДЖИЛКИШИЕВ РУСЛАН БУЛАТОВИЧ

Расследование преступлений в сфере информационных технологий

8D12301 - Правоохранительная деятельность

Диссертация на соискание
степени доктора философии (PhD)

Научные консультанты:
доктор юридических наук,
профессор
Бегалиев Е.Н.

доктор юридических наук,
доцент
Аубакирова А.А.

Республика Казахстан
Костанай, 2025

Джилкишиев Р.Б.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ..... 3
ВВЕДЕНИЕ..... 5
1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ..... 11
1.1 Современное состояние и перспективы противодействия преступлениям в сфере киберпреступности..... 11
1.2 Уголовно-правовая характеристика правонарушений в сфере киберпреступности..... 30
1.3 Содержание элементов криминалистической характеристики правонарушений в сфере информационных технологий и киберпреступности..... 46
1.4 Международный опыт в противодействии киберпреступности..... 73
2 ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ И АЛГОРИТМЫ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ ОБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ..... 95
2.1 Начало досудебного производства и обстоятельства, подлежащие доказыванию по уголовным делам об информационных технологиях и киберпреступности..... 95
2.2 Типичные ситуации на первоначальном этапе расследования информационных технологий в сфере киберпреступности и алгоритм действий следователя…..... 106
2.3 Последующий этап расследования уголовных дел о правонарушениях в сфере информационных технологий и киберпреступности..... 134
ЗАКЛЮЧЕНИЕ..... 161
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ..... 173
ПРИЛОЖЕНИЯ
Приложение А Акт внедрения..... 184
Приложение Б Акт внедрения..... 185
Приложение В Акт внедрения..... 186

Джилкишиев Р.Б.

ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

В настоящем диссертационном исследовании применены следующие обозначения и сокращения:

АНБ	-	Агентство Национальной Безопасности
АСУ ТП	-	автоматизированные системы управления технологическими процессами
АФМ	-	Агентство Республики Казахстан по финансовому мониторингу
БРИКС	-	Объединение государств: Бразилии, России, Индии, КНР, ЮАР, ОАЭ, Ирана, Египта, Эфиопии и Индонезии
ГП	-	Генеральная прокуратура
ДП	-	департамент полиции
ЕРДР	-	Единый реестр досудебного расследования
ЕС	-	Европейский Союз
ЕС3	-	Европейский центр по борьбе с киберпреступностью
ЖЭК		жилищно-эксплуатационная контора
ЗРК	-	Закон Республики Казахстан
ИИ	-	искусственный интеллект
ИТ	-	информационные технологии
КПСиСУ	-	Комитет по правовой статистике и специальным учетам
КНБ	-	Комитет национальной безопасности
КРК	-	Конституция Республики Казахстан
КУИ	-	книга учета информации
МВД	-	Министерство внутренних дел
НАТО	-	Организации Североатлантического договора
НПО	-	неправительственная организация
НСД	-	негласные следственные действия
НЦУКЦК	-	Национальный центр управления кибербезопасностью и цифровой криминалистики
ОВД	-	органы внутренних дел
ООН	-	Организация Объединенных Наций
ОРД	-	оперативно-розыскные действия
ПК	-	персональный компьютер
ПО	-	программное обеспечение
п., п.п.	-	пункт, подпункт
РК	-	Республика Казахстан
РФ	-	Российская Федерация
СЕ	-	Совет Европы
СМИ	-	средства массовой информации

Джилкишиев Р.Б.

СНГ	-	Содружество Независимых Государств
СПАК	-	Специализированный программно-аналитический комплекс
ст., ст. ст.	-	статья, статьи
США	-	Соединенные Штаты Америки
УК РК	-	Уголовный кодекс Республики Казахстан
УНП ООН		Управление Организации Объединенных Наций по наркотикам и преступности
УПК РК	-	Уголовно-процессуальный кодекс Республики Казахстан
ФБР	-	Федеральное бюро расследований
ФСБ	-	Федеральная служба безопасности
ч., ч.ч.	-	часть, части
ШОС	-	Шанхайская организация сотрудничества

Джилкишиев Р.Б.

Джилкишиев Р.Б.

ВВЕДЕНИЕ

Актуальность темы исследования. Основоположниками становления информационных технологий (середина XX в.) принято считать Клода Шеннона и Роберта Винера, работы которых заложили основы для понимания процессов передачи и обработки информации и оказали значительное влияние на развитие автоматизированных систем. Достижения в области компьютеров, современных телекоммуникаций и средств связи стали, своего рода, «спусковым механизмом» для развития абсолютного нового сектора экономики, демонстрирующего самые быстрые темпы развития на сегодняшний день.

Процесс усовершенствования и развития технологий характеризуется значительными изменениями в существующих системах коммуникации. Доминирующие две формы общения вплоть до середины XX века — почта и печатные издания (газеты, журналы, книги) — были интегрированы и объединены в единое информационно-коммуникационное — кибернетическое пространство.

Появление персональных компьютеров и интернета в 1970-х годах, а позже создание глобальной сети Интернет привело к кардинальным изменениям в различных сферах жизни человека, включая экономику, образование, медицинское обслуживание и социальные взаимодействия. Это в свою очередь привело к развитию новых форм преступности, связанных с использованием информационных технологий. В настоящей диссертационной работе предполагается исследовать вопрос совершения противоправных деяний через глобальную сеть интернет или международных систем связи.

Сеть Интернет предоставляет ряд неоспоримых преимуществ для совершения противоправной деятельности. В первую очередь, это неограниченный объем различной информации (текстовая, графическая, аудио-, видео-), передаваемой по сети. Во-вторых, возможность использования психологических приемов для манипулирования пользователями в глобальных масштабах.

Согласно статистическим сведениям, с 2021 по 2025 годы в Казахстане зарегистрировано 345 деяний: 2021 – 41, 2022 – 50, 2023 – 43, 2024 – 60, 2025 – 151 – в сфере информационных технологий и киберпреступности [1].

Совершаемые киберпреступления имеют высокий уровень латентности, наносят значительный ущерб как индивидуальным пользователям, так и коммерческим компаниям и государственным учреждениям. Учитывая вышеперечисленные моменты, становится очевидным, что традиционные методы расследования противоправных деяний являются недостаточными и малоэффективными. Это делает задачу усовершенствования методов борьбы с киберпреступностью одной из приоритетных в сфере правопорядка и безопасности, что, в свою очередь, создает потребность в разработке специальных методик, учитывающих специфику компьютерных правонарушений [2, с. 65].

Актуальность киберпреступности с одной стороны, недостаточная ее разработанностью, с другой стороны (детально будет рассмотрено в рамках данной диссертационной работы), вызывает острую необходимость дальнейшего развития криминалистики как научной дисциплины, использование знаний из различных областей науки (информационные технологии, психология, юридические науки и пр.), а также улучшение существующих методов расследования и разработки новых подходов.

Несмотря на наличие значимых исследований в отдельных областях расследования киберпреступлений, в настоящее время наблюдается нехватка целостности и системности работ, охватывающих все аспекты криминалистической методики расследования, отсутствует достаточная интеграция методов и знаний, что снижает (затрудняет) эффективное расследование данной категории дел.

Таким образом, с нынешним состоянием знаний и рекомендаций в области расследования киберпреступлений необходимо глубокое, системное исследование, способное оказать реальное влияние на практическую деятельность и повышение эффективности расследования в данной сфере, поскольку отдельные частные рекомендации могут быть полезны в отдельных случаях, но не носят системный характер. Практические работники нуждаются в четких, системных и интегрированных методах работы, полученные же несистематизированной, частичной информации не может решить основные проблемы, с которыми сталкиваются следователи. Стремление разработки более системной методики, желание предложить новые подходы, основанные как на теории, так и на практике, подтолкнуло нас к выбору данной темы диссертационной работы.

Целью настоящего диссертационного исследования является разработка практических рекомендаций, направленных на повышение эффективности процесса расследования противоправных деяний в сфере информационных технологий. Нами поставлены следующие **задачи:**

- проанализировать текущую ситуацию в сфере противодействия киберпреступности;
- разработать классификационные признаки преступлений в сфере информационных технологий;
- раскрыть содержание элементного состава криминалистической характеристики киберпреступлений;
- выявить механизмы начала досудебного производства расследования преступлений в сфере информационных технологий;
- сформулировать алгоритмы первоначального этапа расследования преступлений в сфере информационных технологий;
- разработать алгоритмы последующего этапа расследования преступлений в сфере информационных технологий.

Объектом данного диссертационного исследования являются противоправные деяния, совершаемые в сфере информационных технологий, а также изучение практических аспектов их раскрытия и расследования.

Джилкишиев Р.Б.

Предметом диссертационного исследования является выявление закономерностей и уникальных черт, характерных для противоправных деяний рассматриваемой сферы, методов и подходов, используемых для расследования, определение следственных действий, которые следователю следует предпринимать в ходе первоначальных и последующих следственных действий.

Методологическая основа диссертационного исследования включает в себя различные методы и подходы. В методологической основе — использование дидактических принципов и системного подхода, позволяющие рассматривать предмет исследования в контексте более широкой системы. Применение сравнительно-правового и статистического методов способствует проведению более глубокого анализа, а также позволяет сопоставить различные аспекты расследования противоправного деяния в рассматриваемой сфере.

Теоретической основой диссертации являются: Конституция Республики Казахстан, а также международные правовые акты, относящиеся к теме диссертации. Проанализированы в части, соответствующей объекту исследования, действующее уголовное, уголовно-процессуальное законодательство, а также имеющаяся по теме литература, позволившая построить работу как логическое продолжение и развитие ранее проводившихся исследований в сфере информационных технологий, с учетом новых реалий, сопоставив с ними полученные результаты.

В своей работе диссертант исходил из научных достижений в области исследования теоретических проблем уголовного права и процесса, который внесли: Ж.К. Аманов, Е.О. Алауханов, Б.Т. Исатаева, А.Н. Агыбаев, К.А. Бегалиев, Б.А. Бекназаров, В.Б. Вехов, Р.Е. Джансараева, А.А. Исаев, В.В. Крылов, Е.И. Каиржанов, И.Ю. Лоскутов**,** В.А. Мещеряков, В.Ю. Рогозин, И.И. Рогов, С.М. Рахметов, Л.Н. Соловьев, Т.Б. Сеитов, Б.Х. Толеубекова.

Нормативную базу диссертационного исследования составили: международные правовые акты, Конституция Республики Казахстан, Уголовно-процессуальный кодекс РК, Уголовный кодекс РК.

Эмпирической основой диссертационного исследования послужили данные проведенного автором анализа статистических отчетов за 2021-2025 годы в предоставленных Комитетом правовой статистики и специальных учетов ГП РК по правонарушениям, в сфере информационных технологий, законы «О национальной безопасности», «Об информатизации», «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», Уголовный кодекс РК, Кодекс РК «Об административных правонарушениях», Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (постановление Правительства РК от 20.12.2016 г. №832), Концепция кибербезопасности («Киберщит Казахстана»).

В диссертации автор использовал личный опыт работы на различных должностях в правоохранительных органах.

Научная новизна исследования. Используемый системный подход впервые позволил не просто изучить отдельные вопросы расследования преступлений в сфере информационных технологий, но и провести их комплексный анализ в контексте более широкой системы во взаимосвязи и взаимодействии исследуемой проблемы с другими элементами.

Настоящий диссертационный труд затронул ряд ключевых проблем организационного, тактического, методического характера, а также правовые и этические аспекты, работу правоохранительных органов.

Предложены новые идеи, способствующие лучшему пониманию и систематизации знаний о противоправных деяниях в рассматриваемой сфере, представляющие теоретический интерес.

Выводы и рекомендации, выработанные в ходе исследования, могут быть применимы в практической деятельности органов правопорядка и других организаций, имеющих непосредственное отношение к расследованию правонарушений в сфере информационных технологий.

На рассмотрение вынесены отдельные вопросы, касающиеся превентивных мер совершения преступлений в сфере информационных технологий.

Новизна работы обусловлена также существенным изменением нормативной правовой базы, сложившейся в последние годы обширной судебной практикой применения нового законодательства по правонарушениям в сфере информационных технологий.

Положения, выносимые на защиту:

1. Проведенным исследованием осуществлена авторская категоризация совокупности мер и усилий правоохранительных органов и служб, участвующих в раскрытии и расследовании киберпреступлений, которая включает в себя правовое регулирование; специализацию правоохранительных органов; технические инструменты и методы расследования; международное сотрудничество, которые, при условии взаимных реализаций, могут оказать эффективное воздействие на текущую ситуацию в сфере совершения рассматриваемой разновидности преступлений.

2. Предложена классификационная характеристика уголовно-правовых правонарушений, составы которых подпадают под собирательную дефиницию «Правонарушения в сфере информационных технологий», среди которых: неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК); неправомерное уничтожение или модификация информации (ст. 206 УК); нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК); неправомерное завладение информацией (ст. 208 УК); принуждение к передаче информации (ст. 209 УК); создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК); неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК); предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК); неправомерные изменение

Джилкишиев Р.Б.

идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК).

3. Создан авторский вариант криминалистической характеристики преступлений в сфере информационных технологий, включающий в себя следующие элементы: предмет преступного посягательства; время, место, орудие и обстановка совершения; способы подготовки, совершения и сокрытия правонарушений в сфере информационных технологий; следовая картина; типологические особенности личности правонарушителя в сфере информационных технологий; причины и условия, способствующие совершению правонарушения в сфере информационных технологий.

4. Аргументирован прикладной инструментарий автора, применительно к началу досудебного производства: какие конкретно данные или системы подверглись воздействию злоумышленников, каков характер преступления, какова структура объекта, где, возможно, было совершено противоправное деяние. Следователю необходимо проанализировать условия, в которых функционирует объект: способ обработки и хранения данных; система документооборота (товарооборота); параметры оборудования и программного обеспечения, позволяющие определить способ взаимодействия между компьютерами и пользователями; уровень организации мер безопасности для защиты конфиденциальной информации; должностные инструкции сотрудников, в чьи обязанности входит обработка и хранение компьютеров и информации, ставшей объектом преступного посягательства.

5. Разработана автором классификация однотипных и неоднотипных следственных ситуаций первоначального этапа расследования правонарушений в сфере информационных технологий, которые обусловливают основные направления раскрытия и расследования рассматриваемых правонарушений, выбор оптимального алгоритма действий по организации и производству необходимого комплекса неотложных следственных действий, включающие в себя: а) наличие лишь частичной информации о факте самого правонарушения, личности пострадавшего, отсутствие сведений о лице, совершившем правонарушение, мотивы которого неясны; б) имеется полная информация о личности пострадавшего, мотивах совершения правонарушения и лицах, его совершивших, однако подозреваемое лицо заявляет о своей непричастности и отказывается от дачи признательных показаний; в) имеется полная картина следствия, однако подозреваемое лицо не желает сотрудничать со следствием, заявляя о своей непричастности к совершенному противоправному деянию, отказываясь признавать свою вину; г) подозреваемое лицо сотрудничает со следствием, полностью признав свою вину в совершении противоправного деяния, давая признательные показания.

6. Обоснован алгоритм производства проверочных следственных действий на последующем этапе расследования преступлений в сфере информационных технологий, с целью преодоления противоречий, устранения

Джилкишиев Р.Б.

нестыковок и несоответствий по следующей формуле: следственный эксперимент – последующие допросы – дополнительные экспертизы.

Теоретическое и практическое значение исследования обусловлено масштабностью, актуальностью и новизной рассмотренных в нем проблем. Целью выработки практических рекомендаций, как результата настоящего диссертационного исследования, является совершенствование законодательства в сфере информационных технологий и киберпреступлений.

Материалы диссертации могут найти применение в научно-исследовательской и преподавательской работе высших юридических учреждений, при повышении квалификации работников правоохранительных органов, при организации научных исследований по данной проблематике (Приложения А, Б, В).

Структура работы логически организована и соответствует общепринятым стандартам научного исследования. Работа состоит из введения, двух основных разделов, 6 подразделов, заключения, списка использованных источников и приложений.

Джилкишиев Р.Б.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

1.1 Современное состояние и перспективы противодействия преступлениям в сфере киберпреступности

Состояние в Казахстане

Процессы глобализации информационных технологий предоставляют огромные возможности для воздействия на людей и общество. Одним из негативных последствий является развитие преступности в сфере высоких технологий, когда компьютеры или сети Интернет выступают в качестве объекта преступлении и способа (средства) совершения преступлений.

Интересным является позиция специалистов «Лаборатории Касперского» о том, что киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли [3].

Как следует из Концепции, кибербезопасность охватывает широкий спектр мер и практик, направленных на защиту информации и систем от различных угроз. То есть под кибербезопасностью понимается комплекс технических и организационных мер, направленных на защиту данных в цифровом формате, ресурсов и информационных систем от несанкционированного доступа, возможных утечек, повреждений и прочих внутренних и внешних угроз [4].

В условиях развития инновационных технологий и цифровых сервисов особую тревогу вызывает нарастающая угроза киберпреступности. Преобладают преступления, связанные с мошенничеством и хищениями денежных средств со счетов граждан. Такими преступлениями наносится колоссальный ущерб не только экономике, но и национальной безопасности страны. Они затрагивают интересы широких слоев населения и носят трансграничный характер.

Сумма ущерба, нанесенного мошенничеством в целом, за 5 лет (2021-2025 гг.) превышает 300 млрд тенге, в том числе по интернет-мошенничеству – 39 млрд тенге. При этом возмещаемость составила не более 20 % и 6,3 %, соответственно [1].

Киберпреступления могут совершаться при помощи различных способов, включая методы социальной инженерии, когда потенциальная жертва вводится в заблуждение с целью получения с нее финансовых средств. Это может быть предоплата за несуществующие услуги или кража персональных данных, дающих возможность доступа к аккаунтам и банкам. Высокий уровень нераскрываемости киберпреступлений связан с высокой степенью анонимности через иностранные IP-адреса, что значительно усложняет их выявление и задержание. Большой пласт проблем возникает из-за отсутствия правовых оснований для расследования киберпреступлений, поскольку они совершаются с территорий третьих стран, которые имеют разное законодательство. Данный

Джилкишиев Р.Б.

аспект значительно затрудняет совместное расследование данного вида преступлений, а также обмен информацией. В настоящий момент четкий механизм международного сотрудничества между правоохранительными органами стран и представителями социальных сетей отсутствует. Это еще более в значительной степени затрудняет борьбу с киберпреступностью [5].

В конце 50-х годов XX века мировое сообщество наблюдало резкий экономический рост и технологический бум, что привело к увеличению использования компьютеров и информационных технологий. Увеличение доступности технологий, их интеграция в повседневную жизнь человека открыли также новые возможности и для совершения преступной деятельности, то есть развитие технологий создало и новые уязвимости, используемые мошенниками. Таким образом, развитие общества привело к росту преступности в сфере компьютерной информации, такой как киберпреступления, мошенничество и утечка данных.

Данный период характеризируется ростом значимости знаний и навыков, что приводит и к росту числа людей, занятых в сферах, имеющих отношение к информации и технологиям, следовательно, и к числу людей, имеющих доступ к ним. Преобладание сферы услуг, науки, образования и культуры изменило структуру экономики, увеличив число пользователей информационных систем, тем самым увеличив риски совершения киберпреступлений.

Таким образом, середина XX века стала поворотным моментом в развитии информационных технологий. Работы Винера и Шеннона позволили понять способы передачи и обработки цифровой информации, что стало основой для дальнейшего развития компьютерных технологий. Это, в свою очередь, привело к развитию нового, быстрорастущего сектора экономики — сектора информационных технологий, что открыло не только новые возможности, но и новые риски, связанные с киберпреступностью.

Указанные изменения не могли не коснуться сложившихся систем коммуникаций. Развитие цифровых технологий привело к слиянию в единое информационно-коммуникационное пространство двух основных форм коммуникаций: печатные издания (почта, газеты, журналы, книги), распространяемые методом физической передачи (хранимые в библиотеках), и средства радио и телевидения, имеющие закодированные сообщения, передаваемые посредством радиосигналов или кабельной связи. Это пространство получило название киберпространства, создавшего не только множество удобств для потребителей информации, но и породив ряд глобальных проблем с точки зрения права и правоприменителей [6].

Информационная структура представляет собой основу для функционирования современного общества и имеет колоссальное влияние на такие сферы жизнедеятельности как экономика, социальные отношения и безопасность. К ее основным компонентам можно отнести:

- hardware: средства вычислительной техники, обеспечивающие обработку и хранение данных (физические устройства: компьютеры, серверы, сети и пр.);

Джилкишиев Р.Б.

- software: программно-математическое обеспечение, обеспечивающее взаимодействие с аппаратным обеспечением, а также обработку данных и выполнение различных задач;

- communications: системы и технологии, посредством которых осуществляется передача данных и информации между устройствами, в том числе мобильные сети, коммуникационные каналы, сеть Интернет [7].

Отличительной особенностью информационной структуры является стойкая тенденция увеличения численности средств вычислительной техники и роста числа их пользователей. Это приводит к более эффективным процессам управления, однако также требует внимания к безопасности и защиты информации [8].

Глобальная сеть Интернет позволила более эффективно использовать ресурсы, кардинально изменив подходы к бизнесу в различных сферах, предоставив новые возможности доступа к информации [9]. На сегодняшний день интернет — неотъемлемая часть практически всех сфер жизнедеятельности человека, включая не только бизнес, но образование, медицину и многие другие. С развитием глобальной сети получили широкое распространение:

- маркетплейсы (онлайн платформы, предоставляющие услуги покупки/продажи товаров и услуг широчайшего спектра);

- новые способы поиска работы, в том числе платформы для фриланса и удаленной занятости;

- различного рода услуги: информационные (получение актуальной информации в реальном времени, например, о состоянии фондовых, биржевых рынков, аналитические обзоры, прогноз погоды и пр.), консультационные (получение советов по различным вопросам), лечебные (получение медицинской консультации и даже диагностики без необходимости визуального посещения специалиста).

Все это стало возможным, благодаря легкости доступа к информации и возможности взаимодействия через Интернет. Однако с развитием технологий возникли и новые виды правонарушений, имеющих отношение к использованию компьютеров и информационных технологий — киберпреступлений (хакерство, мошенничество, вирусы и пр.). Крайне важно адаптировать действующее законодательство к новым реалиям, связанным с киберпространством. Законодателем Республики Казахстан закреплены такие понятия как «компьютерные правонарушения», «информационные правонарушения» [10].

Как было обозначено ранее, использование глобальной коммуникационной системы Интернет объединило миллионы пользователей по всему миру и создало новые возможности для коммуникаций, обмена информацией, ведения бизнеса. Но также и открыло двери для злоупотреблений и совершения противоправных деяний [11]. На этом хотелось бы сделать особый акцент.

Джилкишиев Р.Б.

IT-специалисты отметили, что «интернет быстро превращается из общественного собрания и рынка в зону конфликта, где угроза исходит от многих факторов. Мы находимся на грани; мы можем сохранить Интернет, как ресурс для нашего и будущих поколений во всем мире – независимо от страны происхождения, политических или религиозных убеждений, или позволить ему быть уничтоженным взаимным недоверием и ограниченными интересами» [12].

На сегодняшний день проблема борьбы с киберпреступностью приобрела международный характер. В современном компьютеризованном обществе почти все виды преступлений могут совершаться с помощью имеющейся компьютерной технологии и все расширяющейся сферы ее применения. Особую озабоченность вызывают две тенденции развития преступности в сфере высоких технологий.

Во-первых, благодаря транснациональным информационным сетям, прежде всего Интернету, такая преступность может миновать любые границы.

Во-вторых, организованные преступные группировки. Оценка потерь, которые несет экономика в развитых странах Запада, составляет гигантские цифры – порядка миллиардов долларов. Очевидно, что информационные технологии развиваются с огромной скоростью. Возможности вторжения в частную жизнь или, по крайней мере, потенциальные возможности тоже возрастают.

Кроме этих очевидных аспектов (возможности и цена) есть также целый ряд важных факторов, влияющих на нарушения прав человека:

- глобальность, то есть исчезновение географических границ для потока данных;
- конвергенция, то есть падение технологических барьеров между системами;
- мультимедиа, то есть современные формы представления данных и изображений; информация, представленная в одном формате, может быть легко конвертирована в другие форматы [13].

По мнению Завотпаевой А.Т., преступления, связанные с использованием высоких технологий, выходят за рамки обычных и нередко представляют собой неразрешимые для действующего законодательства задачи. Первоначально столкнувшись с преступностью в данной категории, правоохранительные органы начали борьбу с ней при помощи традиционных правовых норм о краже, присвоении, мошенничестве, злоупотреблении доверием. Однако такой подход оказался не вполне удачным, поскольку многие преступления не охватываются составами традиционных преступлений [14, с. 24].

Итак, анализ статистических данных отражает явную тенденцию роста зарегистрированных преступлений в сфере информационных технологий и связи на территории Казахстана за последние пять лет (с 2021 по 2025 гг.). За указанный период органами следствия было зафиксировано всего 345 уголовных правонарушений: минимальное число – 41 случай – отмечено в 2021 году, а максимальный уровень достигнут в 2025 году, составив 151 деяние (2022 – 50, 2023 – 43, 2024 – 60) [1] (рисунок 1).

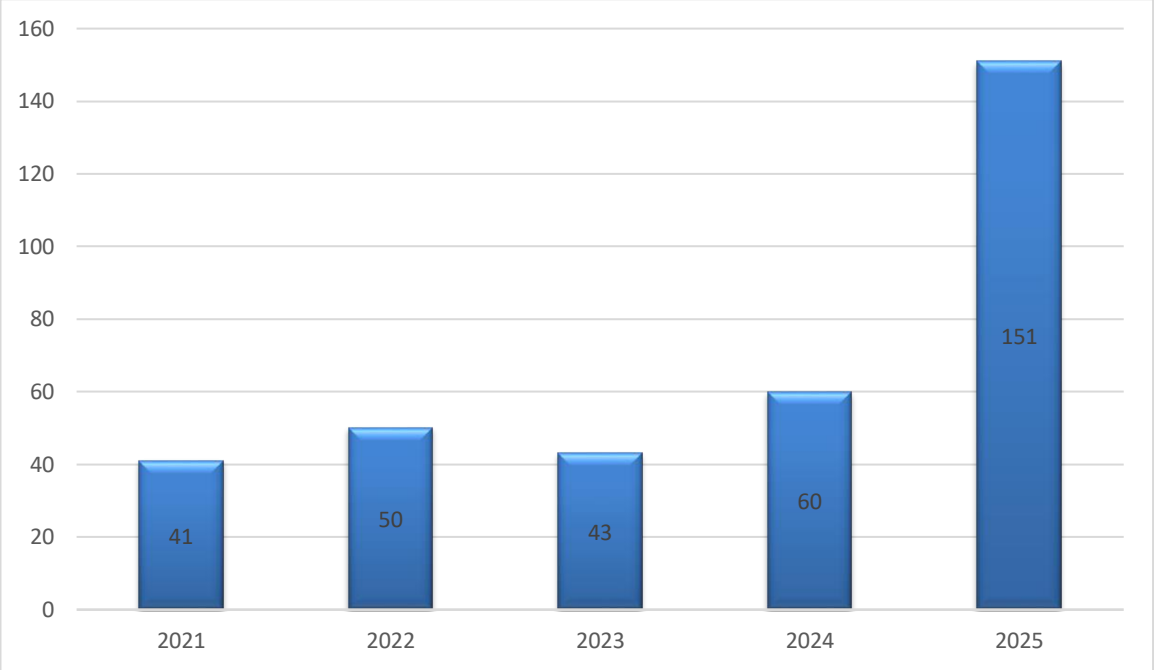

Рисунок 1 - Количество зарегистрированных в ЕРДР правонарушений в сфере информационных технологий и связи

Таким образом, количество правонарушений за пятилетний период увеличилось практически в 3,7 раза, что обусловлено активным проникновением современных цифровых и телекоммуникационных технологий, а также неуклонным увеличением числа пользователей сети Интернет и различных средств коммуникации.

Аналогичная тенденция прослеживается и в статистике уголовных дел, находившихся в производстве. За рассматриваемый промежуток времени количество таких дел устойчиво увеличивалось и составило: в 2021 году – 94 дела, 2022 – 112, 2023 – 106, 2024 – 118, а в 2025 году достигло рекордного значения – 219 дел [1] (рисунок 2). Прирост за пятилетие составил 133%, что подчеркивает значительное усиление активности правоохранительных органов в сфере выявления и расследования преступлений указанной категории.

Джилкишиев Р.Б.

Джилкишиев Р.Б.

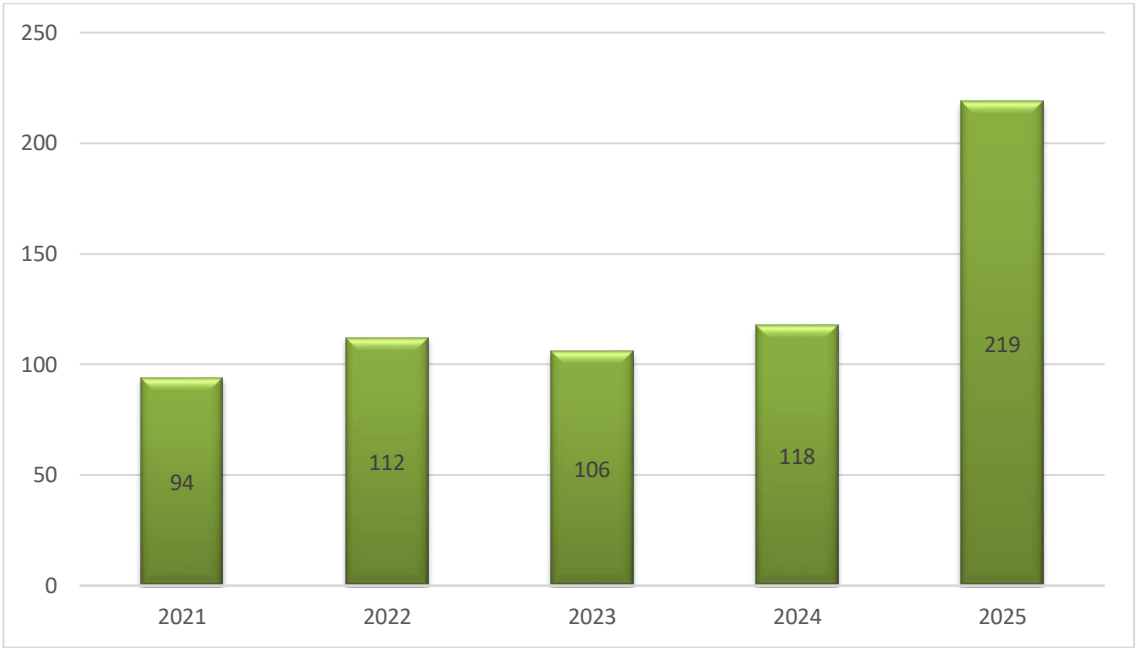

Рисунок 2 - Количество правонарушений в сфере информатизации и связи, находившихся в производстве

Отдельного внимания заслуживает показатель уголовных дел, направленных в суд. Несмотря на очевидный рост количества расследуемых уголовных производств, число переданных в суд дел остается на сравнительно низком уровне и характеризуется следующими значениями: в 2021 году – 11, в 2022 году – отсутствовали, в 2023 году – 3, в 2024 году – 20 и в 2025 году – 29 дел [1] (рисунок 3), что обстоятельство может свидетельствовать как о наличии сложностей при сборе доказательственной базы, так и о низкой эффективности следственных мероприятий.

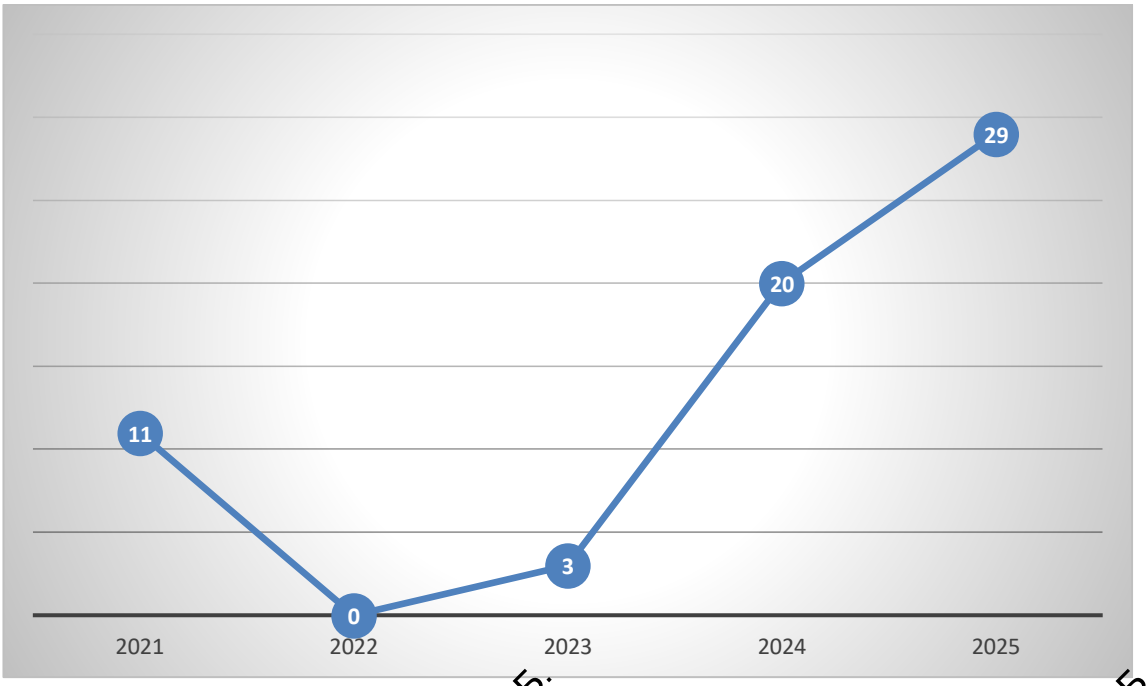

Рисунок 3 - Уголовные дела по правонарушениям в сфере

информатизации и связи, направленные в суд

Кроме того, следует указать на увеличение числа уголовных производств, по которым в указанный период были прерваны сроки досудебного расследования. Данный показатель характеризуется стабильным ростом: в 2021 году – 1 случай, 2022 – 4 случая, 2023 – 8 случаев, 2024 – 15 случаев, а в 2025 году – уже 25 таких случаев (рисунок 4). Подобная статистика дополнительно подтверждает наличие трудностей доказывания, обусловленных спецификой преступлений в области информационных технологий.

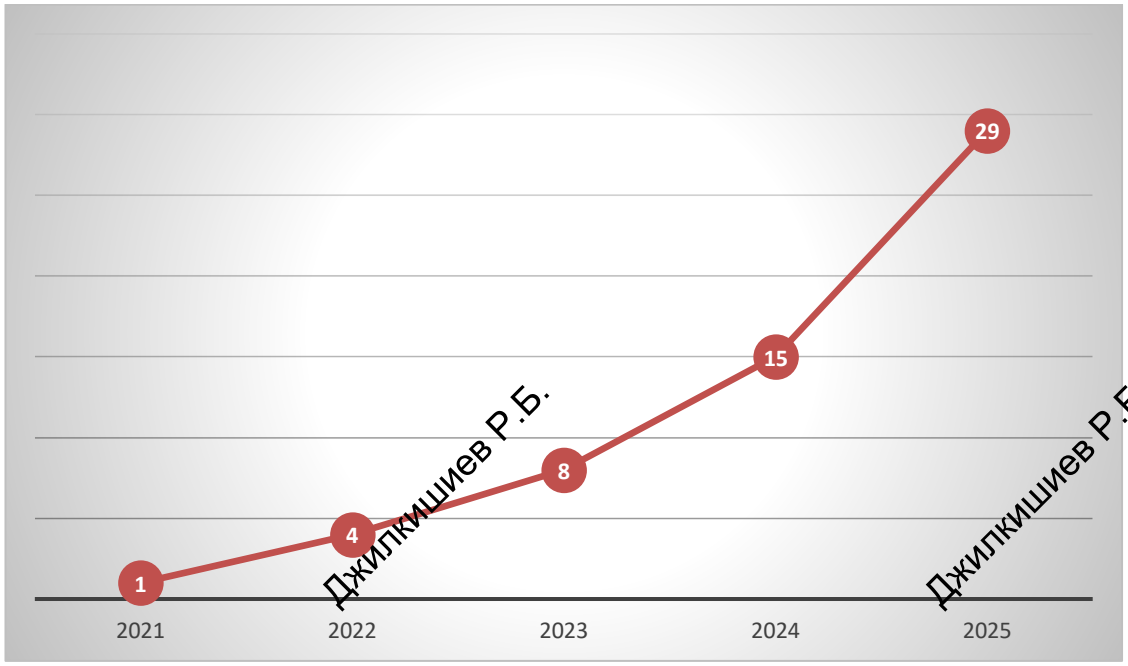

Рисунок 4 - Уголовные дела по правонарушениям в сфере информатизации и связи, по которым в указанный период были прерваны сроки досудебного расследования

Также необходимо учитывать и высокую степень латентности анализируемой категории преступлений, достигающую, по экспертным оценкам, порядка 95%. Указанное обстоятельство существенно осложняет адекватную оценку криминальной обстановки в сфере информационных технологий и требует разработки и внедрения эффективных методов выявления и расследования данных уголовных деяний.

Наряду с общими тенденциями роста преступлений в сфере информационных технологий особую тревогу вызывает стремительное распространение интернет-мошенничества, ставшего наиболее динамично развивающимся видом киберпреступлений в Казахстане за последние пять лет. С 2021 по 2025 год включительно официально зарегистрировано 53 368 уголовных правонарушений по фактам мошенничества с использованием интернет-технологий. Наибольшее количество таких преступлений зафиксировано в 2025 году – 12 390 случаев, минимальное – в 2023 году (9545). Данные за другие годы выглядят следующим образом: 2021 – 11 843, 2022 – 9654, 2024 – 9936 случая [1] (рисунок 5). Сравнивая текущие показатели с 2018

годом, следует отметить беспрецедентный рост интернет-мошенничества в 42 раза, почти на 98%, что подчеркивает масштаб и актуальность проблемы.

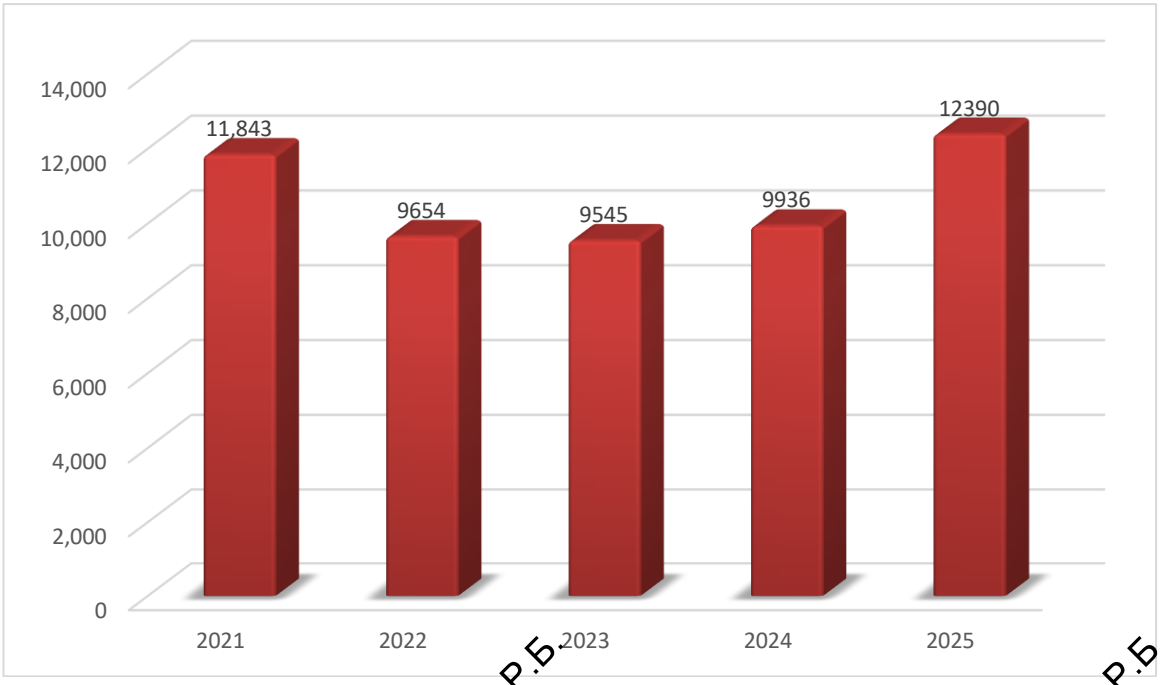

Рисунок 5 - Количество зарегистрированных в ЕРДР правонарушений в сфере интернет-мошенничества

Анализ обстоятельств и причин такого устойчивого роста преступлений данного вида указывает на то, что они тесно взаимосвязаны с интенсивностью цифровизации повседневной жизни казахстанцев, ростом числа пользователей онлайн-платформ, а также отсутствием у граждан достаточного уровня цифровой грамотности и навыков безопасного поведения в сети. Кроме того, по мнению специалистов, стремительное распространение интернет-мошенничества напрямую обусловлено как увеличением количества онлайн-транзакций, так и появлением новых методов обмана, таких как фишинг, социальная инженерия, мошенничество на платформах интернет-торговли и финансовых площадках.

Динамика уголовных дел по интернет-мошенничеству, находившихся в производстве правоохранительных органов, также характеризуется высокой интенсивностью. За отчетный период в общей сложности зафиксировано 63 282 таких дела. Наибольшее количество расследуемых уголовных производств приходится на 2025 год – 14 229, а наименьшее – на 2023 год (11 609). В 2021 году расследовалось 13 807 дел, в 2022 – 11 924, в 2024 – 11 713 [1] (рисунок 6). Очевидно, что правоохранительные органы на протяжении всех пяти лет были перегружены делами, связанными с интернет-мошенничеством, что свидетельствует о значительных трудностях в организации оперативно-розыскных мероприятий, проведении следственных действий и выявлении лиц, причастных к совершению данных преступлений.

Джилкишиев Р.Б.

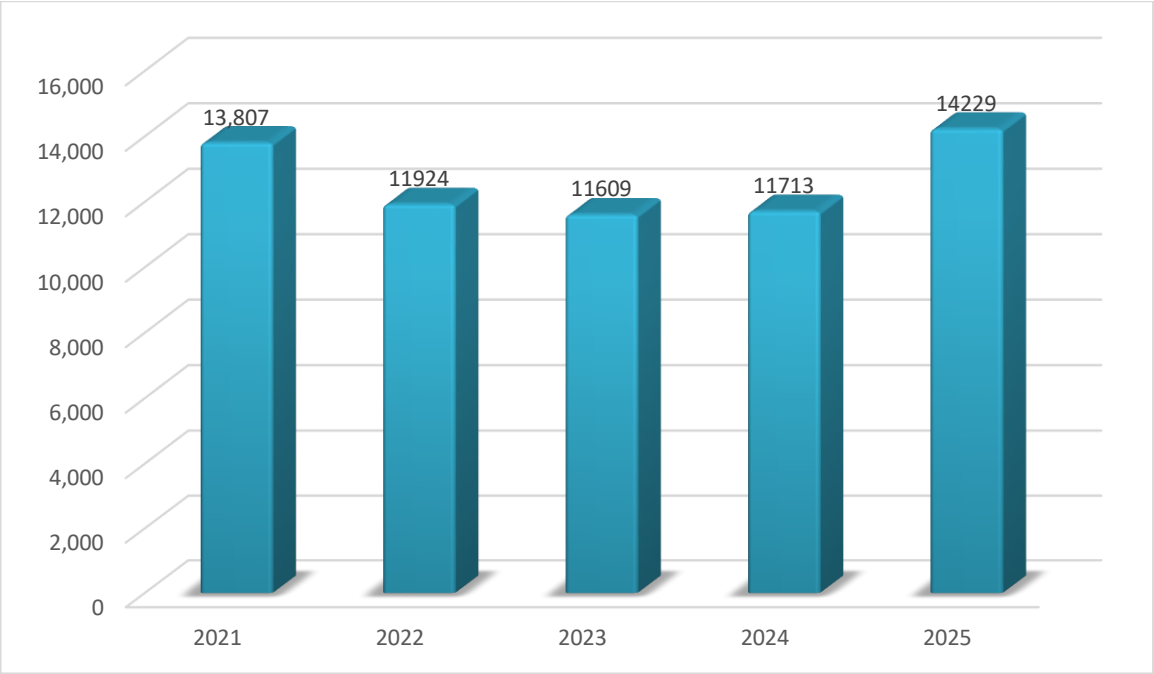

Рисунок 6 - Количество уголовных дел, находящихся в производстве по фактам интернет-мошенничества

Тем не менее, на фоне большого числа расследуемых уголовных дел, отмечается сравнительно низкий уровень передачи таких дел в суд. За весь рассматриваемый пятилетний период только 9307 уголовных дел по фактам интернет-мошенничества были направлены в судебные инстанции, при этом наибольшее количество – 2446 дел – передано в суд в 2025 году, а наименьшее – 1545 – в 2021 году (2022 – 1713, 2023 – 1771, 2024 – 1832) [1] (рисунок 7). Данная диспропорция сигнализирует о значительных сложностях в доказывании состава преступления, сборе цифровых доказательств и их надлежащем процессуальном закреплении, а также говорит о несовершенстве законодательного регулирования и нехватке квалифицированных специалистов по цифровой криминалистике.

Джилкишиев Р.Б.

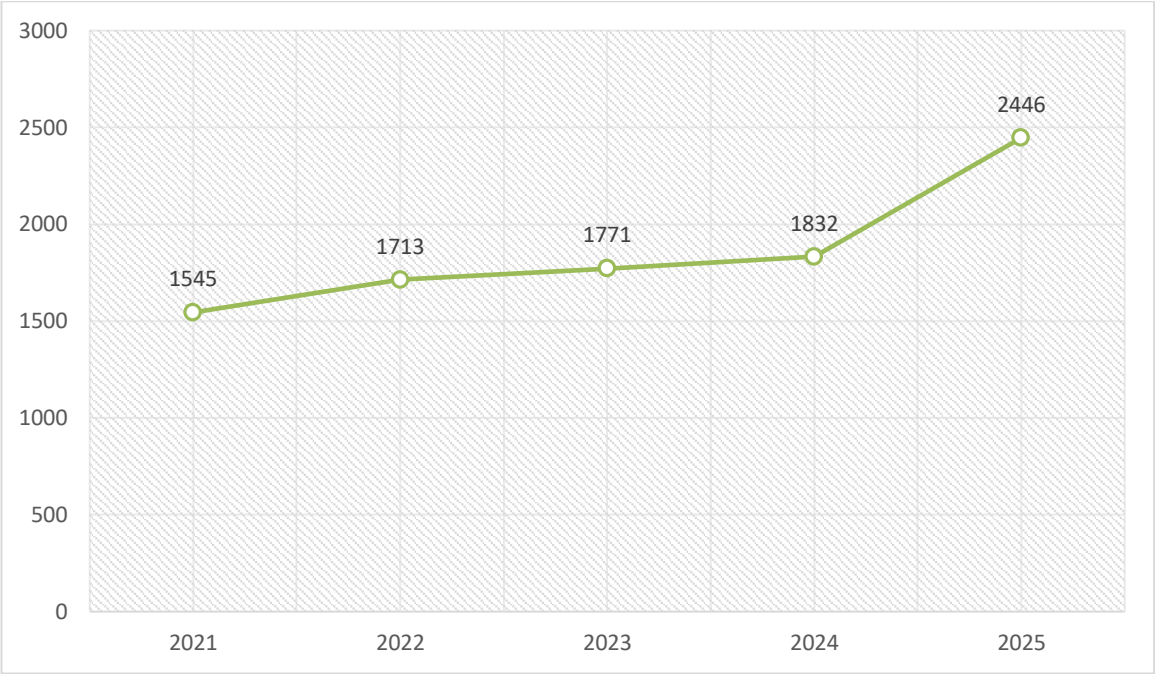

Рисунок 7 - Уголовные дела, направленные в суд по фактам интернет-мошенничества

Отдельно следует отметить тревожную тенденцию прерывания сроков досудебного расследования по уголовным делам данной категории. В общей сложности, за пять лет расследование было приостановлено по 31 332 фактам интернет-мошенничества. Ежегодные показатели выглядят следующим образом: 2021 – 7430, 2022 – 5779, 2023 – 6103, 2024 – 6238 и 2025 – 6782 [1] (рисунок 8).

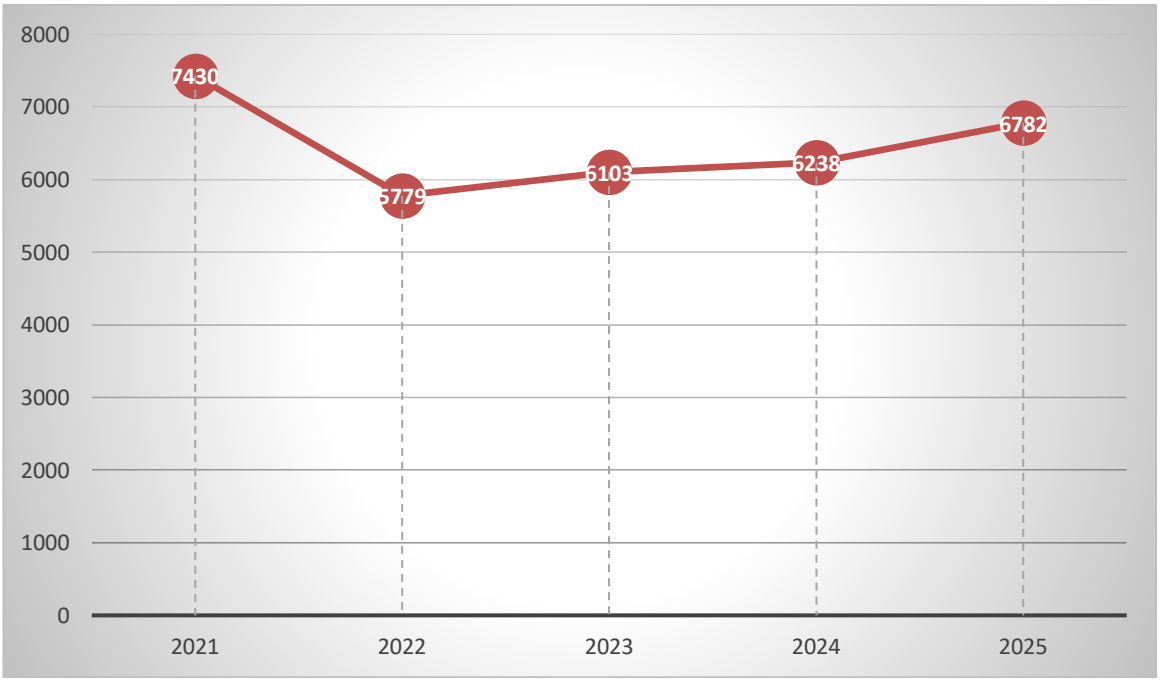

Рисунок 8 - Уголовные дела по фактам интернет-мошенничества, по которым в указанный период были прерваны сроки досудебного расследования

Такое обстоятельство указывает на системные проблемы, связанные с выявлением и идентификацией преступников, особенно в условиях анонимности интернет-пространства, применения технологий шифрования и удаленного совершения преступлений. Это создает серьезные преграды для полноценного завершения расследования и требует принятия новых подходов в правоохранительной практике и внедрения современных технических решений.

Таким образом, глубокий анализ представленных статистических данных демонстрирует серьёзные вызовы, с которыми сталкиваются правоохранительные органы Республики Казахстан в противодействии интернет-мошенничеству. Для изменения текущей ситуации необходимо принятие комплексных мер, включающих совершенствование законодательства, развитие цифровой криминалистики, повышение квалификации сотрудников правоохранительных органов и систематическое проведение профилактических мероприятий среди населения.

В настоящее время возникает объективная необходимость в совершенствовании форм, средств и методов деятельности правоохранительных органов. Назрел вопрос и о подготовке сотрудников, обладающих специфическими знаниями в области информационных технологий, способных противостоять противоправным явлениям в данной сфере.

Например, в структуре МВД РК при Департаменте криминальной полиции в 2019 году создан Центр по борьбе с киберпреступностью, к задачам которого относятся:

- организация и осуществление работы по предупреждению, пресечению, выявлению и раскрытию киберпреступлений, реализация государственной политики в сфере борьбы с киберпреступностью, в пределах своей компетенции. Обеспечение неотвратимости наказания за совершенные преступления;

- защита прав и законных интересов граждан, организаций и государства от преступных посягательств;

- международное сотрудничество;

- изучение, обобщение и внедрение в практику органов внутренних дел положительного отечественного и зарубежного опыта раскрытия киберпреступлений [15].

Агентство Республики Казахстан по финансовому мониторингу (далее – АФМ) осуществляет финансовый мониторинг и принимает иные меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, а также предупреждение, выявление, пресечение, раскрытие и расследование экономических и финансовых правонарушений, в том числе совершаемых в сети Интернет и связанные с криптоактивами.

Наряду с этим, одной из функций АФМ является реализация комплекса правовых, организационных и технических мероприятий, направленных на сохранность объектов информатизации, предотвращение неправомерного и

Джилкишиев Р.Б.

(или) непреднамеренного доступа и (или) воздействия на них в деятельности Агентства [16].

Правительством РК утверждена Концепция обеспечения общественной безопасности в партнерсе с обществом (далее — Концепция), где особое внимание уделено борьбе с киберпреступностью на период с 2024 по 2028 годы. В данной Концепции утверждены основы тактики работы по противодействию киберпреступлениям, основывающиеся на «доказательной аналитике» и «прогнозе рисков новых угроз», направленные на предотвращение потенциальных угроз. Для достижения поставленных задач, определенных Концепцией, планируется создание организации, в задачи которой будет входить управление киберрисками и координация усилий между различными участниками, в том числе органами правопорядка, государственными органами, финансовыми учреждениями и организациями, а также НПО [5].

Задачами Концепции определены:

- Присоединение Казахстана к Конвенции Совета Европы (далее – СЕ) в первой половине 2024 года с целью улучшения международного сотрудничества.
- Установление более тесного межгосударственного взаимодействия с целью выявления киберпреступлений, в том числе и новых, разработка превентивных мер (первое полугодие 2024 года).
- Разработка и принятие четких алгоритмов действий в рамках противодействия использованию информационных технологий в преступных целях (первое полугодие 2024 года).
- Создание цифровой коммуникации между банками и правоохранительными органами с целью минимизации бюрократических процессов и ускорения процесса расследования (период реализации — 2027-2028 годы).
- Развитие волонтерской деятельности, поддержка волонтерских инициатив в сфере противодействия киберпреступлениям (второе полугодие 2024 года).
- Предусмотрение ответственности в случае оформления банковских карт на одно лицо и передачи их третьим лицам для дальнейшего использования их в преступных целях (декабрь 2024 года).
- Обязательство финансовых организаций осуществлять проверку новых IT-услуг на соответствие нормам информационной безопасности (первое полугодие 2026 года).
- Обучение сотрудников правоохранительных органов на постоянной основе (не реже одного раза в полугодие) по вопросам противодействия киберпреступлениям с участием экспертов (период реализации — 2024-2028 годы).

Состояние в мире

Высокие технологии постоянно развиваются, активно внедряясь во все сфере жизнедеятельности человека, открывая новые возможности, но вместе с

Джилкишиев Р.Б.

тем, одновременно создавая новые риски. Глобализация привела к тому, что в любой точке планеты можно воспользоваться информацией и новыми технологиями. Это способствует быстрому обмену данными, но и дает возможность преступным элементам осуществлять противоправную деятельность в информационно-теллекоммуникационной сфере, находясь в любой стране, невзирая на территориальные ограничения. То есть киберпреступность имеет трансграничный характер, что делает поимку преступников и привлечение их к ответственности более сложной, а порой, невозможной.

Современные средства связи и технологии, ввиду простоты их использования, стали доступны не только профессионалам, но и рядовым пользователям. Действительно, на сегодняшний день практически любой человек, не обладающий специальными познаниями, но имеющий доступ к сети интернет, может воспользоваться данными технологиями, порой далеко не во благо общества. И чем больше число таких пользователей, тем больше и число совершаемых правонарушений.

Киберпреступность становится все более распространенной, стремительный процесс компьютеризации и быстрое внедрение технологий может опережать способность общества к их адаптации. Общество приходит к осознанию негативных последствий таких процессов: экономические проблемы (потеря рабочих мест в связи с автоматизацией рабочих процессов), политические риски (вмешательство в выборы), проблемы в социальной сфере (расслоение общества) и пр. Все вышеобозначенное подчеркивает актуальность рассматриваемого вопроса и риски растущей киберпреступности.

Можно констатировать тот факт, что большинство государств, столкнувшихся с киберпреступностью, были не готовы противостоять данному явлению, не имея эффективных инструментов борьбы ни на техническом и информационном уровнях, ни эффективной правовой базы. Киберпреступность оказала серьезные негативные последствия для экономики и общества: финансовые потери, репутационный ущерб, утечка информации и прочие проблемы, повлекшие потерю доверия к финансовым системам и институтам. Таким образом, борьба с рассматриваемым видом преступности — важнейшая часть обеспечения экономической и социальной стабильности, включающая разработку эффективных мер безопасности, законодательные инициативы, взаимодействие между частным сектором и государственными органами, а также межгосударственное сотрудничество.

Так, на на постоянной основе Генеральная Ассамблея ООН выступает в качестве платформы для обсуждения и выработки международных иинициатив, способствующих межстрановому диалогу, а также координации усилий по борьбе с киберпреступностью. Киберпреступность является глобальной проблемой, приобретающей все более широкие масштабы, и многие страны и организации во всем мире стремятся всеми силами остановить киберпреступников и добиться более надежной защиты систем.

Джилкишиев Р.Б.

Один из наиболее эффективных методов предупреждения такой преступности – это образование. В рамках инициативы «Образование во имя правосудия» (E4J) УНП ООН совместно с учеными и педагогами создало и разработало серию прошедших рецензирование университетских модулей и другие пособия с целью помочь ученым и педагогам в деле ознакомления учащихся с некоторыми наиболее актуальными угрозами.

Одна из серий таких модулей – это учебно-методическое пособие по противодействию киберпреступности, которое включает в себе темы и ресурсы, необходимые для всестороннего обучения по различным аспектам киберпреступности и расследования киберпреступлений. В них рассматриваются тенденции, теории, перспективы, законы, меры и практические методы, относящиеся к киберпреступности, в мультидисциплинарном контексте [17].

В Конвенции СЕ о киберпреступности, принятой в 2001 году, выделяется ряд преступлений, имеющих отношение к использованию информационных технологий. Данная Конвенция четко и логически структурирована, что помогает легко ориентироваться в различных типах киберпреступлений. Так, в ч. 1 гл. 2 все преступления сгруппированы, исходя из общего объекта нападения, т.е. преступления, имеющие схожие характеристики, объединены в одну категорию, что значительно упрощает их понимание. Каждый подраздел имеет подгруппы, исходя из конкретных признаков или аспектов преступления, что способствует более подробному рассмотрению характеристик различных видов преступлений, а также пониманию правоприменения и привлечения к ответственности. Согласно Конвенции СЕ, а также Протоколу № 1 к ней, датированным 2002-м годом, выделяются следующие группы преступлений:

1. Преступления против основополагающих принципов информационной безопасности (конфиденциальность, целостность, доступность данных): несанкционированное вхождение в системы или ее составные части, что является нарушением безопасности и конфиденциальности (ст. 2 Конвенции СЕ); перехват информации, предназначенной для общего пользования, что нарушает принцип конфиденциальности (ст. 3 Конвенции СЕ); осуществление определенных действий, результатом чего может быть повреждение, изменение или уничтожение данных, что нарушает принцип целостности (ст. 4 Конвенции СЕ); осуществление противоправных действий, воздействующих на функционирование системы.

2. Правонарушения, связанные с незаконным содержанием информации. Согласно ст. 9 Конвенции СЕ, к ним относится создание, распространение, пользование, предложение к распространению контента, содержащего детскую порнографию посредством сети интернет. Под детской порнографией понимаются материалы с изображением несовершеннолетних лиц (лица, не достигшие 18-летнего возраста), участвующих в откровенных сексуальных действиях. Однако страны могут самостоятельно устанавливать и более низкий

Джилкишиев Р.Б.

возрастной предел для привлечения к уголовной ответственности, исходя из норм действующего в данной стране уголовного законодательства.

3. Правонарушения, связанные с незаконным использованием защищенных авторским правом материалов (творческие работы как фильмы, музыка, ПО и прочий контент, распространение которого влечет нарушение прав интеллектуальной собственности).

4. Использование интернет-платформ с целью распространения ненависти, насилия, высказываний и действий дискриминирующего характера на основе расовых, этнических, религиозных различий (ненавистнические комментарии, создание групп, основная цель которых — пропаганда расизма и ксенофобии).

Каждое из перечисленных правонарушений несет серьезные угрозы и требует пристального внимания, как со стороны правительств, так и социума в целом. Эффективность борьбы с данным видом правонарушений зачастую зависит от скоординированности действий в рамках международного сотрудничества, разработки грамотных законодательных инициатив, а также высокого уровня осведомленности о возможных рисках и угрозах в пользовательской среде.

Преступления, совершаемые в киберпространстве, характеризуются высокой мобильностью, активной модификацией, способностью совершенствоваться по мере развития технологий. Поэтому и правовому сотрудничеству крайне важно идти в ногу со временем.

Нормы Конвенции СЕ касательно такого явления, как киберпреступность, нашли отражение в законодательстве многих стран, вобрав в себя множество положений, не вошедших в прочие нормативные правовые акты и договоры. Тем не менее, положения Конвенции распространяются лишь на страны, ратифицировавшие ее [18].

На сегодняшний момент из 195 государств в мире Конвенция СЕ ратифицирована лишь 47, включая 37 государств-членов Совета Европы.

Одним из сдерживающих факторов, на наш взгляд, является наличие ряда ограничений, несмотря на декларируемую открытость присоединения к ней. Так, государства, не входящие в Совет Европы, но желающие присоединиться к Конвенции СЕ, обязаны проходить обязательные консультации, а также необходимо получение единогласного решения всех государств-участников данной международной межправительственной организации.

Казахстан не является действующим членом Конвенции СЕ на сегодняшний день. Присоединение запланировано на второе полугодие текущего года в рамках Концепции обеспечения общественной безопасности в партнерстве с обществом на 2024-2028 годы.

В регулировании вопросов борьбы с правонарушениями в сфере киберпространства в рамках международного регулирования имеются следующие основные проблемы:

- различия в национальных законодательствах и практиках, выражающиеся в различных подходах к проблеме кибербезопасности;

Джилкишиев Р.Б.

- использование странами различных дефиниций для одного и того же вида киберпреступления, т.е. отсутствие унифицированного, действительного для всех, категорийного аппарата;

- отсутствие эффектиной координации, а также обмена информацией между органами правопорядка различных стран, ввиду отсутствия налаженных каналов;

- недостаточно развитый (неэффективный) уровень взаимодействия между частным бизнесом и государственными органами.

Это лишний раз подчеркивает необходимость организации сотрудничества на международном уровне, разработки согласованных и общепринятых норм, которые способствовали бы устранению правовых и технических барьеров, что, в конечном счете, приведет к более эффективному взаимодействию между странами и повышению общей безопасности в киберпространстве.

На уровне СНГ подписано «Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации» (Минск, 1 июня 2001 г.), утвержденное Указом Президента РК от 25 июня 2002 года № 897 [19].

В рамках данного нормативного правового акта под «преступлениями в сфере компьютерной информации» понимается уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация.

А под «компьютерной информацией» понимается информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию компьютером, или передающаяся по каналам связи.

Участники взяли обязательство признавать в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния, если они совершены умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, его системы или сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютера, компьютерной системы или сети лицом, имеющим доступ к компьютерам, компьютерной системе или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред или тяжкие последствия;

г) незаконное использование программ для компьютеров и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб [20].

Также подписан еще один документ под названием «Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» (Душанбе 28

сентября 2018 года), ратифицированное Законом Республики Казахстан от 9 декабря 2019 года № 277-VI ЗРК [21].

Согласно положениям данного Соглашения, страны-участники организуют совместную работу, целью которой является повышение безопасности в сфере информационных технологий и борьбы с киберпреступностью, что является важным шагом в обеспечении кибербезопасности как на региональном, так и на международном уровнях.

Концепция взаимодействия государств-участников СНГ в борьбе с преступностью стала первым документом, инициировавшим дальнейшее сотрудничество в рамках СНГ в данной сфере, а также основой для разработки и принятия других соглашений и документов.

Вывод. На основе проведенного анализа современного состояния противодействия киберпреступности в Республике Казахстан, а также мировой практики, можно сделать ряд фундаментальных выводов, отражающих текущие вызовы и перспективы данной сферы.

Анализ выявил, что за последние годы значительно увеличилось число зарегистрированных киберпреступлений, причем основную долю составляют интернет-мошенничества. В частности, статистика последних пяти лет демонстрирует постоянный рост правонарушений в области информационных технологий, а также свидетельствует о высоком уровне латентности подобных преступлений. Значительный объем преступлений остается нераскрытым, что связано как с техническими сложностями расследования, так и с пробелами в нормативно-правовой базе и недостаточной подготовленностью специалистов правоохранительных органов.

На основе исследования представляется очевидным, что существующая законодательная база Казахстана нуждается в дальнейшем совершенствовании и актуализации. Следует предусмотреть дополнительные нормы, регулирующие ответственность за специфические виды преступлений, такие как криптокражи, фишинг и интернет-шантаж. Важным аспектом является законодательное закрепление процедур быстрого реагирования и взаимодействия банковского и правоохранительного секторов, включая цифровые инструменты взаимодействия.

Результаты анализа также свидетельствуют о необходимости усиления международного сотрудничества в борьбе с киберпреступностью. Республика Казахстан стоит на пороге важного этапа — присоединения к Конвенции Совета Европы о киберпреступности, что позволит значительно улучшить международный обмен информацией и взаимодействие правоохранительных органов на глобальном уровне. Вместе с тем, целесообразно активизировать региональное сотрудничество в рамках СНГ, уделяя внимание унификации законодательства и процедур расследования.

На наш взгляд, необходимо разработать и принять в нашей стране новый закон «О противодействии киберпреступности» по аналогии с модельным законом «О противодействии киберпреступности», разработанным и утвержденным Межпарламентской Ассамблеей государств-участников СНГ

Джилкишиев Р.Б.

[22]. Необходимость данного закона в Казахстане вызвана стремительным ростом числа преступлений в цифровой сфере, которые представляют серьезную угрозу правам граждан, устойчивости экономики и национальной безопасности. Актуальность данного закона определяется не только увеличением общего количества киберпреступлений, их число за последние годы возросло более чем в 40 раз, но и низкой эффективностью их раскрываемости в рамках действующего законодательства, которое фрагментарно и не всегда соответствует международным стандартам и реалиям цифровой экономики.

Научная и практическая значимость предлагаемого закона заключается в том, что он впервые вводит единый правовой механизм противодействия киберпреступлениям, унифицирует терминологию и дает четкие правовые определения понятий «киберпространство» и «киберпреступление». В законе необходимо предусмотреть криминализацию новых составов преступлений, таких как компьютерное мошенничество, подделка цифровых данных и распространение вредоносного программного обеспечения, тем самым устраняя существующие правовые пробелы. Кроме того, он должен создать условия для эффективного международного сотрудничества в расследовании трансграничных преступлений в цифровой среде.

Важной особенностью нового закона является закрепление принципов системной профилактики и обеспечения кибербезопасности, что предполагает обязательные меры по мониторингу угроз, защите критической информационной инфраструктуры и повышению цифровой грамотности населения. Также закон должен усилить межведомственную координацию, определяя функции и взаимодействие правоохранительных органов, судебной системы и частного сектора в процессе выявления и расследования киберинцидентов.

Ожидаемый эффект от внедрения закона включает значительное повышение эффективности раскрываемости киберпреступлений, снижение уровня цифрового мошенничества, укрепление доверия граждан и бизнеса к электронным сервисам и цифровым технологиям, а также усиление защиты национальной безопасности от современных цифровых угроз. Принятие закона позволит Казахстану интегрироваться в международную систему борьбы с киберпреступностью и обеспечить надёжную правовую защиту в условиях цифровой трансформации общества.

Одной из главных рекомендаций, вытекающих из проведенного исследования, является необходимость постоянного и системного повышения квалификации сотрудников правоохранительных органов. Целесообразно создать специализированные образовательные программы на основе международного опыта, внедрять в учебный процесс технологии цифрового расследования, такие как искусственный интеллект и аналитические системы обработки больших данных. Дополнительно необходимо развивать специальные подразделения, оснащенные передовыми техническими

Джилкишиев Р.Б.

средствами, и формировать экспертные группы, занимающиеся разработкой и внедрением инновационных методов противодействия киберпреступности.

С учетом выявленных особенностей и тенденций необходимо активно развивать методы профилактики киберпреступлений, включая просветительскую работу с населением, волонтерскую деятельность и общественные инициативы, направленные на повышение уровня цифровой грамотности граждан.

Успешное противодействие праовнарушениям в сфере информации и связи, а также киберпреступности требует комплексного и многогранного подхода, которое содержит в себе регулярное обновление законодательства, внедрение новых и передовых технических решений, активизации международного и межведомственного взаимодействия, а также целенаправленную подготовку специалистов в области информационной безопасности. Указанные меры позволят эффективно реагировать на возникающие угрозы и снизить общий уровень преступности в киберпространстве, укрепляя тем самым безопасность и стабильность общества и государства в условиях стремительно развивающейся цифровой эпохи.

Джилкишиев Р.Б.

1.2 Уголовно-правовая характеристика правонарушений в сфере киберпреступности

В настоящее время стремительное развитие цифровых технологий и широкое распространение интернета существенно изменили характер и масштабы преступности, сформировав новую и чрезвычайно опасную категорию противоправных деяний — киберпреступления. Данные правонарушения отличаются не только высокой технической сложностью, но и специфическими способами совершения, которые зачастую выходят за рамки традиционных подходов к расследованию и квалификации преступлений.

Проведенный анализ уголовного законодательства Республики Казахстан выявляет, что хотя в действующем Уголовном кодексе страны предусмотрены статьи, направленные на противодействие основным видам киберпреступлений, таким как неправомерный доступ к информации, создание и распространение вредоносных программ, неправомерное завладение и модификация данных, значительная часть цифровых угроз и преступных деяний остается вне поля уголовно-правового регулирования. Это порождает проблемы правоприменения и усложняет задачи, стоящие перед правоохранительными органами и судами в части квалификации и расследования киберпреступлений.

Сложность правовой оценки данных преступлений усугубляется их трансграничным характером и технической спецификой, что требует не только совершенствования национального законодательства, но и активного взаимодействия на международном уровне, включая обмен опытом, методиками и технологиями выявления и расследования преступлений. В данном подразделе диссертации подробно рассматриваются правовые основы, классификации и составы киберпреступлений, дается характеристика основных правонарушений.

В действующем УК, в главе 7, содержатся нормы по неправомерному доступу и распространению информации ограниченного доступа.

В данной главе определены наиболее серьезные преступления, представляющие наибольшую угрозу безопасности и правопорядку в сфере информационных технологий и информационных систем и подпадающие под уголовное преследование. К ним относятся:

- неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК);
- неправомерное уничтожение или модификация информации (ст. 206 УК);
- нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК);
- неправомерное завладение информацией (ст. 208 УК);
- принуждение к передаче информации (ст. 209 УК);
- создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК);

Джилкишиев Р.Б.

- неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК);

- предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК);

- неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК).

Как следует из представленной информации, Уголовный кодекс охватывает лишь определенные виды киберпреступлений: вне правового поля остаются множество киберпреступлений, которые могут быть классифицированы в данной категории. Не все действия или преступления, которые могут рассматриваться как нарушения в сфере информатизации, попадают под действие уголовного законодательства, т.е. они могут быть расценены как административные правонарушения. Это вызывает огромные трудности как для следственных органов, так и для судов, так как определение классификации тех или иных действий с точки зрения уголовного права крайне затруднено. Законодательство не включает все существующие угрозы в цифровом пространстве, т.е. в настоящий момент мы можем говорить о проблеме правовой классификации киберпреступлений.

Законодателем определены конкретные действия, которые могут быть признаны преступными, представляющие реальную угрозу для общества в сфере безопасности информации и связи, и лишь эти действия подлежат уголовной ответственности.

Таким образом, хотя в Уголовном кодексе РК и содержится ряд статей, касающихся наказания за совершенные преступления в сфере кибербезопасности, не все аспекты защиты рассматриваемой области в полной мере разработаны и реализованы. Включение новых норм в действующий Уголовный кодекс не завершает процесс создания механизма защиты от киберпреступлений с высокой степенью эффективности. Это всего лишь первый шаг: на данный момент существует множество правовых вопросов, требующих решения с целью обеспечения адекватной защиты прав и свобод граждан в цифровом пространстве, без решения которых создание эффективной правовой системы, способной справляться с вызовами XXI века, не представляется возможным.

Криминальная статистика последних 10-15 лет показывает резкий всплеск числа хищений денежных средств. Как было указано выше, к основным преступлениям в сфере информационных технологий можно отнести создание, применение, распространение вредоносных программ, позволяющих наносить значительный вред компьютерам, осуществлять хищение данных и нарушать работу компьютерных систем; несанкционированный доступ к учетным записям пользователей посредством кражи (подбора) паролей; фишинг (один из видов мошенничества, целью которого является получение конфиденциальных данных по кредитным карточкам и банковским реквизитам); распространение

Джилкишиев Р.Б.

противоправной информации, контента, разжигающего ненависть между различными группами.

Последние десятилетия характеризуются быстрыми темпами развития информационных технологий во всем мире. Казахстан не является исключением. Сегодня нет ни одной отрасли, где бы не использовались цифровые технологии.

Однако благами такого развития могут воспользоваться и преступные элементы. Огромная сеть с базами данных, социальные сети не только значительно облегчают доступ к информации и коммуникациям, но и создают возможности использовать данные платформы для совершения противоправных деяний (мошенничество, кражи и пр.), которые могут быть сложными и непредсказуемыми, способными нанести значительный материальный и моральный ущерб. Так как преступные схемы все более и более усложняются и совершенствуются, законодателю необходимо адаптировать действующее законодательство под складывающиеся реалии, а правоохранительным органам необходимо развивать соответствующие навыки для раскрытия киберпреступлений.

Ученые сходятся во мнении, что для полного и эффективного рассмотрения вопроса о киберпреступности следует разграничить дефиниции «киберпреступление» и «компьютерное правонарушение». Понятие «киберпреступление» гораздо шире, поскольку киберпреступления совершаются не только лишь посредством использования компьютеров, но и других технических устройств и виртуального пространства. Компьютерные же преступления происходят непосредственно и только лишь с использованием компьютеров как средства совершения противоправного деяния или как средство посягательств, но не обязательно с использованием глобальных сетей. Киберпреступления могут совершаться не только в рамках интернета, т.е. охватывают широкий спектр преступных действий. Данный вид преступлений может затрагивать различные аспекты информационной инфраструктуры, при этом предметом преступного посягательства может быть как информация, технологические устройства и системы, а также непосредственные преступные действия, направленные против информации и ресурсов [23].

Таким образом, приходим к выводу, что под киберпреступлениями следует понимать умышленно совершаемые противоправные деяния в виртуальном пространстве посредством применения способов и средств телекоммуникаций. Необходимо отметить, что отсутствие общепринятых определений в значительной мере затрудняет правоприменение, чем активно пользуются преступники, используя различия в законодательстве разных стран, что позволяет порой беспрепятственно совершать противоправные деяния и избегать ответственности [24].

Согласно международной классификации, преступления подразделяются следующим образом: преступления против основных принципов информационной безопасности и преступления, совершаемые посредством использования компьютерных систем.

Джилкишиев Р.Б.

Такие преступления могут быть связанные с незаконным использованием защищенных авторским правом материалов (творческие работы, такие как фильмы, музыка, ПО и прочий контент, распространение которого влечет нарушение прав интеллектуальной собственности); использование интернет-платформ с целью распространения ненависти, насилия, высказываний и действий дискриминирующего характера на основе расовых, этнических, религиозных различий (ненавистнические комментарии, создание групп, основная цель которых — пропаганда расизма и ксенофобии).

В качестве инструментов, при помощи которых возможно совершение киберпреступлений, выступают вредоносное ПО, незаконно используемые домены, ботнеты, черные рынки. Понимание данных инструментов позволит ораганам правопорядка осуществлять разработку эффективных стратегий защиты и превентивных мер от киберугроз.

Одним из наиболее часто сообщаемом виде киберпреступления является мошенничество, в том числе сопряженное с кражей персональных данных (путем осуществления фишинга, методов социального инжиниринга), электронных платежных средств, осуществлением атак на онлайн-банкинг. Мошенничество также может включать в себя неправомерное использование номеров счетов, злоупотребление доверием с использованием массового маркетинга, сетевых пирамид, аукционов и прочих платформ. Следующими по частоте упоминания видами киберпреступлений являются: распространение с целью извлечения коммерческой выгоды незаконного контента, содержащего сцены насилия над несовершеннолетними, фальсификация медикаментов и средств медицинского назначения, незаконные азартные игры, незаконное использование защищенных авторским правом материалов, вымогательство, а также прочие правонарушения, целью которых является получение криминального дохода.

Киберпреступность представляет собой угрозу не только для отдельно взятых членов общества, но и национальной безопасности государства, где жизненно важные отрасли экономики достигли значительного уровня компьютеризации [25].

Борьба с данными видами противоправных деяний требует постоянного и планомерного развития, совершенствования на государственном уровне, а также бдительности и образованности частных лиц и специалистов с хорошей должностной подготовкой в организациях.

Классифицировать данные виды правонарушений с точки зрения экспертизы в области информационных технологий можно исходя из различных требований.

1. По области взаимодействия: Развитие интернет-связей позволяет мошенническим схемам взаимодействовать с объектом преступной деятельности, находясь на дистанционном расстоянии. Причем схемы преступной деятельности могут носить как бытовой характер: порча имущества из-за завирусованных программ, или мошеннические схемы по вымоганию средств, так и нести угрозу для жизни и здоровья человека.

Джилкишиев Р.Б.

Причем, если подобного рода операции происходят в локальных условиях Республики Казахстан, т.е. покрываются юрисдикцией страны, то возможно быстрое реагирование на подобное правонарушение; в противном случае необходимость решить эту проблему не всегда представляется возможным (вербовка в запрещенные на территории РК террористические организации)

Необходимо отметить, что для своевременного регулирования юридических вопросов на территории РК необходимо постоянное сотрудничество с международными организациями правопорядка как в области поиска и поимки преступных элементов, так и в законодательной области в целях приобретения опыта при столкновении с новыми преступными схемами.

2. По явности правонарушения: Открытые хакерские атаки, направленные вирусы, асоциальная пропаганда, причем преступные оранизации и синдикаты могут базироваться как на территории РК, так и иметь представителей в различных странах. Также преступная деятельность может иметь неявный характер: знакомство и общение в социальных сетях с целью вымогательства или мошенничества на доверии, вербовка в запрещенные организации (например в ИГИЛ или Исламское Государство), асоциальные игры (клубы самоубийц) и пр.

Если при явной угрозе принимаются соответствующие меры со стороны законодательных органов РК, как в области аполитических тенденций, контролю над безопасностью информации в действиях государственных организаций и др., а также в больших корпоративных организациях существуют отделы по разработке и сопровождению безопасной работы IT структур, то при неявной угрозе реагирование на подобные криминальные взаимодействия с потенциальными жертвами очень затруднено, а часто просто нереально.

3. По сложности исполнения: Когда объектом преступной деятельности является возможность доступа к крупным материальным средствам банка или другой крупной организации, или проникновение и угроза нанесения вреда на опасном предприятии велика своими последствиями, как правило, преступник или группа лиц с преступным умыслом, сталкиваются с определенными методами защиты. В данном случае схема нанесения ущерба представляется вполне сложной, опирается на различные виды информации и требует высокой профессиональной подготовки; В более простых случаях преступнику нет необходимости обладать высоким уровнем подготовки.

Специфика правонарушений и выявления, отслеживания данного рода правонарушений вынуждает в качестве экспертов привлекать высококвалифицированных специалистов из области IT-технологий, которые смогли бы точно и явно определить не только точки локации правонарушения, но и юридически обосновать и доказать методы преступной деятельности, а также установить потенциальный и явный урон, нанесенный лицами, действующими с преступным умыслом.

Для более детального анализа правонарушений и, как следствие, особенностей, требуемых от специалистов, работающих в области экспертизы

Джилкишиев Р.Б.

правонарушений в киберпространстве, необходимо систематизировать специфику правонарушений. Для этого необходима определенная схема по распределению правонарушений.

Вместе с тем существуют определенные сложности правоприменения в сфере киберпреступлений, так как данная категория противоправных деяний, совершаясь через интернет-среду, затрагивает несколько юрисдикций. То есть преступление может совершаться в одной стране, но затрагивать интересы жертв в другой. Законодательство данных стран в области кибербезопасности может кардинально отличаться, что приводит к разночтению норм и интерпретации законов. Кроме того, могут возникать и сложности в сборе доказательной базы, так как доказательства находятся на серверах, расположенных в разных государствах.

Таким образом, эффективное расследование киберпреступлений требует международного сотрудничества с соблюдением всех соответствующих правовых процедур. Состояние информационной безопасности в Казахстане на данный момент, к сожалению, указывает на то, что системы защиты информации и меры, предпринимаемые по ее защите, находятся не на должном уровне и не удовлетворяют потребностям как отдельно взятого лица, так и государства в целом.

Нельзя не отметить, что с появлением первых технологий в области телекоммуникаций, возникло и развилось множество исследований, в том числе и законодательного характера. За последние десятилетия в вопросах безопасности киберпространства можно отметить большое количество исследователей.

В проведении данной работы нельзя не отметить анализ и исследования специалистов относительно угроз информационной безопасности, их содержания и основных характеристик. Серьезный вклад в их развитие отражен в работах: Аманова Ж.К., Алауханова Е.О., Агыбаева А.Н., Бегалиева К.А., Бекназарова Б.А., Вехова В.Б., Джансараевой Р.Е., Исаева А.А., Крылова В.В., Каиржанова Е.И., Лоскутова И.Ю., Мещерякова В.А., Рогозина В.Ю., Рогова И.И., Рахметова С.М., Соловьева Л.Н., Сеитова Т.Б., Толеубековой Б.Х. и др.

В анализе управления сетью Интернет с целью достижения максимально эффективной безопасности в данном исследовании были изучены работы следующих российских и зарубежных ученых: Гелбстайна Э., Голдсмита Дж., Зиновьевой Е.С., Кнейка Р., Кукьера К., Курбалия Й., Лонга Д., Малколма Дж., Мансела Р., Матиасона Дж., Мюлера М., Пескова Д.Н., Серфа В.

Основным объектом уголовных преступлений в сфере кибербезопасности выступают отношения, непосредственно связанные с информацией, а именно обеспечением ее конфиденциальности (защита от несанкционированного доступа), целостности (сохранение в неизменном виде) и доступности (доступ имеют лишь авторизированные пользователи). Данная информация может находиться на физических носителях, в системах хранения данных, либо в процессе передачи по сети интернет.

Джилкишиев Р.Б.

Неудовлетворительно организована защита персональных данных, налоговой, таможенной, имущественной и другой информации.

Вместе с тем статус электронных информационных ресурсов, содержащих персональные данные, определен в Законе Республики Казахстан от 24 ноября 2015 года №418-V «Об информатизации».

Согласно п.2) ст.1 указанного Закона, информатизация – это организационный, социально-экономический и научно-технический процесс, направленный на автоматизацию деятельности субъектов информатизации.

Кроме того, под субъектами информатизации понимаются государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации [26].

В соответствии с п.10) ст.2 Закона Республики Казахстан от 5 июля 2004 года №567-II «О связи», «связь – прием, сбор, обработка, накопление, передача (перевозка), доставка, распространение информации, почтовых и специальных отправлений, почтовых переводов денег» [27].

Закон Республики Казахстан от 21 мая 2013 года №94-V «О персональных данных и их защите» регулирует общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных [28].

Как следует из вышеперечисленных составов преступлений, их последствия непосредственно затрагивают права и интересы как физических, так и юридических лиц.

УК РК в рамках п. 14) ст. 3 данные последствия классифицирует как «существенный вред», т.е. имеющие серьезное значение и влекущие за собой уголовную ответственность. К видам последствий, подпадающих под определение существенного вреда, относятся: посягательства на основные права и свободы людей, такие как право на личную жизнь, свободу слова и пр., т.е. нарушение конституционных прав и свобод человека и гражданина; нарушение прав и законных интересов юридических лиц, ведущих к финансовым потерям или (и) репутационному ущербу; нарушение интересов общества и государства; значительные материальные потери, вызванные правонарушениями; социальные потери, т.е. возникновение трудной жизненной ситуации у лица, которому причинен ущерб; сбои в работе государственных органов и учреждений; снижение обороноспособности страны (кратковременное снижение уровня боевой готовности), выражающееся в срыве важных воинских мероприятий; несвоевременное обнаружение или отражение нападения вооруженных групп или отдельных вооруженных лиц; незаконная миграция, контрабанда и прочие действия, как результат беспрепятственного и незаконного перехода через государственную границу; прочие последствия, которые могут быть признаны существенными [29].

Для правильной квалификации преступного деяния необходимо брать во внимание психическое состояние преступника, его намерения. Все преступления, указанные в гл. 7 УК РК, предполагают умышленную форму

Джилкишиев Р.Б.

вины, т.е. лицо, совершившее правонарушение, в полной мере осознавало совершаемые им незаконные действия, и также имело намеренное желание их совершить. В некоторых случаях преступления могут рассматриваться как особый квалифицированный вид неправомерного доступа к информации посредством использования информационной системы или информационно-коммуникационной сети. Согласно нормам ч. 3 ст. 205 УК РК, данный вид может быть совершен с двойной формой вины — умышленной и неосторожной [30].

Уголовная ответственность для лиц, совершивших противоправные деяния, предусмотренные главой 7 УК РК, наступает с 16 лет.

К более серьезным формам преступлений, имеющим дополнительные признаки, отягчающие данные противоправные деяния (квалифицированные и особо квалифицированные виды правонарушений), относятся:

- с использованием или воздействием на электронные системы или данные;
- направленные на несанкционированное получение критически важной информации, обладание которой может повлиять на безопасность и жизнедеятельность общества;
- в отношении объектов, имеющих важное значение для функционирования информационных систем;
- заранее спланированные, совершенные группой лиц;
- спланированные и совершенные организованной преступной группой;
- совершенные с применением физической силы;
- совершенные должностным лицом при исполнении;
- совершенные с целью получения материальной выгоды;
- повлекшие тяжкие последствия.

Давайте рассмотрим классификацию электронных информационных ресурсов в контексте законодательства Республики Казахстан, а именно ст. 32 Закона «Об информатизации». Согласно данной статье, под государственными ресурсами понимаются ресурсы, приобретаемые и накапливаемые за счет бюджетных средств и (или) полученные государственными органами прочими легальными способами. Негосударственные ресурсы — ресурсы, создаваемые или (и) приобретаемые за счет коммерческих компаний, граждан, физических и юридических лиц. Общедоступность определяется условиями доступа. Ресурсы, предоставляемые или распространяемые собственниками без каких-либо специальных условий или требований, относятся к общедоступным. Ресурсы ограниченного доступа — ресурсы, содержащие данные, доступ к которым ограничен законодателем или собственником.

В соответствии с п.12) ст. 1 Закона Республики Казахстан «Об информатизации», информационная система — это структурированное объединение множества компонентов, работающих как единое целое, выполняющих определенные технологические действия в рамках осуществления информационного взаимодействия. В качестве подобных

Джилкишиев Р.Б.

компонентов могут выступать информационно-коммуникационные технологии, программное и аппаратное обеспечение, техническая документация, а также персонал, отвечающий за обслуживание и управление данной системой.

Также они бывают государственными и негосударственными, общедоступными и ограниченного доступа.

В соответствии со ст. 37 ЗРК «Об информатизации», информационные системы, создаваемые или развиваемые за счет бюджетных средств, а также полученные государственными юридическими лицами иными способами, установленными законами Республики Казахстан, являются государственными. Негосударственными являются системы, создаваемые или развиваемые за счет средств физических и юридических лиц, а также полученные ими иными способами, установленными законами Республики Казахстан. Общедоступные системы содержат общедоступные электронные информационные ресурсы, а системы ограниченного доступа содержат электронные информационные ресурсы ограниченного доступа [26].

В соответствии с п.1) ст.1 «О доступе к информации», «информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированных в любой форме» [31].

Под критически важными объектами информационно-коммуникационной инфраструктуры понимаются объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электро-, газо-, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, «электронного правительства».

В свою очередь, объекты информационно-коммуникационной инфраструктуры – это информационные системы, технологические платформы, аппаратно-программные комплексы, серверные помещения (центры обработки данных), сети телекоммуникаций, а также системы обеспечения информационной безопасности и бесперебойного функционирования технических средств [26].

В соответствии с п. 55) ст. 1 Закона РК «О связи», под сетями телекоммуникаций понимается совокупность множества физических компонентов (кабели, линейно-кабельные сооружения, абонентские линии) и электронных устройств (маршрутизаторы, станции, подстанции, концентраторы), а также технологий, посредством которых осуществляется передача информации и организация сообщений между пользователями и системой [27].

Джилкишиев Р.Б.

В качестве отягчающих обстоятельств совершения рассматриваемого вида правонарушений следует признавать нарушение работы промышленных и сельскохозяйственных предприятий; сбои в деятельности жилищно-коммунального хозяйства, работе транспортных систем; дезорганизацию систем и объектов жизнеобеспечения, обеспечивающих жизнедеятельность населения; угрозу национальной безопасности, угрозы техногенного характера, природных бедствий, катаклизмов, которые могут привести к потере значительных ресурсов и разрушениям; нанесение травм или гибель людей; нанесение ущерба в крупном и особо крупном размере.

В соответствии с УК РК, в частности, главой 7, классификация уголовных правонарушений, совершаемых в рассматриваемой области, выглядит следующим образом:

а) статьи 205-211 УК РК: преступления, затрагивающие информационную защиту данных, хранящихся на электронных носителях, в информационных системах, а также передаваемой посредством телекоммуникационных сетей (уничтожение, изменение и прочие действия, несущие угрозу безопасности данных);

б) статьи 212, 213 УК РК: иные виды противоправных деяний, напрямую не касающиеся защиты информации, но с использованием информационных технологий и систем связи, нарушающие закон в контексте информатизации.

Ст. 205 УК РК «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций». Основание для квалификации — наличие конкретных последствий и результатов совершения противоправных деяний (материальный состав); преступление совершено умышленно, с осознанием нарушения закона; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 206 «Неправомерное уничтожение или модификация информации». Основание для квалификации — фактическое уничтожение, повреждение или изменение информации, наступление реальных последствий в виде утраты, изменения данных или их содержания; преступление совершено умышленно, с осознанием нарушения закона; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 207 УК РК «Нарушение работы информационной системы или сетей телекоммуникаций». Основание для квалификации — наличие конкретных последствий и результатов совершения противоправных деяний (материальный состав); преступление совершено умышленно, с осознанием нарушения закона; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 208 УК РК «Неправомерное завладение информацией». Основание для квалификации — наличие конкретных последствий и результатов совершения противоправных деяний (материальный состав); преступление совершено умышленно, с осознанием нарушения закона; под уголовную

Джилкишиев Р.Б.

ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 209 УК РК «Принуждение к передаче информации». Основание для квалификации — наличие факта принуждения, вне зависимости от факта передачи (формальный состав); преступление совершено с прямым умыслом принудить другое лицо к передаче информации и намеренным использованием методов для достижения данной цели; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 210 УК РК «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов». Основание для квалификации — наличие факта создания, использования или распространения вредоносного ПО, вне зависимости от наступления последствий; преступление совершено с прямым умыслом или намерением создать, использовать или распространить вредоносное ПО с целью причинения вреда; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 211 УК РК «Неправомерное распространение электронных информационных ресурсов ограниченного доступа». Основание для квалификации — наличие факта неправомерного распространения информации, вне зависимости от факта ее дальнейшего использования (формальный состав); преступление совершено умышленно, с осознанием нарушения закона; под уголовную ответственность подпадают лица, которым на момент совершения преступления исполнилось полных 16 лет.

Ст. 212 УК РК «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели». Основание для квалификации — наличие факта намеренного предоставления данного вида услуг, осознавая противоправность целей их оказания; к ответственности могут быть привлечены только определенные лица: собственник или владелец аппаратно-программных комплексов, открыто функционирующих в телекоммуникационной сети, контролирующие инфраструктуру, дающую возможность распространения подобных ресурсов.

Ст. 213 УК РК «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства»; состав – формальный, с субъективной стороны характеризуется умышленной формой вины, субъект – лицо, достигшее 16-летнего возраста.

Общественная опасность уголовных правонарушений в сфере информатизации и связи определяется высокой значимостью технологий электронно-вычислительных систем в экономической деятельности общества, в результате чего причиняется значительный ущерб организациям или отдельным гражданам либо государству в целом.

Джилкишиев Р.Б.

Общим объектом указанных уголовных правонарушений являются права на информацию ее владельца и третьих лиц.

По мнению ученых, «объектом рассматриваемых преступлений являются общественные отношения в сфере:

- обеспечения конфиденциальности, целостности и доступности компьютерной информации;
- сохранности и неприкосновенности средств хранения, обработки и передачи такой информации.

В качестве предмета выступают:

- компьютерная информация;
- средства хранения, обработки или передачи компьютерной информации;
- информационно-телекоммуникационные сети;
- оконечное оборудование» [32].

По мнению Курбатовой М.С., «облачные сервисы хранения данных могут являться объектом преступного посягательства. Опасность использования таких сервисов обуславливается в утечке информации. В случае неправомерного доступа к каким-либо данным организации имеется риск утери конфиденциальной информации» [33, с. 117].

Ученые едины во мнении, что «в главе 6 УК РК (Уголовные правонарушения против собственности) указаны деяния, предусмотренные ст.190 ч.2 п.4 УК РК, а именно «мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием», совершенное «путем обмана или злоупотребления доверием пользователя информационной системы» и ст.188 ч.2 п.4 УК РК – «кража, то есть тайное хищение чужого имущества, совершенное «путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций».

При этом, в ряде статей УК РК *(147 – «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите»; 148 – «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»; 159 – «Незаконное ограничение права на доступ к информационным ресурсам»; 161 – «Пропаганда или публичные призывы к развязыванию агрессивной войны»; 174 – «Возбуждение социальной, национальной, родовой, расовой, сословной или религиозной розни»; 179 - «Пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя Республики Казахстан»; 180 - «Сепаратистская деятельность»; 188 – «Кража»; 190 – «Мошенничество»; 256 – «Пропаганда терроризма или публичные призывы к совершению акта терроризма и другие»)* также содержатся квалифицирующие признаки, где высокие технологии выступают в роли объекта, орудия преступления или способа совершения незаконного деяния» [34, с.44].

Объективная сторона уголовных противоправных деяний в сфере информатизации и связи показывает, что преступления могут проявляться как в

активных действиях (ст. ст. 205, 206, 208-213 УК РК), так и в бездействии (ст. 207 УК РК).

По мнению С.А. Яшкова, «объективная сторона состава анализируемого преступления – неправомерный доступ – может быть представлена, с одной стороны, как действие, а, с другой, – как определенный результат этих действий – состояние. Если виновный занимается непосредственно доступом к компьютерной информации, например, подбирает пароль или пытается «взломать» систему защиты, то указанные в законе последствия могут наступить» [35, с. 31].

В целом, правонарушения основываются на наличии материальных (реальные последствия) (ст.ст. 205, 206, 208 УК РК) и формальных (наличие непосредственного факта нарушения) составов (ч.ч. 1, 2 ст.ст. 207, 209-213 УК РК).

В настоящее время существуют различные точки зрения относительно понятия киберпреступлений, поглощая в себе и уголовные правонарушения в сфере информатизации и связи. Проблема точного определения этого понятия заключается в том, что практически невозможно выделить единый объект и предмет посягательства. Потому что стремительное развитие информационно-телекоммуникационных технологий, виртуальных цифровых отношений порождает абсолютно новые объекты циркуляции цифровой информации, персональных данных.

Субъективная сторона уголовных правонарушений в сфере информатизации может характеризоваться прямым умыслом и целью. То есть преступник отдает отчет, что его действия могут привести к нарушению закона и имеют опасный характер, но он намеренно идет на совершение преступления. Цель преступления может быть как корыстной, направленной на получение материальной или иной выгоды, либо иметь иные мотивы (месть, желание нанесения вреда и пр.). Это крайне важно для определения квалификации противоправного деяния и назначения наказания.

В качестве субъекта выступает лицо, которому на момент совершения противоправного деяния исполнилось полных 16 лет, а также *специальный* статус (собственник или владелец аппаратно-программных комплексов, функционирующих в сети телекоммуникаций).

Итоги проведенного анализа подраздела «Уголовно-правовая характеристика правонарушений в сфере киберпреступности» позволяют утверждать, что на сегодняшний день уголовное законодательство Республики Казахстан обеспечивает лишь частичное покрытие тех угроз и вызовов, которые связаны с развитием информационных технологий. Рассмотренные составы преступлений, указанные в главе 7 УК РК, отражают наиболее типичные и серьезные виды противоправных действий, однако остаются без надлежащего внимания многочисленные случаи правонарушений в сфере цифровой безопасности, которые по формальным причинам не подпадают под критерии уголовного законодательства и квалифицируются как

Джилкишиев Р.Б.

административные правонарушения или вовсе остаются вне поля зрения правоохранительных органов.

К числу наиболее серьезных недостатков следует отнести отсутствие комплексного подхода к классификации и правовой оценке киберпреступлений. Преступления в киберпространстве характеризуются высокой технической сложностью и трансграничным характером, что значительно осложняет их квалификацию, расследование и привлечение виновных к ответственности. В этой связи предлагается конкретизировать и расширить перечень признаков и форм уголовно-наказуемых деяний, связанных с неправомерным доступом, хищением данных, мошенничеством и распространением вредоносного контента.

В ходе анализа было выявлено, что существующее законодательство Республики Казахстан в недостаточной степени учитывает быстро развивающиеся методы и технологии совершения преступлений. Преступники активно используют новейшие программные и аппаратные средства, что значительно усложняет деятельность правоохранительных органов по предотвращению, выявлению и расследованию подобных преступлений. Очевидна необходимость постоянного мониторинга и оперативного обновления законодательных норм, включая введение новых квалифицирующих признаков и уточнение формулировок уголовных составов, адаптированных под цифровые реалии.

На основании глубокого анализа отечественной и зарубежной практики, а также с учетом опыта правоприменения, предлагается внести следующие авторские изменения и дополнения в Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 19.05.2025 г.)

А) В ст. 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций» добавить пункт 4) и внести дополнение, изложив его в следующей редакции:

«Те же действия, совершенные с использованием технологий искусственного интеллекта или с применением специальных программных средств, позволяющих осуществлять массовый автоматизированный подбор паролей или обход систем идентификации и защиты информации, -

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет».

Рост использования технологий ИИ в киберпреступности требует выделения этого признака в отдельный квалифицирующий пункт. Данное нововведение позволит обеспечить дифференцированный подход к преступлениям, совершаемым с использованием передовых технологий, и усилить профилактическое воздействие уголовного закона.

Б) Добавить **ст. 213-1 «Незаконное использование цифровых персональных данных»,** далее добавить нижеследующие части с авторским

Джилкишиев Р.Б.

изложением в следующей редакции: **«1. Сбор, хранение, распространение или незаконное использование цифровых персональных данных без согласия лица, если эти действия повлекли значительный ущерб, -**

наказываются штрафом в размере до двух тысяч месячных расчетных показателей или исправительными работами на срок до двух лет.

2. Те же действия, совершенные группой лиц по предварительному сговору, либо с использованием служебного положения, либо повлекшие тяжкие последствия, -

наказываются лишением свободы на срок до пяти лет с лишением права занимать определенные должности на срок до трех лет».

Предлагаемое нововведение обусловлено необходимостью защиты цифровой приватности граждан в условиях широкого распространения цифровых платформ. Предлагаемая статья призвана урегулировать актуальные общественные отношения и обеспечить защиту фундаментальных прав человека в цифровом пространстве.

В) В ст. 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» добавить часть 4 новым квалифицирующим признаком и внести дополнение, изложив его в следующей редакции:

«Деяния, предусмотренные частями первой-третьей настоящей статьи, совершенные с целью дестабилизации работы объектов критической информационной инфраструктуры, -

наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества или без таковой».

Усиление ответственности обусловлено повышением общественной опасности атак на критически важные информационные системы, чья стабильная работа является основой национальной безопасности и экономики.

Г) Добавить **ст. 212-1 «Цифровое мошенничество»,** далее внести дополнение в виде нижеследующих частей с авторским изложением в следующей редакции:

«1. Мошенничество с использованием информационных технологий, включая обман или злоупотребление доверием пользователей интернета, цифровых платформ, систем электронных платежей, -

наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо ограничением или лишением свободы на срок до четырех лет.

7. Те же деяния, совершенные организованной группой, либо причинившие особо крупный ущерб, наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества».

Исключить п. 4) путем обмана или злоупотребления доверием пользователя информационной системы, в ст.190 Мошенничество, ч. 2. Мошенничество, совершенное.

Джилкишиев Р.Б.

Предложение обусловлено увеличением числа случаев мошенничества с применением цифровых технологий и потребностью в четком законодательном регулировании ответственности за указанные деяния.

Д) В ст. 53 «Обстоятельства, смягчающие уголовную ответственность и наказание» Общей части УК добавить пункт 12) и внести дополнение, изложив его в следующей редакции: **активное содействие расследованию преступлений в сфере информационных технологий, повлекшее раскрытие преступления, возмещение причиненного ущерба или предотвращение дальнейших негативных последствий.**

Предлагаемая мера направлена на стимулирование сотрудничества обвиняемых или подсудимых с правоохранительными органами, что позволит значительно повысить эффективность борьбы с киберпреступностью.

Таким образом, предложенные авторские изменения в Уголовный кодекс РК и дополнения призваны существенно повысить эффективность правоприменительной практики Республики Казахстан в области противодействия киберугрозам, усилить защиту прав и законных интересов граждан и организаций, а также обеспечить стабильность национальной информационной безопасности страны.

Джилкишиев Р.Б.

1.3 Содержание элементов криминалистической характеристики правонарушений в сфере информационных технологий и киберпреступности

Развитие технологий, изменение социально-экономических условий в современных реалиях неизбежно вызвало также и появление новых видов противоправных деяний, таких как киберпреступления. Данные вид преступлений, ввиду сложности схем, методов их совершения, требует специфических знаний и навыков для их расследования, поскольку традиционные методы, как правило, оказываются неэффективными. Таким образом, в условиях новых форм преступности необходимо разрабатывать специальные методики, учитывающие специфику современных видов правонарушений, разработка которых должна основываться на междисциплинарном подходе, а также использовании технологий.

С целью эффективной работы по данным правонарушениям полицейским, проводящие расследование, необходимо на постоянной основе совершенствовать свои умения, навики и знания. К числу источников профессиональных следственных знаний относятся частные методики расследования правонарушений и их криминалистические характеристики [36].

В основе создания частных методик расследования лежат выделенные компоненты: механизм следообразования и другие элементы криминалистической характеристики определенного вида правонарушений, а также следственные ситуации разной степени общности, возникновение которых возможно на различных этапах их расследования. Применительно к каждому отдельному виду преступлений они наполняются конкретным содержанием и соответствующим образом углубляются и дифференцируются [37, с. 193].

Мы используем компьютерные технологии и услуги на постоянной основе. Они значительно облегчают нашу жизнь, однако создают и новые риски. На сегодняшний множество преступлений совершаются с использованием компьютерной техники. Данные обстоятельства позволяют предположить, что неправомерный доступ к компьютерной информации можно рассматривать в качестве метода (например, хакерская атака), средства (компьютер, глобальная сеть) и предмета преступления (похищенные данные).

Помимо обладания знаниями в определенных направлениях криминалистики следователи обязаны понимать, какую социальную ценность они несут и насколько они важны для практической деятельности.

Криминалистическая техника должна позволять решать познавательные задачи в расследовании, что требует от него наличия практических навыков, обладания аналитическим типом мышления и способности к критическому анализу.

Из этого следует, что действующее законодательство требует обновления и разработки новых частных методик ввиду наличия многообразия уголовных правонарушений [38, с. 102].

Джилкишиев Р.Б.

Нельзя не признать тот факт, что в последнее время создано достаточное количество методических разработок по отдельным видам противоправных деяний. Тем не менее, преступность имеет тенденцию постоянно эволюционировать, примером тому может служить появление киберпреступности, организованной преступности и пр., что требует разработки новых методик расследования, соответствующих актуальным вызовам. В современных реалиях многие традиционные методы расследования преступлений устарели и неэффективны. Здесь важно не только разработать новые подходы, но и адаптировать уже существующие методики к современным условиям. Как отмечено Нукеновым М.О., одним из ключевых направлений криминалистики является нахождение новых методов выявления и доказывания организованной преступной деятельности, позволяющей следователям своевременно выявлять закономерности и связи между различными противоправными деяниями [39, с. 228].

Интеграция современных технологий в процесс расследования преступлений может значительно повысить уровень эффективности их расследования, выявив определенные закономерности, упущенные при использовании традиционных методов.

Сегодня можно констатировать факт, что единство в трактовании определения «криминалистическая характеристика преступления» все еще отсутствует.

Так, ряд авторов (Расаев В.В., Коновалова В.Е., Колесниченко А.Н.) предлагают рассматривать данную дефиницию как набор признаков, дающих возможность идентифицировать и классифицировать противоправные деяния конкретного вида. Акцент при определении сделан на конкретных признаках, которые могут быть использованы в расследовании [40, с. 21], [41, с. 16].

Сергуновым А.В. предлагается более широкое понимание криминалистической характеристики как системы информации, которая располагает не только фактической информацией о непосредственном преступлении, но и криминалистически значимых обстоятельствах, имеющих важное значение для процесса расследования [42, с. 3].

Куклин В.И. и Куклин В.В. акцентируют внимание на существующие взаимосвязи между различными элементами. То есть для полноты понимания термина необходимо учитывать такие факторы, как механизм совершения противоправного деяния, последствия его совершения, профиль участников, а также условий, при которых совершено преступление. Данный подход указывает на то, что криминалистика — комплексная наука со множеством взаимосвязанных аспектов, имеющих взаимное влияние [43].

Подобная неоднозначность характеризует и отечественную криминалистическую науку. Так, например, Еркенов С.Е. рассматривает криминалистику транснациональных преступлений как набор характеристик, проявляющих закономерность в процессе их совершения на международном уровне. То есть, указывается на наличие ряда специфических признаков у

Джилкишиев Р.Б.

преступлений, специфичность которых вызвана их транснациональным характером [44, с. 16].

С точки зрения Исаева А.А., это инструмент, метод формирования содержания, т.е. криминалистическая характеристика представляет собой динамическую систему, а не статичный набор данных, способную адаптироваться и изменяться при определенных условиях расследования [2, с. 84-85].

Мозговых Г.А. рассматривает данную дефиницию как совокупность взаимосвязанных признаков и особенностей, включающую не только отдельные признаки, но также и их взаимосвязь [45, с. 129].

Криминалистическая характеристика обладает как теоретической, так и практической ценностью, т.е. может применяться при реальных расследованиях.

Мы считаем, что в основе понятия «криминалистическая характеристика преступления» должны браться наиболее значимые признаки, способствующие раскрытию и расследованию противоправного деяния, включающие ключевые аспекты, которые могут быть использованы следователем для анализа и понимания сути преступления.

Криминалистическая характеристика имеет явное отличие от прочих видов характеристик: она базируется на характерных криминалистически значимых признаках, чертах и качествах [46, с. 51].

Таким образом, мы считаем, что криминалистическая характеристика - это инструмент, при помощи которого следователь может проводить поиск важной информации. Данная характеристика ориентирует следователя на правильную расстановку приоритетов в расследовании и фокусировании внимания на имеющих наибольшее значение в расследовании аспектах. Также криминалистическая характеристика дает возможность следователю более точно сформулировать необходимые обстоятельства для доказывания в суде.

Предлагаемая структура поможет максимально эффективно раскрыть и расследовать преступления в условиях разнообразия и сложности преступности.

Дискуссионным является вопрос касательно элементов структуры криминалистической характеристики.

Элементы криминалистической характеристики не обладают универсальным характером и варьируются в зависимости от конкретного вида совершенного противоправного деяния, т.е. различные виды преступлений требуют и различных подходов в анализе. Тем не менее, существует ряд элементов, информативных для большинства видов противоправных деяний.

Подобную точку зрения можно найти в трудах Белкина Р.С., Васильева А.Н., Яблокова Н.П., Гаврилина Ю.В., Еркенова С.Е., Исаева А.А., Мозговых Г.А., Толеубекова Б.Х. и других ученых.

Определение элементов криминалистической характеристики является недостаточным для успешного расследования преступления. Ключевым моментом является определение закономерных связей между элементами.

Джилкишиев Р.Б.

Понимание взаимосвязи позволяет следователю увидеть полную картину и выявить определенные закономерности, более эффективно планировать следственные действия и определять направления расследования.

Правонарушения в сфере информационных технологий содержат в себе как распространение вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации посредством интернет-сети [47].

Предлагаем более подробно рассмотреть данные элементы, имеющие, на наш взгляд, ряд особенностей, позволяющих построить целостную модель расследования преступления, оптимизировать процесс расследования, а также разработать конкретные рекомендации.

1. Предмет преступного посягательства

В зависимости от объекта и предмета посягательства, все правонарушения в сфере информационных технологий можно разделить на два вида:

1) в сфере самих информационных технологий;

2) где информационные технологии являются орудием или средством совершения другого преступления.

Непосредственным предметом преступного посягательства правонарушений в сфере информационных технологий являются информация и компьютерные средства, если конкретно, то:

- данные и сведения;
- устройство хранения данных;
- информационные системы;
- информационно-коммуникационная инфраструктура;
- программные продукты;
- электронные информационные ресурсы;
- сетевые ресурсы;
- абонентские устройства сотовой связи;
- устройства идентификации абонента;
- программы для изменения идентификационного кода абонентского устройства.

В соответствии с Законом РК от 24 ноября 2015 года № 418-V «Об информации» (далее – ЗРК «Об информатизации» в статье 1 под информатизацией понимается «организационный, социально-экономический и научно-технический процесс, направленный на автоматизацию деятельности субъектов информатизации» [26].

Понятие электронного носителя раскрывается в пункте 41 статьи 3 УК РК, как «материальный носитель, предназначенный для хранения информации в электронной форме, а также записи и ее воспроизведения с помощью технических средств».

В ЗРК «Об информатизации» даны понятия и остальных предметов преступного посягательства, так:

Джилкишиев Р.Б.

Информационная система – это «организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач».

Информационно-коммуникационная инфраструктура – данные в электронно-цифровой форме, содержащиеся на электронном носителе и в объектах информатизации.

Программный продукт – самостоятельная программа или часть программного обеспечения, являющаяся товаром, которая независимо от ее разработчиков может использоваться в предусмотренных целях в соответствии с системными требованиями, установленными технической документацией.

Электронные информационные ресурсы – информация, предоставленная в электронно-цифровой форме и содержащаяся на электронном носителе, интернет-ресурсе и (или) в информационной системе.

Интернет-ресурс – информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете (с. 46).

В Законе РК от 5 июля 2004 года № 567-II «О связи» (далее – ЗРК «О связи») закреплены следующие понятия:

Абонентские устройства сотовой связи – «средство связи индивидуального использования, формирующее сигналы электрической связи для передачи или приема заданной абонентом информации и подключаемое к сети оператора связи» [27].

Централизованная база данных абонентских номеров – аппаратно-программный комплекс управления базой данных, содержащей информацию об абонентских номерах сотовой связи, включая сведения, определяемые правилами переноса абонентского номера в сетях сотовой связи.

К устройствам, на которых возможно хранение информации, относятся: дискеты, жесткие, оптические диски, карты памяти, флэш-накопители с подключением к интерфейсу USB и пр. Инструментом, при помощи которого возможна обработка информации, является компьютер, а также любое электронное устройство, поддерживающее определенные операции с данными (мобильный телефон, цифровой аппарат и прочие аналоговые устройства).

2. Время, место, орудие и обстановка совершения правонарушений, в сфере информационных технологий

В киберпространстве крайне сложно определить место генерации информации, пути ее прохождения, места уничтожения, поскольку данные можно легко скопировать или передать без непосредственного физического контакта или перемещения. Также достаточно затруднительно, а порой и невозможно, определить оригинальную информацию, ввиду возможности репликации данных. Это вызывает значительные трудности при расследовании

Джилкишиев Р.Б.

данной категории дел и требует использования специальных инструментов и методов.

Поскольку преступления данной категории совершаются в виртуальном пространстве, определение конкретного места их совершения значительно затруднено. Например, в случае, когда преступник, являясь резидентом одной страны, совершает противоправное действие в отношении банка, расположенного в другой стране, сам физически находясь в третьей стране, встает вопрос, где именно произошло данное преступление. Правильный ответ на данный вопрос имеет критическое значение для установления юрисдикции, поскольку в трех разных странах свое законодательство и важно понять, какое из них может быть применимо к совершению данного правонарушения. Верное определение места происшествия поможет правильно квалифицировать деяние как уголовное правонарушение.

В традиционной трактовке место происшествия — место совершения преступления. Виртуальное же пространство размывает данное понятие, делая его более абстрактным, поскольку данные могут перемещаться за считанные доли секунд без непосредственного физического перемещения. Также процесс расследования рассматриваемой категории дел затрудняет способность информации к копированию, изменению или удалению.

Такая дефиниция как «место происшествия» — имеет более широкое понимание. Это понятие включает как непосредственное место совершения противоправного деяния, так и место его подготовки, место сокрытия следов. В специальной литературе исследованию данного вопроса уделено достаточно места и времени [48-50].

К особенностям данного определения можно отнести:

1) Изменчивость границ места совершения преступления. Динамическое изменение границ может происходить в зависимости от способа перемещения и обработки данных. К примеру, при использовании прокси-серверов или VPN определение реального местонахождения преступника затруднено.

2) Отсутствие неизменности состояния места совершения преступления. В киберпространстве состояние места не фиксировано и может быстро меняться, выражающееся в возможности удаления, изменения и перемещения данных. Неограниченные территориальные размеры. Киберпреступления могут совершаться с использованием большого количества устройств и систем, которые могут находиться в абсолютно разных местах на значительном расстоянии друг от друга. Они могут играть не только пассивную роль, представляя собой среду для передачи и хранения вредоносного ПО, но и активную, создавая новые информационные связи [51, с. 7 - 20].

3) Сложная структура места совершения преступления, включающая, как минимум, две автоматизированные системы, находящиеся на значительном расстоянии друг от друга, а также вспомогательные и обеспечивающие системы — система электропитания, заземления и прочие сетевые устройства [52].

Следователь проводит анализ данных, полученных из различных информационных источников и ресурсов, что позволяет более точно

Джилкишиев Р.Б.

определить взаимосвязь элементов и совершенного преступления. Исходя из собранных данных, следователем может быть принято решение об определении наиболее существенных для расследования элементов, с дальнейшим включением их в границы места совершения преступления. Более того, он может отказаться от четкого определения границ места совершения противоправного деяния, включив в качестве объектов осмотра лишь основные (опорные) информационные узлы, исходя из их значимости.

Орудия совершения преступлений в киберпространстве зачастую представляют собой специально разработанные (модифицированные) преступником сложные программы, выполняющие различные действия, целью которых является изменение данных или блокировка функций. Помимо достижения основных целей, данные программы могут выполнять вспомогательные задачи, такие, например, как маскировка следов преступных действий — анонимизация, шифрование данных, удаление логов и прочих методов, действие которых направлено на значительное затруднение следственных действий. Орудия киберпреступления могут действовать без непосредственного вмешательства преступника (неочевидная связь), т.е. действовать автоматически. Программа может инициировать действие через достаточно длительные временные промежутки, речь идет о месяцах или даже годах. Данный факт значительно осложняет следственный процесс, поскольку следы могут быть подвержены изменению, уничтожению до момента фиксации их правоохранительными органами.

Ярким примером служит расследование уголовных дел в рамках ст. 205 УК РК. Большинство из них связано с использованием «троянских коней», применяемых преступниками для получения скрытого доступа к системам и учетным данным с целью получения конфиденциальной информации. В следственных действиях было выявлено, что преступники не обладали высокой квалификацией. Для совершения преступления в качестве инструмента правонарушения был использован готовый продукт — программа «Back Orifice», находящаяся в свободном доступе в интернете и сопровождавшаяся подробной инструкций по использованию. Использование вышеупомянутой программы определило способ совершения преступления. Более того, специфика «троянского коня» и его совместимость с конкретными операционными системами (для Windows 95/98, но не для Windows NT, Unix, Linux, например) позволила значительно сузить круг потенциальных жертв преступников и помогло определить места оставления следов преступления.

Как показывает практика, правонарушения в области информационных технологий имеют место, в большинстве случаев, в результате недостатков, образовавшихся при проектировании или реализации автоматизированных систем. Данные изъяны могут быть умышленными (создание умышленной уязвимости) или случайными (ошибки при написании кода, недостаточная защищенность данных). Субъект, который получил информацию о таких изъянах, может использовать данную ситуацию для совершения противоправных действий в виде получения несанкционированного доступа к

системам, использование, кражи конфиденциальных данных. Здесь очень важно различать умышленные действия или случайные ошибки, так как это может иметь решающее значение при проведении правовой оценки действий преступника, а также для разработки превентивных мер.

Под обстановкой совершения преступления следует понимать объективные условия, при которых оно совершается, т.е. совокупность определенных специфических факторов (технические, организационные и социальные).

К таким специфическим факторам относятся: наличие средств защиты и уровень их эффективности; наличие четко регламентированных норм и стандартов в области информационной безопасности; уровень управления, которые обеспечивают соблюдение всех стандартов безопасности и возможность быстрого реагирования на инциденты.

Средства компьютерной техники могут быть использованы на различных стадиях. На стадии подготовки злоумышленник занимается сбором сведений, разработкой плана действий, а также выбором соответствующих орудий преступления. На стадии непосредственного совершения происходит непосредственный взлом систем или кража конфиденциальных данных. На стадии сокрытия преступник может попытаться сокрыть следы преступного действия.

3. Способы подготовки, совершения и сокрытия правонарушений, в сфере информационных технологий

Киберпреступники тщательно планируют свои действия, преследуя целью минимизировать риск задержания и повысить уровень вероятности успешного совершения противоправного деяния. В ходе следственной практики выделены следующие основные направления подготовки совершения преступления:

1) получение доступа к защищенной информации посредством установления аутентификационных данных;

2) подбор соответствующих исполнителей, проведение инструктажа и закрепление обязанностей за каждым соучастником;

3) подбор соответствующих специализированных средств для успешного совершения преступления, облегчающих взлом, дешифровку и т.д.

Преступники, в процессе совершения противоправных деяний в сфере информационных технологий, могут совершать определенные действия, которые сами по себе могут квалифицироваться как самостоятельные правонарушения, т.е. действия, нарушающие закон и являющиеся уголовно наказуемыми (покупка ПО или компьютерного оборудования, электронных устройств, сотовых телефонов, материалов для осуществления преступной деятельности).

Важным элементом при расследовании преступлений является учет особенностей оборудования, используемого при совершении преступного деяния. К примеру, если оно было совершено с помощью определенного вида компьютеров (Apple), данное обстоятельство значительно сужает круг

Джилкишиев Р.Б.

подозреваемых, так как компьютеры на базе Windows являются более распространенными. Устройство же Apple имеет более узкоспециализированное направление: видеомонтаж, графический дизайн. То есть устройство может указать на определенную группу пользователей (профессионалов), имеющих доступ к нему. Более того, специфическая особенность программного или аппаратного обеспечения определяет непосредственный способ совершения преступления и инструментов для его совершения.

Для ухода от ответственности от совершенного преступления преступник использует анонимные методы. К примеру, через прокси-сервисы, обеспечивающие анонимность, он может создавать собственные сайты и размещать на них сведения. Это позволяет скрывать реальный IP-адрес и местоположение, что значительно затрудняет отслеживание их действий преступника. Указание вымышленных имен, ссылка на иных пользователей также играет на руку преступникам, создавая дополнительные трудности для установления их реальной личности. Доступность сети интернет может сделать нарушителем практически любого пользователя, например, размещение материалов оскорбительного характера или незаконных материалов может быть осуществлено любым пользователем ПК. Это увеличивает круг потенциальных подозреваемых.

Использование общественных мест, таких как интернет-кафе, является достаточно серьезной проблемой, поскольку дают возможность выхода в интернет без предоставления личных данных пользователей. Отсутствие необходимости идентификации создает анонимность поведения с одной стороны и затрудненность работы по поиску для правоохранительных органов с другой. Работая через интернет-кафе, злоумышленники могут использовать различные технологии для сокрытия своей настоящей личности, включая временные электронные почтовые ящики, анонимные браузеры, тем самым затягивая следственные действия.

Изучение способов совершения преступлений в сфере компьютерной информации, берет свое начало с середины семидесятых годов прошлого века, но, тем не менее, остается актуальным и на сегодняшний день. Первое упоминание о проблемах кибербезопасности и несанкционированного доступа к системам встречается в трудах Хоффмана Л. Дж. Несмотря на то, что методы защиты информации постоянно эволюционируют, изначальные способы неправомерного доступа все еще могут быть действенны и активно используются преступниками, т.е. это позволяет злоумышленникам адаптироваться к новым условиям, используя старые, но весьма эффективные техники.

Данные описания в дальнейшем нашли свое отражение в специализированной литературе, посвященной изучению информационной безопасности, а затем и в специализированной криминалистической литературе [53-55]. Однако их многократное заимствование привело к потере контекста и существенному смысловому искажению важных технических особенностей.

Джилкишиев Р.Б.

Это чревато появлением неправильной интерпретации работы определенных техник и значительно затрудняет разработку эффективных мер защиты. Здесь крайне важно использование критического анализа со стороны специалистов по информационной безопасности и правоохранительных органов, что позволит им избежать распространения ложных и (или) потерявших актуальность данных.

Предлагаем рассмотреть основные типы атак операционных систем, рассмотренных в работе Хоффмана Л. Дж., принятых в качестве основы для всех последующих описаний [56].

Атаки на основе асинхронности. Современные вычислительные системы — многозадачны, т.е. способны выполнять несколько процессов одновременно. Однако подобная многозадачность может привести к неожиданному результату: в процессе взаимодействия друг с другом, один из процессов может повлиять на параметры, изменив их, при этом другой процесс подобные измененные параметры еще не использовал. Это может создать уязвимости, которыми пользуются преступники. К примеру, зафиксирован случай, когда текстовый файл MS Word содержат фрагмент из файла MS Excel, который одновременно обрабатывался на том же компьютере. Данный факт показывает, как асинхронность процессов может привести к утечке данных, что предоставляет собой реальную угрозу для безопасности систем безопасности информационных систем.

Атаки на основе включения «между линиями». Подобный вид атаки происходит при подключении преступника к каналу связи между двумя истинными устройствами, в качестве которых, к примеру, могут выступать терминал и сервер, посредством чего происходит перехват или изменение передаваемой информации. Атаки могут происходить и при неактивности пользователя, но когда он все еще удерживает соединение.

Атаки на основе тайного кода. При атаках подобного типа несанкционированный доступ к системе происходит при внесении преступником изменений в существующее программное обеспечение путем добавления скрытых функций, позволяющий получать такой доступ. В качестве примера можно привести случай с Внешэкономбанком (рассмотрен в первой главе настоящей диссертационной работы), когда преступники, воспользовавшись уязвимостью в программном обеспечении, получили доступ к конфиденциальной информации и возможность управления системой безопасности.

Атаки на основе маскировки. Атака происходит при использовании преступником украденных идентификационных данных (имена пользователей, коды, пароли). Доступ к таким данным может осуществляться не техническим, а «традиционным» способом — подслушиванием, подкупом, манипуляциями и пр.

Атаки типа «NAK». Для осуществления данного вида атаки преступник использует метод прерывания процессов, т.е. использование уязвимостей операционных систем для их прерывания. Это может позволить

Джилкишиев Р.Б.

злоумышленнику активно вмешиваться в работу систем и копировать их состояние, с целью внесения изменений.

Атаки на основе перестановочного программирования. Проводятся с целью определения нестандартных (непредусмотренных системой) реакций и нахождения уязвимостей. Осуществляются путем внедрения специально разработанных программ, использующих алгоритмы для генерации различных комбинаций входных данных.

Атаки на основе поэлементной декомпозиции. Основываются на разбивке критической информации (пароли, идентификационные имена) на отдельные элементы. Далее данные фрагменты представляются системам защиты атакуемой системы. Реакция системы позволяет преступнику провести анализ и изучить строение защитных механизмов для их преодоления. Также преступник может получить идентичную копию программного обеспечения, функционирующую в системе с целью проведения реассемблирования.

Атаки типа «Piggy back». Осуществляются при подключении к каналу связи между пользователем и системой, пользуясь, например, уязвимостью в сетевой инфраструктуре. После подключения злоумышленником отправляются ложные сообщения, которые заставляют пользователя думать, что произошла какая-то ошибка или доступ временно заблокирован. Пользователь начинает повторное подключение, при этом используя определенные действия, какие и считываются преступником с целью дальнейшего несанкционированного доступа к системе.

Атаки на основе «троянского коня». Представляет собой внедрение вредоносной программы, маскирующейся под легитимную (антивирусы, утилиты), что позволяет преступнику скрытно проникать в систему с целью выполнения вредоносных действий (кража данных, создание «задних дверей» и пр.).

Большинство из упомянутых выше атак актуальны для локальных сетей и отдельных компьютеров. Однако технологическое развитие и широкое использование глобальных сетей активизировали и угрозы, делая их более разнообразными и сложными. Следовательно, наибольший интерес представляют противоправные деяния, совершаемые в киберпространстве.

На основании данных, полученных в ходе проведенного в 1996 году анализа CSI (Computer Security Institute), специализирующегося на вопросах безопасности информации и кибербезопасности, определен перечень основных способов совершения преступлений в сфере кибербезопасности [57]. Основными из них являются:

- brute-force (подбор паролей): перебор всех возможных комбинаций паролей с целью доступа к учетной записи;

- IP-spoofing (подмена IP-адресов): подмена ложными IP-адресами пакетов, выглядящих легитимными;

- Denial of Service, DoS (отказ в обслуживании): основная цель — перегрузка системы или сети, тем самым, делая их недоступными для пользователя;

- sniffer (анализ трафика): «прослушка» сетевого трафика, конечной целью которой является сбор конфиденциальных данных;

- scanner (сканирование): использование вредоносных программ для поиска точек уязвимости;

- data diddling (изменение данных): манипуляция с данными, позволяющая подменять или уничтожать их;

- прочие типы атак и диверсионных действий.

Ранее большинство придерживалось мнения, что совершение киберпреступлений — характерная особенность развитых стран. Однако с развитием технологий и увеличением доступа к интернету ситуация кардинально изменилась. Сегодня хакерские группировки технически оснащены, интеллектуально развиты и могут действовать из любой точки мира. Они могут осуществлять обмен знаниями и опытом посредством онлайн-ресурсов, форумов и чатов. Более того, сегодня хакеры организовывают бизнес по предоставлению услуг взломов, продаже украденной информации, разработке вредоносного ПО и осуществления атак.

Говоря о способах сокрытия правонарушений в сфере информационных технологий, можно условно их поделить и описать по следующих видам:

1) утаивание информации или (и) ее носителей. Предполагает собой намеренное сокрытие фактов и сведений от следственных органов, выражающееся в игнорировании предоставления информации на запросы, отказе от дачи показаний, нежелании выполнять законные требования органов, ведущих расследование, недонесении, равно как и сокрытии физических доказательств;

2) уничтожение информации или (и) носителей, на которых она содержится. Подразумевается целенаправленное уничтожение как непосредственно самих данных, так и носителей таких данных;

3) маскировка информации или (и) носителей, на которых она содержится. Предполагает выполнение целенаправленных действий, направленных на изменение или сокрытие объектов правонарушения как перемещение документов, арипляция (манипуляции с внешностью), либо маскировка происходящих действий (например, с использованием шумов);

4) фальсификация информации или (и) носителей, на которых она содержится. Предполагает создание поддельной документации или предоставление ложных данных с целью введения в заблуждение следственных органов.

Это может включать действия, направленные на фальсификацию фактов, документов и прочих сведений (паспорта, контракты, финансовая отчетность); дача заведомо ложных свидетельств или показаний; оставление ложных следов (создание ложной доказательной базы, подброс фальшивых улик); копирование (дублирование) объектов (подделка произведений искусств, ценностей); намеренное изменение данных о предназначении объекта или документа (изменение назначения финансовых средств в финансовых отчетах с целью сокрытия неправомерных умышленных действий) и пр.

Джилкишиев Р.Б.

Глобализация угроз, доступность высоких технологий и высокотехнологичных инструментов для создания атак породили рост числа группировок хакерского толка, использующих различные методы сокрытия следов преступления. К наиболее распространенным способам программно-технического сокрытия относятся: использование специализированных серверов, позволяющих скрывать адреса и данные пользователей (анонимизаторы, ремейлеры); создание фальшивых адресов, с которых отправляются сообщения с целью введения в заблуждения и затруднения обнаружения фактического нахождения преступника; использование промежуточных (прокси) серверов для маскировки реального местоположения; применение вредоносного ПО, способного удалять, изменять данные с целью уменьшения фактического присутствия следов; уничтожение данных, указывающих на то, что было совершено преступление; применение задержек и условий активации между внедрением вредоносного ПО и непосредственным совершением преступления (ПО может быть активировано в конкретный период времени или при запуске определенных программ).

4. Следовая картина

Любое противоправное деяние рассматривается как некое действие, нарушающее законы или общественные нормы, т.е. преступление можно рассматривать как явление. Всякое явление имеет под собой последствия (материальные, нематериальные), которые могут быть зафиксированы и проанализированы, следовательно, оставлять следы. Следы преступления представляют собой определенные изменения в окружающей среде, имеющие физический (объекты, которым нанесено повреждение, улики) или цифровой (письма, файлы) характер [58, с. 63].

Понимание природы образования следов преступления и их роли в расследовании является критически важным моментом. От этого зависит своевременность, полнота и эффективность проведения следственных действий.

В сфере киберпреступности стадии формирования информационных следов выглядят следующим образом:

- определение цели: на данной стадии злоумышленник выбирает информационную систему для атаки (сервер, база данных, любая другая система, которая содержит ценную информацию);

- выбор информации: этап предполагает выбор информации, которая должна быть получена или изменена (личные, финансовые и прочие данные, представляющие интерес);

- предварительный сбор информации: преступник занимается сбором сведений о целевой системе, изучает ее функционал, технологии, которые используются для обработки информации, ПО, в котором могут быть выявлены уязвимые места;

- планирование преступления: включает разработку общей стратегии атаки, вовлечение подельников и их подготовку;

Джилкишиев Р.Б.

- воздействие на информацию: непосредственное проведение атаки посредством внесения изменения данных либо создания их копии (взлом, установка вредоносного ПО и пр.);

- наступление эффекта: преступник достигает поставленной цели, получив доступ к нужной информации;

- сокрытие следов: стадия предполагает принятие мер по сокрытию преступных действий, значительно затрудняющих расследование (удаление логов, использование анонимизаторов и пр.).

Положения криминалистики классифицируют следы совершения противоправного деяния следующим образом:

Материальные следы — изменение среды физического характера (поврежденные компоненты устройства, наличие логов доступа, файлы и пр.).

Идеальные следы — следы, остающиеся в памяти людей (преступники, соучастники, свидетели).

Данный традиционный подход оказался неэффективным при расследовании преступлений, совершенных в киберпространстве: методы, которые хорошо зарекомендовали себя при расследовании «традиционных» преступлений, не всегда применимы к киберпреступлениям. В основе традиционных медов следообразования — механический подход, предполагающий их образование вследствие физического взаимодействия объектов. Но мы знаем, что в цифровом пространстве следы менее очевидны, зачастую, не связанные с непосредственным физическим контактом. В классической криминалистике под следом, как правило, понимается отображение одного объекта на другом. В рамках киберпреступности данное понятие слишком узко, так как цифровые следы могут быть представлены в виде определенных форм информации, не оставляя физических отпечатков [59, с.13].

Расследование правонарушений в сфере информационных технологий имеет ряд специфических особенностей. Так, в качестве основных объектов выступают не физические, а информационные объекты (данные и программы), имеющие сложную иерархию. Это значительно затрудняет проведение их анализа в рамках традиционной криминалистики. Более того, следы в киберпреступлениях не обязательно оставляют видимые материальные отпечатки, в отличие от традиционных преступлений, где следы имеют четкую физическую форму (сколы, царапины, деформации, измененный химический состав и пр.). Поскольку информация может передаваться и храниться в виде электромагнитных сигналов, сегодня криминалистика имеет дело с изучением следов, существующих в электромагнитном поле. Таким образом, традиционные методы криминалистики, основанные на механическом подходе, оказываются недостаточными при анализе цифровых следов.

Исходя из криминалистики, процесс получения информации о каком-либо объекте состоит из ряда этапов, исследование следообразования, обнаружение следов, фиксация следов, изъятие следов. Указанные действия предпринимаются с единственной целью — идентификация и установление

Джилкишиев Р.Б.

тождества обнаруженных следов, что способствует воссозданию картины произошедших событий и пониманию, как и что произошло [60, с.36].

Механизм следообразования в зависимости от способа совершения правонарушения будет различаться.

Выявленные особенности следообразования при совершении киберпреступлений актуализировали вопрос необходимости адаптации криминалистических методов к новым реалиям и, как следствие, введения такого термина как «виртуальные следы». Это — промежуточное понятие между материальными и идеальными следами. Под виртуальными следами понимается любое изменение в состоянии автоматизированной информационной системы, фиксирующееся в виде компьютерной информации.

В науке существует достаточно большое число подходов к классификации виртуальных следов. Они могут классифицироваться, исходя из следующих критериев:

- электронный носитель информации (компьютерное оборудование, мобильные устройства, серверы, облачные хранилища);

- место, где могут находиться виртуальные следы (удаленные, локальные устройства, сети);

- форма, в которой могут быть отображены виртуальные следы (файлы в текстовом формате, графические файлы, базы данных и т.д.).

Мы, в свою очередь, предлагаем классификацию виртуальных следов в зависимости от их трансформации, которая состоит из следующих основных типов:

- появление, где в результате действий пользователя создается новая информация или данные;

- исчезновение, где информация или данные могут стать недоступными вследствие определенных намеренных действий пользователя или сбоя системы;

- модификация, где информация подвергается существенному изменению (редактирование, изменение начальных настроек, обновление ПО).

При этом виртуальные следы могут храниться на разнообразных носителях информации: эфир (в случае передачи информации по беспроводным сетям); магнитные и оптические диски (традиционные носители); полупроводниковые устройства (чипы, микросхемы, процессоры, способные хранить данные в виде кода).

Виртуальные следы могут проявляться и в изменении характеристик систем: изменении в производительности, отказе в выполнении запрашиваемой операции, изменении последовательности операции.

Мы уверены, что разработка более детализированных и адаптированных подходов к классификации виртуальных следов — важный шаг для эффективного расследования противоправных деяний рассматриваемой категории дел.

Ключевыми характеристиками следообразующих объектов являются:

1) размер сообщений электронной почты и программы — позволяет идентифицировать тип содержимого;

2) временные метки создания (получения, модификации) — позволяют определить хронологию совершения преступления и связать с другими возможными событиями или действиями;

3) атрибуты файлов и сообщений — позволяют понять, был ли использован или изменен файл. Понимание уровня конфиденциальности может помочь в оценке его значимости;

4) записи исполняемых программ и файлов конфигурации — содержащиеся в них идентификаторы позволяют определить конкретные версии вредоносного ПО.

Анализ следовоспринимающих объектов выявил следующее:

На компьютере лица, которому причинен ущерб:

- таблица размещения файлов (FAT, NTFS и др.), содержащая информацию о нахождении файлов, позволяет совершить их восстановление даже после удаления;

- реестр операционной системы, в котором хранятся настройки и параметры операционной системы, позволяет выявить определенные изменения в свете установления вредоносного ПО;

- физические единицы хранения данных на диске (отдельные кластеры), позволяет восстановить фрагменты удаленных файлов и выявить следы вредоносного ПО;

- файлы, каталоги, где хранится входящая электронная почта, помогает в выявлении вредоносного вложения или фишинговых сообщений;

- файлы конфигурации программ удаленного соединения, позволяет выявить несанкционированные подключения к интернету или другим сетям и изменения в конфигурации.

На компьютере лица, совершившего противоправное деяние:

- таблица размещения файлов (FAT, NTFS и др.), содержащая информацию о созданных или измененных файлах и времени манипуляций с ними;

- файлы конфигурации программ удаленного соединения, помогают определить конкретные методы, при помощи которых преступник устанавливал соединения и получал доступ к информации;

- физические единицы хранения данных на диске (отдельные кластеры), позволяют восстановить фрагменты удаленных файлов и выявить следы вредоносного ПО, в том числе свидетельствующие о сокрытии действий или удалении доказательств.

Проведенный анализ опыта следственных действий выявил наиболее часто используемые инструменты и технологии для поиска виртуальных следов, их наиболее существенные недостатки, на основе которых выработаны предложения по формированию программно-технических средств. Анализ технологий, используемых в области компьютерной криминалистики, необходимо проводить на регулярной основе. Это позволит следственным

Джилкишиев Р.Б.

органам своевременно и эффективно реагировать на новые вызовы и угрозы в сфере информационной безопасности.

Специфика виртуальных следов вызывает необходимость совершенствования законодательных норм, поскольку существующие процессуальные нормы не соответствуют требованиям расследования противоправных деяний, совершаемых в киберпространстве.

Непосредственные экземпляры материальных следов являются носителями максимально полной следовой информации, т.к. при детальном изучении указанных материальных объектов представляются возможными выдвижение следственных версии и решение вопросов, возникающих на первоначальном этапе расследования данной разновидности правонарушений:

- кем осуществлялось изготовление материальных следов;
- оборудование, на котором производилось изготовление;
- количество лиц, задействованных в производстве материальных следов;
- качественные характеристики исследуемых образцов.

Выявление идеальных следов в расследовании правонарушений, связанных с клеветой, возможно путем проведения допросов. Для успешного расследования и получения полного представления о ситуации, необходим сбор данных от различных источников. Здесь крайне важно получить сведения не только от лиц, ставших свидетелями совершения преступления, но и других лиц.

К следам, указывающим на несанкционированный доступ к охраняемой законом информации, можно отнести следующие признаки, указывающие на факт доступа к данным посторонних лиц:

- изменение в файловой системе: изменение названий файлов, каталогов, их размеров, реквизитов, а также изменение их содержимого;
- проявления, не свойственные обычной работе компьютера: замедленная реакция на ввод информации с клавиатуры, длительная загрузка операционной системы, проблемы при работе с дисковыми накопителями;
- сетевые изменения как появление новых устройств или удаление старых;
- трансляция на мониторе необычных символов и знаков.

Таким образом, под следами компьютерных правонарушений следует понимать преобразование компьютерной информации в результате ее уничтожения, блокирования, дублирования/копирования, модификации. Также в качестве следов правонарушений могут рассматриваться изменения, которым подверглись физические носители информации, связанные с конкретным событием правонарушения.

Наиболее распространенным противоправным деянием в настоящее время является распространения вредоносных программ по типу «троянского коня» (Back Orifice, Dolly 16 и т.п.). Данный тип программ маскируется под видом вполне легитимного приложения с целью обмана пользователя. После установки программы создают видимость нормальной программы и даже могут выполнять ряд незначительных функций, чтобы отвлечь пользователя.

Джилкишиев Р.Б.

Основная же их работа направлена на установку вредоносного кода на компьютер и прописывание его в системном реестре, после чего он будет запускаться в автоматическом режиме при включении компьютерного устройства. Действие установленной вредоносной программы заключается в установлении соединения с интернет-провайдером и настройки порта для удаленного доступа, далее вредоносная программа опрашивает диапазон IP-адресов, находя жертву, к которой можно подключиться. После установления соединения злоумышленник беспрепятственно получает возможность к подключению компьютера жертвы и управления им.

В процессе совершения такого противоправного деяния как распространение вредоносного ПО по типу «троянского коня», в качестве объектов, служащих доказательствами, могут выступать:

- на этапе внедрения — электронное письмо, к которому прикреплен вредоносный файл;

- на этапе активизации — непосредственно сам исполняемый файл.

При этом основными, наиболее криминалистически значимыми характеристиками следообразующих объектов, являются размер файлов, дата и время, атрибуты файлов, фрагменты кода (конфигурации), способные идентифицировать конкретный экземпляр вредоносной программы.

Также к дополнительным следообразующим объектам относятся:

1) Файлы, используемые для рассылки «троянских коней»:

- стандартные почтовые программы, используемые для отправки вредоносных сообщений или иные специализированные программы, предназначенные для аналогичных целей;

- файлы в текстовой формате, содержащие списки рассылок, дату и время отправки, а также количество попыток при повторной отправке;

- файлы программ, обеспечивающие удаленное соединение с компьютером жертвы.

2) Файлы компилятора:

- в компиляторах (специализированные программы) происходит преобразование исходного кода в исполняемую программу. Каждая версия компилятора обладает своими собственными особенными настройками, которые могут быть автоматически внедрены в создаваемую программу;

- библиотеки компилятора и операционной системы. Функционирование многих программ зависит от функционирования сторонних библиотек или пакетов приложения. Известны случаи, когда злоумышленники, используя стандартные платформы и инструменты для коммуникации (например, ICQ), скрывали свои действия и упрощали процесс передачи украденных данных.

Так как при совершении киберпреступления принимают участие минимум два компьютерных устройств (компьютер лица, которому причинен ущерб и компьютер лица, причинившего ущерб), объектов тоже может быть несколько.

Компьютер лица, которому нанесен ущерб:

Джилкишиев Р.Б.

Таблица размещения файлов (FAT, NTFS и др.). Данный тип представляет собой первую часть вредоносной программы. Как правило, это исполняемый файл и файл конфигурации. Таблица содержит файлы с произвольными именами с фиксированной длиной, при этом дата и время их создания или модификации должны соответствовать временным рамкам установления программы.

Пострадавшими от рассматриваемого вида преступлений могут быть учреждения и предприятия, пользующиеся автоматизированными компьютерными системами для обработки бухгалтерских и финансовых документов. Особенно уязвимыми являются банковские учреждения [61, с.87].

Компьютер лица, который нанес ущерб:

Таблица размещения файлов (FAT, NTFS и др.). Данный тип представляет собой вторую часть вредоносной программы. Как правило, это два файла: исполняемый файл и файл конфигурации.

Достаточно даже беглого взгляда, чтобы понять, что анализ следов, оставленных вредоносными программами, играет ключевую роль при расследовании противоправных деяний рассматриваемой категории.

Как было сказано выше, виртуальные следы имеют свою особенную специфику. В отличие от физических улик они не подлежат изъятию в традиционном смысле. Их можно либо скопировать, либо удалить. Таким образом, их обнаружение и фиксация требует особого подхода и может осуществляться лишь силами специализированных следственно-оперативных групп с использованием различных программно-технических средств.

Специализированные утилиты (DiskEdit из Norton Utility) помогут с поиском и копированием заданной информации, а также с просмотром отдельных кластеров магнитных носителей.

Командная оболочка FAR или утилитой «Copy» позволяет копирование обнаруженных файлов с виртуальными следами (режим F5).

Более сложной задачей является выявление и регистрация виртуальных следов второго типа, такого как изменение характеристик информационных процессов. Выявление таких следов требует ведения мониторинга определенных параметров системных процессов в автоматизированной системе: нагрузка на процессор, объем памяти, количественные характеристики входящих и исходящих запросов и пр. Оценка данных параметров (количественные и качественные характеристики) происходит в течение интервала времени, определенного заранее (интервал наблюдения). Ввиду наличия множества возможных изменений и особенностей функционирования информационных систем, процесс выявления таких виртуальных следов достаточно проблематичен. Более того, преступники могут предпринять действия по сокрытию следов или манипулированию параметрами, что существенно осложняет мониторинг.

5. Типологические особенности личности правонарушителя в сфере информационных технологий

Джилкишиев Р.Б.

Анализ личности преступника, совершающего преступные деяния в сфере информационных технологий, является критически важным и играет одну из ключевых ролей. Преступники, обладающие высоким уровнем технических знаний, способны разрабатывать свои собственные методы атак. Их действия — более изощренные, следовательно, более трудоемки в плане отслеживания. Готовыми решениями, как правило, пользуются злоумышленники с меньшим опытом и ограниченными навыками. Способы совершения киберпреступлений могут в значительной степени характеризовать преступника, их совершающего. К примеру, подготовка DDoS-атаки требует тщательной подготовки, четкой координации и затратных ресурсов, в то время как использование фишинга указывает на более низкий уровень технических знаний и подготовки. Также о намеренном желании избежать ответственности путем использования более высокотехнологических методов является использование анонимизаторов (VPN, Tor). Зачастую практика показывает, чем технически сложнее преступление, тем меньшее количество людей может его совершить. Порой конкретный инструмент совершения преступления может с большой долей вероятности указать на конкретного исполнителя.

Большинство авторов, занимающихся исследованием данного вида противоправного деяния, сходятся во мнении, что киберпреступники, в большинстве случаев — одаренные и уникальные личности, обращающие на себя внимание.

Тем не менее, необходимо всегда помнить, что киберпреступление — это сложное явление, где может быть задействовано значительное количество людей, обладающих разной степенью технических знаний, с индивидуальными чертами характера, различной мотивацией, идейными убеждениями и ролями.

В зависимости от того, как преступник задействован и вовлечен в преступление, можно выделить следующие ключевые роли:

- организатор — лицо, планирующее и осуществляющее координацию преступления, обладает высокими лидерскими качествами и высокими навыками в области технологий;

- исполнитель — лицо, непосредственно осуществляющее преступление, может быть достаточно технически подкованным, но с менее высокими навыками;

- соучастник — лицо, участвующее в организации преступления, но не осуществляющее непосредственное его исполнение, как правило, не обладает какими-либо глубокими знаниями, но может представлять другие ресурсы и информационное сопровождение.

Говоря о «типовых свойствах личности преступника в сфере компьютерной информации», подразумевается именно исполнитель, поскольку он осуществляет непосредственное взаимодействие орудием правонарушения. Тем не менее, необходимо подчеркнуть, что личностные характеристики могут изменяться, исходя из роли, которую играет злоумышленник. Например, организаторы более вдумчивы, отличаются аналитическим складом ума. Исполнители же более импульсивны, склонны к спонтанным решениям.

Джилкишиев Р.Б.

При проведении следственных действий крайне важно установить круг лиц, которые взаимодействовали с системой, где было зафиксировано правонарушение. Данный круг не должен ограничиваться лишь программистами или системными администраторами. Он включает в себя также специалистов вспомогательных служб (связисты, электрики) и даже обслуживающий технический персонал, имеющий доступ к помещению с оборудованием. Современные реалии таковы, что доступ к автоматизированным системам может осуществляться удаленно, при этом круг лиц, имеющих к ним доступ, достаточно широк. Это могут быть сотрудники других организаций или даже люди, проживающие в других странах. Таким образом, принимая во внимание факт, что киберпространство не ограничивается какой-либо определенной географической территорией, следует учитывать всех лиц, имеющих доступ к системе, независимо от их роли или местоположения.

Помимо установления круга лиц немаловажным является вопрос получения информации об уровне их подготовки в области информационных технологий, так как это поможет выявить лицо, вовлеченное в совершение преступления. Данная информация, к примеру, может быть предоставлена службой информационной безопасности, так как сотрудники данной службы имеют доступ к необходимой информации по каждому работнику. Здесь крайне важно не ограничиться лишь информацией о занимаемой должности. Известны случаи, когда высококвалифицированные специалисты могли находиться на низкооплачиваемой должности (уборщики, электрики), но, имея прямой доступ к системам, имели возможность совершения преступления. Таким образом, необходимо подходить к вопросу проверки сотрудников тщательно и скрупулезно, независимо от занимаемой им официальной роли.

В первую очередь, в поле зрения следователя должны попадать сотрудники, обладающие специфическими навыками в области программирования или управления специализированными устройствами. Например, работники, разбирающиеся в языках программирования низкого уровня (ассемблер), могут иметь уникальные навыки, которые дают возможность взаимодействовать с нестандартными устройствами, что делает их потенциально опасными, поскольку они могут манипулировать системами на более высоком уровне. Если к работе по программированию или управлению устройствами были привлечены сторонние специалисты, необходимо выяснить, кто из действующих сотрудников мог коммуницировать с ними. Более того, анализу должны подлежать не только профессиональные, но и личные связи.

Анализ стиля программирования в расследованиях — еще одна немаловажная задача, поскольку это может установить автора программного вируса. Полезно создать своеобразную базу образцов кодов, написанных известными программистами. Эти образцы являются референсными точками, при помощи которых можно провести сравнительный анализ похожих структур, стили и алгоритмы написания. Каждый программист использует свой уникальный, присущий исключительно ему, стиль программирования. Он

Джилкишиев Р.Б.

формируется на основе его знаний и набранного практического опыта. При постановке одной и той же задачи, различные программисты подходят к ее решению индивидуально, используя свои приемы и методы. Зачастую программисты при решении задачи не придумывают каждый раз новые способы, а работают по своим же шаблонам, что дает возможность распознавать их стиль. Таким образом, вполне возможно идентифицировать автора вредоносной программы по устойчивым приемам написания кодов, присущих конкретным программистам. Однако необходимым условием для точной идентификации является наличие достаточного объема образцов программного кода, написанного конкретным программистом.

В среде программистов часто используется профессиональный сленг или жаргон, не понятный другим, далеким от сферы кибербезопасности.

Согласно данным Интерпола, представленным на первой международной конференции, правонарушители классифицируется по возрасту на три основные группы: от 11 до 15 лет, от 17-25 лет, 30-45 лет. Указанным возрастным группам свойственен свой тип поведения и мотивация при совершении преступления, что может влиять на стратегии борьбы с киберпреступностью. Также градация преступников по возрастным группам может помочь следователю понять суть компьютерного правонарушения и выработать соответствующие меры для их предотвращения.

При проведении анализа противоправного деяния необходимо учитывать характеристики лица, непосредственно осуществившего преступление. Уголовно-правовая характеристика личности преступника включает, возраст вина, вменяемость, обстоятельства, при которых совершено преступление, квалификация противоправного деяния и наказание, назначенного за его совершение (ст. ст. 15, 16, 19 УК РК).

Давайте более подробно остановимся на вышеназванных возрастных группах.

Первой возрастной группой, в основном, совершаются кражи через кредитные карты и номера телефонов. Как правило, подростки не осознают (не до конца осознают) серьезность и последствия своих действий. Ими движет любопытство, желание экспериментировать, стремление к самоутверждению и привлечение внимания сверстников. Получение выгоды, как таковое, стоит на втором плане.

Вторая возрастная группа совершает похищение из баз данных. В основном, это студенты, стремящиеся к дальнейшему проведению экспериментов и использования уже накопившиеся знания с целью повышения «профессионального» уровня. Их намерения менее криминальные, но, тем не менее, рассматриваются как нарушение закона и могут иметь достаточно серьезные правовые последствия.

Третья возрастная группа совершают умышленные противоправные деяния, основной целью которых является получение прибыли, либо осознанное повреждение компьютерных сетей. Представители данной группы

Джилкишиев Р.Б.

обладают достаточным опытом, преступление совершают по заранее выработанной стратегии.

Исследование личности преступника — комплексный подход, предполагающий изучение разнообразных социальных и психологических характеристик. То есть анализ не должен ограничиваться лишь с учетом уголовно-психологических аспектов, но и должен охватывать такие социальные характеристики как возраст, гендерная принадлежность, культурный уровень, уровень образования, социальные нормы и стереотипы, личностные ценности и убеждения, индивидуальные (психологические) черты характера. Все это формирует поведенческий механизм, содержащий причины и мотивы, побудившие злоумышленника совершить преступление. Понимание данного механизма поможет следователю правильно оценить риски и разработать превентивные и реабилитационные меры.

В подавляющем большинстве киберпреступники — это мужчины. Тем не менее, в последнее время все чаще можно услышать заявление, что растет число и женщин-киберпреступниц. Однако статические данные за последние пять лет не подтверждают данное заявление. Вместе с тем известны факты, когда женщин-хакеров привлекали к киберпреступлениям в рамках преступных групп для осуществления неправомерного доступа к информации в банковской сфере.

Наибольшую опасность для сферы информационной безопасности представляют специалисты с высоким уровнем знаний в области информационных технологий. Потенциально высокая угроза связана с тем, что они обладают доступом к системам и данным, более того, понимают, как эти системы функционируют. Это позволяем им достаточно быстро находить уязвимые места и использовать данный факт в своих интересах. Примерный список должностей обслуживающего персонала может дать приблизительную информацию об уровне доступа к информации, а также степень влияния на безопасность данных. За каждой должностью закреплены свой функционал, который может иметь отношение к обработке, хранению, защиты данных. Понимание функциональных задач способствует выявлению потенциальных рисков или уязвимостей, которые могут быть использованы для совершения преступления.

В реальных автоматизированных системах функциональные задачи нескольких должностей могут быть закреплены за одним человеком или могут вообще отсутствовать, т.е. это указывает на то, что четкая иерархия к доступу информации может отсутствовать или быть достаточно размытой, что значительно увеличивает риски. Например, несмотря на высокий доступ и широкие права, управляющий банка все же является пользователем системы. Таким образом, его действия могут быть более контролируемыми в контексте совершения преступлений, а также свидетельствует о том, что не всегда пользователи с высокой ролью представляют реальную угрозу и наоборот. Также стоит отметить, что высокопрофильные пользователи более строго

Джилкишиев Р.Б.

контролируемые, что значительно снижает вероятность их вовлечения в противоправные деяния.

Принимая во внимание вышесказанное, приходим к выводу, что структура и распределение ролей имеет прямое непосредственное влияние на уровень безопасности и риски, связанные с киберпреступностью.

Сотрудники могут быть разделены, исходя из выполняемой им роли и доступа к системе, на различные категории. В свою очередь, каждая категория обладает индивидуальной степенью риска, исходя от уровня возможного ущерба, который может быть причинен системе (от неосторожных действий до умышленного нарушения).

Основная отличительная особенность криминалистического изучения личности преступника заключается в выявлении причинно-следственных связей, способствующих установлению связи между конкретным совершенным преступлением и конкретным лицом, совершившим преступление. Также исследование личности злоумышленника напрямую связано с анализом следов преступлений, позволяющих указать на причастность конкретного человека к совершению преступления. Здесь крайне важно выработать эффективную методику расследования и тактику проведения следственных действий. В отличие от других направлений криминалистики, акцентирующихся на технических аспектах, данное направление сосредотачивается на психологических и поведенческих аспектах, позволяя детально понять мотивацию и действия преступника.

В рамках изучения рассматриваются не только поведенческие моменты, но и биологические и физиологические характеристики: пол, возраст, физическое состояние и прочие аспекты, влияющие на его действия. Профессиональные навыки также играют немаловажную роль и могут непосредственно влиять на способ совершения преступления и успешность его совершения.

Криминалистическая литература предлагает несколько подходов к классификации личности киберпреступников [48, с.75].

Учет особенностей личности может лучше понять поведение преступника, его мотивацию, выбрать наиболее эффективные тактические приемы. Таким образом, понимание личности подозреваемого — один из ключевых моментов в криминалистике, так как позволяет следователю осуществлять более эффективное расследование и достижения поставленных целей.

Исходя из преступной специализации, выделяют следующие категории преступников: кракеры (кража или разрушение данных); фрикеры (несанкционированный доступ без умысла получения материальной выгоды, а лишь демонстрации навыков); кардеры (кража и использование кредитных карт, финансовой информации); хакеры (этичные, злонамеренные, в зависимости от намерений и целей).

6. Причины и условия, способствующие совершению правонарушения в сфере информационных технологий

Джилкишиев Р.Б.

Характер преступления, рост числа киберпреступлений, а также техническая сложность их совершения вызвали и определенное увеличение внимания к данной проблеме в криминалистической литературе. Однако здесь отсутствует единство в определениях, т.е. на данный момент нет единого подхода к определению дефиниции «криминалистическая характеристика правонарушений в сфере информационных технологий», что в значительной степени затрудняет формирование единой теории и разработку эффективных методов расследования.

Вышеобозначенные причины, а также условия совершения киберпреступлений обладают общим (универсальным) характером и применимы для многих видов объектов, которые могут быть подвержены правонарушениям в сфере информационных технологий, т.е. они имеют широкое распространение, не ограничиваясь лишь отдельными случаями. Устранение данных причин возможно только при выработке системного комплексного подхода, реализуемого на государственном уровне, что может включать совершенствование законодательства, усиление мер безопасности, повышение уровня образования и осведомленности конечных пользователей. Только посредством реформирования можно улучшить ситуацию и добиться значительных изменений в ситуации с киберпреступлениями.

Мы предлагаем с целью повышения эффективности криминалистического обеспечения расследования преступлений, совершенных в сфере информационных технологий, разработать и внедрить специализированный программно-аналитический комплекс (СПАК).

СПАК призван выполнять следующие основные функции:

1. Автоматизированный сбор цифровых доказательств, т.е. выявление, фиксация и изъятие цифровых следов, оставленных на различных электронных носителях (компьютеры, мобильные устройства, серверы, облачные хранилища).

2. Аналитическая обработка информации. Использование алгоритмов и искусственного интеллекта для систематизации и интерпретации собранных данных, выявления закономерностей, связей и схем преступной деятельности.

3. Хранение и управление базами данных цифровых следов. Создание централизованного хранилища данных о типовых цифровых следах, характерных для конкретных видов киберпреступлений, и оперативный доступ к ним.

4. Формирование и автоматическое оформление экспертных заключений, т.е. автоматизация подготовки экспертных отчетов, соответствующих установленным стандартам и требованиям уголовно-процессуального законодательства Республики Казахстан.

5. Мониторинг и обновление методик. Регулярное обновление используемых программных решений и методических подходов на основе анализа новых угроз и передового международного опыта.

Практическое применение. Практическое применение СПАК будет реализовано на базе Центра судебных экспертиз Министерства юстиции

Республики Казахстан, в специализированном отделе по расследованию киберпреступлений и информационной безопасности. Данное учреждение имеет необходимую инфраструктуру и полномочия для проведения судебных экспертиз в сфере информационных технологий.

Также имеется альтернатива в будущем СПАК можно будет применять в предложенном нами ранее новом Национальном центре управления кибербезопасностью и цифровой криминалистики.

СПАК будет включать следующие элементы (оборудование):

- Мощные серверы с высокой вычислительной производительностью для обработки больших массивов цифровых данных.
- Рабочие станции криминалистов с предустановленным специализированным программным обеспечением для анализа цифровых доказательств (например, FTK, EnCase, X-Ways Forensics).
- Устройства для извлечения данных с электронных носителей (физические извлекатели, программно-аппаратные комплексы типа Cellebrite UFED).
- Высокоскоростные системы хранения данных (SAN/NAS) для создания резервных копий и хранения цифровых доказательств.

Специалисты, осуществляющие работу СПАК:

- Судебные эксперты в области компьютерно-технических исследований и кибербезопасности.
- Следователи с профильным образованием и дополнительной специализацией по цифровой криминалистике.
- Технические специалисты, отвечающие за поддержку и обновление программного обеспечения и оборудования.

Способы и методы применения СПАК:

- На первоначальном этапе следователь или эксперт посредством СПАК проводит первичную обработку цифровых носителей, используя специализированные программные средства для выявления, извлечения и фиксации цифровых следов.
- Далее полученные данные направляются на серверную инфраструктуру, где проводится углубленный анализ с использованием алгоритмов искусственного интеллекта для выявления скрытых взаимосвязей и закономерностей.
- Результаты анализа автоматически формируются в экспертные заключения с указанием конкретных действий, фактов и рекомендаций для дальнейших следственных мероприятий.

Этапы внедрения и профессиональной подготовки:

- Подбор, обучение и сертификация экспертов и следователей на специализированных курсах, организованных Центром судебных экспертиз совместно с ведущими международными центрами подготовки специалистов по цифровой криминалистике.

Джилкишиев Р.Б.

- Проведение регулярных тренингов и мастер-классов с целью обновления знаний и навыков персонала, а также внедрения новых методик и технологий в области криминалистического анализа цифровых данных.

Практическое применение предлагаемого комплекса позволит существенно повысить качество и оперативность расследования киберпреступлений. Его использование обеспечит высокую степень достоверности и доказательной значимости собранных цифровых улик, а также создаст возможность быстрого реагирования на новые виды преступных проявлений в цифровой среде.

Введение СПАК в повседневную работу правоохранительных органов и судебно-экспертных учреждений обеспечит:

- Сокращение сроков расследования преступлений за счет ускорения процедуры сбора и анализа цифровых доказательств.
- Повышение квалификации следователей и экспертов, обеспечивающих расследование преступлений в сфере информационных технологий.
- Улучшение межведомственного и международного взаимодействия при расследовании трансграничных киберпреступлений.

Рассмотренные в этом подразделе методы и способы расследования преступлений, позволит значительно улучшить качество работы правоохранительных органов Республики Казахстан, адаптировать криминалистические методики к современным вызовам цифровой эпохи и обеспечить эффективную защиту информационной безопасности государства и общества.

Джилкишиев Р.Б.

1.4 Международный опыт в противодействии киберпреступности

Современные угрозы в сфере киберпреступности приобретают выраженный транснациональный характер, затрагивая практически все страны мира и демонстрируя устойчивую тенденцию к дальнейшему росту сложности и масштабов. В условиях активного расширения информационно-коммуникационных технологий и цифровизации жизненно важных сфер общества традиционные методы противодействия преступности уже не способны обеспечить адекватную защиту от стремительно эволюционирующих угроз. В связи с этим важнейшей задачей становится изучение и заимствование положительного международного опыта, накопленного странами, которые достигли значительных успехов в области противодействия киберпреступности.

Мировой опыт показывает, что эффективное противодействие цифровым угрозам достигается за счет объединения усилий на национальном и международном уровнях посредством создания специализированных структур и центров, которые централизованно координируют борьбу с киберугрозами. В различных странах функционируют специализированные национальные центры кибербезопасности и цифровой криминалистики, обладающие широкими полномочиями и разветвленными сетями взаимодействия с правоохранительными органами, разведслужбами, частным сектором и международными партнерами.

В рамках настоящего подраздела исследуются структуры, подходы и практические методы работы специализированных центров кибербезопасности в различных странах и международных организациях. Анализируется опыт реализации комплексных национальных программ, внедрение передовых технологий и современных инструментов цифровой криминалистики. Особое внимание уделяется международному взаимодействию и обмену информацией, которые становятся ключевыми факторами успешного противодействия трансграничной киберпреступности. Исследование позволяет не только оценить эффективность существующих подходов, но и сформулировать рекомендации по созданию аналогичной структуры в Республике Казахстан с учетом накопленных международных практик.

Таким образом, цель данного подраздела заключается в выявлении наиболее эффективных международных практик противодействия киберпреступности, которые могут быть адаптированы и успешно применены в законодательстве и правоприменительной деятельности Республики Казахстан. Достижение указанной цели позволит повысить уровень национальной кибербезопасности, обеспечить надежную защиту критически важных инфраструктурных объектов и информационных ресурсов, а также укрепить позиции страны в глобальном информационном пространстве.

Многие страны и организации создали специализированные центры для координации кибербезопасности. Такие центры действуют на национальном уровне, в формате международных платформ, а также как публично-частные

Джилкишиев Р.Б.

партнерства. Ниже рассматриваются примеры подобных центров в различных странах с указанием их статуса, задач, методов работы и достигнутых результатов.

В Великобритании действует **Национальный центр кибербезопасности, The National Cyber Security Centre (далее – NCSC).** Статус и структура: Национальный центр кибербезопасности Великобритании (NCSC) создан в 2016 году в составе Центра правительственной связи (GCHQ) как единый технический авторитет страны в сфере киберугроз. Он объединяет ранее разрозненные структуры (включая CESG – службу информационной безопасности GCHQ, национальный CERT-UK и др.) для централизованного управления кибербезопасностью государства. NCSC является государственным учреждением, подотчетным разведывательному ведомству GCHQ, и фактически служит «лицом» этой службы для взаимодействия с гражданским сектором [62].

Цели и функции. Основная миссия NCSC – делать Великобританию наиболее безопасным местом для жизни и работы в сети. Центр выступает техническим лидером по киберинцидентам, отвечая за мониторинг и реагирование на кибератаки, защиту критически важных сервисов, а также за консультирование правительства и бизнеса по вопросам безопасности. NCSC выполняет роль национальной команды реагирования на инциденты (CSIRT): отслеживает киберинциденты, обеспечивает раннее предупреждение, проводит анализ угроз, выпускает технические рекомендации для организаций и координирует реагирование на крупные атаки. Одновременно NCSC назначен национальной точкой контакта (SPOC) по директиве ЕС NIS, что означает координацию обмена информацией о инцидентах с центрами других стран [63]. Центр активно взаимодействует с частным сектором и населением: предоставляет единый пункт контакта для бизнеса, включая малые предприятия и граждан по вопросам кибербезопасности [64]. Он также ведет просветительскую работу и публикует отчеты о киберугрозах. Например, NCSC ежегодно выпускает отчет «Annual Review», где анализирует тенденции; в отчете за 2024 год отмечено, что с сентября 2023 по август 2024 центр обработал 89 киберинцидентов национального значения [65, p. 17] – то есть наиболее серьезных атак, представляющих угрозу государственным интересам.

Полномочия и направления работы. NCSC обладает полномочиями рекомендательного и технического характера, в отличие от правоохранительных органов, он не проводит уголовных расследований. Его ключевые направления – это защита правительственных и ведомственных сетей, поддержка критической инфраструктуры (энергетика, транспорт, связь и т.д.), реагирование на кибератаки против британских организаций, анализ вредоносного ПО и новое направление – активная киберзащита. В рамках программы Active Cyber Defence центр внедряет проактивные меры, например фильтрацию фишинговых писем, блокировку вредоносных доменов и др. Также NCSC тесно сотрудничает с правоохранительным Национальным центром по

борьбе с киберпреступностью NCCU в составе Национального криминального агентства, передавая техническую информацию для уголовных расследований.

Методы и технологии. В работе NCSC опирается на передовые технологии анализа угроз. Центр собирает сведения о миллионах киберинцидентов и индикаторов компрометации по всем секторам, используя для этого национальные платформы обмена информацией, например, CiSP – платформа обмена кибербезопасной информацией между промышленностью и правительством. NCSC выпускает автоматизированные сигнатуры и предупреждения о выявленных уязвимостях. Совместно с партнерами NCSC развивает руководство по безопасности новых технологий, примером служит совместная публикация NCSC, ФБР и CISA по требованиям цифровой криминалистики и мониторинга для сетевых устройств, чтобы улучшить сбор цифровых доказательств в расследованиях [66]. Также центр использует элементы искусственного интеллекта для обработки больших потоков данных об угрозах и аномалиях, помогая прогнозировать атаки. Благодаря таким методам, NCSC еженедельно предотвращает множество попыток атак на государственные сети и сайты, о чем регулярно отчитывается в своих обзорах.

За первые годы работы NCSC зарекомендовал себя как эффективный координационный центр. С момента основания в 2016 году он обработал сотни значимых инцидентов, из них только за последний год – 89 крупнейших атак [65, p.17] По данным правительства, благодаря деятельности NCSC доля британских организаций, пострадавших от киберинцидентов, начала сокращаться с 46% в 2017 году до 32% в 2023 году, хотя в 2024 году наблюдался рост до 50% из-за улучшения выявляемости угроз [65, p.15,18]. NCSC успешно реализовал программы по удалению фишинговых сайтов, в результате чего тысячи мошеннических ресурсов были заблокированы, и запустил «Early Warning Service» для оповещения компаний о признаках компрометации [67]. К концу 2024 года центр объединял усилия сотен экспертов и наладил сотрудничество с десятками отраслевых организаций, сделав защиту киберпространства Великобритании более централизованной и действенной.

В США отсутствует единый «национальный киберцентр» в виде отдельного юридического лица, однако функцию центра управления кибербезопасностью выполняет **Национальный центр интеграции кибербезопасности и коммуникаций, The National Cybersecurity and Communications Integration Center** (NCCIC) в составе Агентства по кибербезопасности и безопасности инфраструктуры (CISA) при Министерстве внутренней безопасности [68]. NCCIC был создан для объединения под одной крышей нескольких подразделений, национальной команды реагирования US-CERT, специализированного центра по промышленным системам ICS-CERT, центра координации телекоммуникаций и др.. Он действует как федеральный центр обмена информацией и реагирования на киберугрозы, располагаясь в структуре государственной службы (CISA/DHS). Помимо DHS, в национальную киберзащиту США активно вовлечены и другие ведомства,

Министерство обороны, включая Киберкомандование США и Центр киберпреступлений Министерства обороны DC3, Министерство юстиции, ФБР и др., однако NCCIC служит главным узлом для связи с частным сектором и координации общенациональных ответных мер.

NCCIC провозглашен национальным координационным центром по кибербезопасности. Его миссия – сокращение вероятности и ущерба от киберинцидентов против критически важных сетей и коммуникаций страны. Центр круглосуточно отслеживает кибератаки и аномальные события на федеральных, государственных и коммерческих системах, обеспечивая ситуационную осведомленность о возникающих угрозах и инцидентах. Он служит центром обмена информацией с частным сектором, через NCCIC правительство и компании обмениваются предупреждениями о уязвимостях, индикаторами атак, тактикой злоумышленников. Центр также предоставляет техническую помощь и выездную поддержку организациям-жертвам, специалисты NCCIC могут на месте проводить анализ инцидента, помогать в устранении последствий атак и восстановлении систем. Во время крупных киберинцидентов, затрагивающих критическую инфраструктуру, NCCIC координирует национальный межведомственный ответ и информирует руководство страны о статусе инцидента. Таким образом, NCCIC играет ключевую роль в реализации Национального плана реагирования на киберинциденты США.

NCCIC не является силовым органом, но тесно взаимодействует с правоохранителями и спецслужбами. Через него осуществляется обмен разведданными о киберугрозах между DHS, АНБ/Киберкомандованием, ФБР и другими структурами. В частности, при NCCIC действует Национальная межведомственная группа по кибератакам (NCIJTF) под эгидой ФБР – совместный штаб, куда стекается информация для расследования хакерских кампаний. Сам NCCIC объединяет четыре ветви, включая US-CERT (координация инцидентов в гражданском секторе) и ICS-CERT (реагирование на инциденты в системах промышленного управления). Благодаря этому центр располагает специализированными экспертами по разным направлениям. Так, аналитики ICS-CERT в рамках NCCIC проводят цифровую криминалистику на критических объектах, включая анализ вредоносных программ для АСУ ТП, исследование образов дисков и сетевого трафика при инцидентах на промышленности. Они же занимаются выявлением уязвимостей в системах управления и координируют их закрытие совместно с производителями оборудования. NCCIC также сотрудничает с региональными оперативными центрами и центрами обмена и анализа информации (ISAO/ISAC) в отраслях – через них он рассылает оповещения и лучшие практики защиты [69].

Для мониторинга угроз NCCIC эксплуатирует национальные сенсорные сети и платформы обмена данными. Например, действует автоматизированная система EINSTEIN для обнаружения вторжений в федеральных сетях, данные которой поступают в NCCIC. Центр применяет технологии глубокой аналитики больших данных и машинного обучения для выявления сложных атак,

Джилкишиев Р.Б.

анализируя миллиарды сетевых событий. При разборе инцидентов используются современные инструменты цифровой криминалистики, средства восстановления данных, реверс-инжиниринга вредоносного ПО, анализаторы сетевых пакетов. Важным направлением работы NCCIC является информационный обмен, через защищенный портал, на базе платформы HSIN участники получают уведомления об индикаторах компрометации, могут сообщать о атаках и запрашивать помощь экспертов. Центр выпускает регулярные бюллетени о выявленных уязвимостях, иногда совместно с партнерами из других стран – например, совместные предупреждения CISA, ФБР и британского NCSC о глобальных киберугрозах. Кроме того, NCCIC разрабатывает наборы методических пособий и плейбуков по реагированию на кибератаки для федеральных агентств, стандартизируя подходы к расследованию инцидентов [70].

Деятельность NCCIC существенно повысила готовность США к киберинцидентам. Ежегодно через центр проходят тысячи уведомлений об атаках; так, только за 2020 год NCCIC получил и обработал до 100 тысяч сообщений об инцидентах от различных источников, по данным CISA. Многие из них решаются на уровне консультаций, а наиболее серьезные (сотни в год) требуют активного вмешательства. В 2019 году конгресс принял закон, закрепляющий за NCCIC группу быстрого реагирования (CyTRT) для оказания неотложной помощи при критических кибератаках [71]. Через механизм обмена информацией с частным сектором, программы добровольного шеринга NCCIC распространил сотни предупреждений, позволивших компаниям предотвратить атаки. Тесная координация внутри страны и с союзниками позволила пресечь ряд крупных кампаний, например, совместно с ФБР и международными партнерами были ликвидированы ботнеты Avalanche, Emotet и др.. Таким образом, США выстроили децентрализованную, но интегрированную систему, в которой NCCIC/CISA играет центральную организационную роль в кибербезопасности на национальном уровне.

В Канаде задействован **Канадский центр кибербезопасности, Canadian Centre for Cyber Security** (далее – CCCS, или просто Cyber Centre) – ведущий национальный орган Канады по вопросам кибербезопасности, созданный в 2018 году в рамках национальной киберстратегии. Он функционирует как подразделение Центра безопасности коммуникаций (CSE) – канадской службы крипто- и киберразведки [72]. Таким образом, центр имеет государственный статус и пользуется техническими возможностями и кадровым потенциалом CSE. Создание CCCS объединило разбросанные ранее функции из трех ведомств, CSE, Министерство общественной безопасности и Shared Services Canada в единую организацию [73]. Штат центра насчитывает несколько сотен сотрудников, около 300 на момент запуска, включая экспертов в области киберзащиты, аналитиков разведданных, специалистов по цифровой криминалистике и оперативных связистов. Центр расположен в Оттаве и отвечает перед Минобороны через CSE, однако обслуживает весь федеральный аппарат и сотрудничает с провинциями и частным сектором.

Cyber Centre обозначает своей миссией защиту информации и систем, на которых держится повседневная жизнь канадцев. Он выступает техническим авторитетом Канады по кибербезопасности и возглавляет федеральное реагирование на киберинциденты. Основные функции CCCS включают:

1) защиту государственных киберсистем – центр развертывает передовые решения киберзащиты для правительственных сетей и отвечает за их кибероборону, пользуясь преимуществами своего положения внутри спецслужбы CSE, например, доступом к уникальной разведывательной информации;

2) информирование – предоставление надежных консультаций и руководств по кибербезопасности для всех секторов Канады. Центр публикует подробные рекомендации, проводит общенациональные кампании повышения осведомленности «Get Cyber Safe» и консультирует критически важные отрасли, финансы, телеком, энергетику и т.д. по укреплению защиты;

3) расширение возможностей (empowerment) – укрепление общей киберустойчивости Канады через партнерства, инновации и обучение. CCCS разрабатывает собственные инструменты киберзащиты и делится ими с партнерами, создает совместные исследовательские проекты с вузами и отраслью, устраивает учения и тренинги. Центр позиционирует себя как национальный CSIRT Канады, он выполняет роль CERT-CA и координатора инцидентов для федерального правительства, взаимодействуя со всеми уровнями власти и международными коллегами для смягчения и ликвидации последствий кибератак [7].

CCCS обладает широкими полномочиями по сбору и анализу технической информации о угрозах. Будучи частью CSE, он может получать данные по зарубежным источникам кибератак (SIGINT-разведка) и обмениваться ими в рамках разведсообщества, но его деятельность сфокусирована на защите внутренних систем. Центр служит технической опорой для правоохранительных органов, по сложным инцидентам, связанным с киберпреступностью, он оказывает экспертную поддержку Королевской канадской конной полиции (далее – RCMP) и другим агентствам. В частности, CCCS тесно сотрудничает с созданным при RCMP Национальным координационным центром по киберпреступности (NC3), выполняя роль единого источника технической экспертизы для следователей и спецслужб. Это означает, что при расследовании киберпреступлений, например, сетевого мошенничества, атак на банки, эксперты Cyber Centre помогают проводить цифровую криминалистику, анализируют вредоносное ПО, атрибуцию атак, собирают цифровые доказательства, необходимые для предъявления обвинений. Одновременно центр сам не является правоохранительным органом и не имеет мандата на аресты – все такие действия осуществляются RCMP, а CCCS поддерживает их технически. Кроме того, Cyber Centre координирует взаимодействие правительства с телекоммуникационными операторами и интернет-провайдерами в области кибербезопасности, выступая единым

Джилкишиев Р.Б.

каналом связи. К примеру, при распространении индикаторов угроз или при сообщении об инцидентах на критических объектах [74].

Cyber Centre применяет многослойный подход. Для мониторинга сетей федеральных органов центр использует средства обнаружения атак (системы IDS/IPS), установленные на узлах связи ведомств, и аналитику сетевого трафика. При выявлении инцидентов он задействует процедуры инцидент-менеджмента, описанные в национальных планах. Важная технология в распоряжении центра – платформа Assemblyline, разработанная CSE, которая автоматизирует анализ вредоносных файлов и позволяет быстро сортировать большие потоки подозрительных объектов с помощью машинного обучения. Это помогает выявлять новые образцы малвари и связывать их с известными кампаниями. Также CCCS активно использует облачные инструменты анализа и песочницы для динамического изучения вредоносных программ. Для обмена информацией с промышленностью запущена защищенная система сотрудничества, предоставляющая общий пул данных об угрозах. Cyber Centre практикует публично-частные учения, например, в 2021 году он организовал упражнение по сценарию массового киберинцидента с участием 50 организаций, отрабатывая совместное реагирование. С точки зрения цифровой криминалистики, центр располагает современной лабораторией, инструментарий включает средства восстановления данных из различных устройств, анализаторы сетевых логов, утилиты декодирования трафика TOR и криптовалютных транзакций. Методологически CCCS выпускает подробные отчеты об угрозах – так, с 2018 года издается несекретный «Национальный обзор угроз» (National Cyber Threat Assessment), в котором обобщаются данные разведки и статистика киберинцидентов для бизнеса и населения [75].

Согласно отчету CCCS за 2021 год, центр зафиксировал 235 инцидентов с программами-вымогателями в период с 1 января по 16 ноября 2021 года. Более половины этих инцидентов были направлены против критически важной инфраструктуры, включая здравоохранение, энергетику и производство. CCCS активно участвует в международных инициативах по борьбе с программами-вымогателями, включая участие в международной рабочей группе по программам-вымогателям, координируемой Институтом безопасности и технологий (Institute for Security and Technology) в США. В отчете «National Cyber Threat Assessment 2023–2024» CCCS отмечает, что программы-вымогатели остаются одной из основных киберугроз для Канады, особенно для критически важной инфраструктуры [76].

Благодаря усилиям Cyber Centre, Канада повысила свой уровень готовности, международные индексы кибербезопасности, например, Global Cybersecurity Index отмечают Канаду в числе лидеров. Центр наладил обмен информацией с более чем 50 иностранными партнерами и вступил в глобальные инициативы, такие как сеть CSIRT Global. Таким образом, в Канаде сформирована надежная национальная площадка, сочетающая функции кибер разведки, оперативного реагирования и цифровой криминалистической поддержки правоохранителей.

Джилкишиев Р.Б.

Австралийский центр кибербезопасности, Australian Cyber Security Centre (далее – ACSC) - главный координационный центр кибербезопасности Австралии. Он был создан в ноябре 2014 года на базе предыдущего Центра операций кибербезопасности (CSOC) при Австралийском управлении сигналов (ASD). ACSC является частью структуры ASD, разведывательного ведомства в составе Министерства обороны, что схоже с моделью Великобритании и Канады, где центры кибербезопасности встроены в национальные спецслужбы. В 2018 году роль ACSC была расширена и укреплена, центр получил отдельный статут в рамках реформ ASD, а руководитель ACSC стал подчиняться непосредственно директору ASD и министру обороны. ACSC расположен в Канберре и действует как интеграционная площадка, куда входят представители нескольких агентств. Помимо экспертов ASD, там работают аналитики стратегической киберразведки из Управления оборонной разведки, специалисты по цифровой криминалистике Федеральной полиции Австралии (AFP), сотрудники Австралийской организации по безопасности связи (ASIO) и Австралийской комиссии по криминальной разведке (ACIC). Этот агентский состав обеспечивает комплексный подход – от разведки и защиты до уголовного преследования. ACSC находится под совместным надзором Оперативного совета по кибербезопасности и курируется министром обороны Австралии [77].

ACSC является ведущим органом правительства Австралии по улучшению кибербезопасности страны. Его ключевые задачи:

1) возглавлять оперативное реагирование на кибератаки – центр координирует действия всех госструктур при крупных инцидентах, обеспечивая единый фронт защиты;

2) организовывать национальные ресурсы и операции в киберпространстве – ACSC распределяет роли и средства между обороной, правоохранителями и гражданскими ведомствами для противодействия угрозам;

3) получать и стимулировать отчетность об инцидентах – центр управляет системой добровольного сообщения о киберинцидентах в портале Report Cyber, призывая бизнес и граждан уведомлять о киберпреступлениях, и обрабатывает эти сигналы;

4) повышать осведомленность об уровне киберугроз – через публичные отчеты, рекомендации для предприятий и просветительские кампании ACSC информирует общество о актуальных киберрисках;

5) изучать и расследовать киберугрозы – специалисты центра проводят анализ новых видов атак, угроз национальной безопасности в киберсфере, исследуют вредоносные инструменты, чтобы предупреждать возможные будущие атаки. Таким образом, ACSC сочетает функции национального информационного и аналитического центра киберразведки [78].

ACSC интегрирует все национальные кибервозможности из разных агентств. Это позволило сконцентрировать под одной крышей экспертов из областей, таких как кибертехнической защиты, разведывательного анализа,

Джилкишиев Р.Б.

цифровой криминалистики, оперативного реагирования и разработки политики. Например, присутствие в ACSC сотрудников Федеральной полиции означает, что при центре действует команда по борьбе с киберпреступностью (сотрудники полиции), которая может сразу инициировать расследование и уголовное преследование злоумышленников, опираясь на технические данные ACSC. Центр наделен полномочиями давать рекомендации органам власти и частному сектору по усилению защиты, а также выступать посредником между бизнесом и правительством в кризисных ситуациях. Одно из ключевых направлений – защита критической инфраструктуры. ACSC курирует программы кибербезопасности в энергетике, транспорте, финансах, для чего выстроил партнерство с операторами инфраструктуры. Также центр отвечает за кибербезопасность государственных служб – устанавливает стандарты, проводит киберучения среди агентств, осуществляет мониторинг ведомственных сетей совместно с ASD. В рамках общефедеральной стратегии ACSC руководит сетью Объединенных центров кибербезопасности (JCSC) – региональных хабов в крупнейших городах Сиднея, Мельбурна и других городов Австралии, где представители бизнеса и властей совместно обсуждают угрозы и обмениваются информацией [79]. Эти объединенные центры являются продлением ACSC «в поле», укрепляя публично-частное взаимодействие. В области цифровой криминалистики специалисты центра вместе с полицией расследуют значимые киберинциденты. Например, крупные взломы данных или атаки, обеспечивая анализ цифровых доказательств, необходимый для поимки и привлечения преступников [80].

Австралийский центр кибербезопасности известен внедрением передовых подходов к реагированию. Одной из особенностей является разведывательно-аналитический фокус, используя возможности ASD, центр получает ранние предупреждения об угрозах из глобальных источников и быстро делится ими с внутренними потребителями. Технически ACSC применяет средства мониторинга интернет-трафика, в рамках законодательно разрешенных пределов и сотрудничает с телекоммуникационными компаниями для отслеживания ботнет-активности. В аналитической работе центр активно пользуется блокчейн-аналитикой при расследовании преступлений с криптовалютами, применяет инструменты на основе ИИ для обработки большого числа инцидент-репортов, поступающих через Report Cyber. Количество таких обращений велико – примерно одно сообщение каждые 8 минут, поэтому автоматизация критична. Для взаимодействия с бизнесом ACSC создал Партнерскую программу, более 4000 организаций-партнеров подключены к платформе центра и регулярно получают уведомления о текущих киберугрозах и уязвимостях. В плане цифровой криминалистики центр имеет лабораторию, оснащенную современными средствами анализа, это и программно-аппаратные комплексы для вскрытия мобильных устройств, и инструменты восстановления данных из облачных сервисов, и специализированные решения для анализа вредоносного ПО, например, Cuckoo Sandbox для динамического анализа. ACSC совместно с NCSC

(Великобритания) разрабатывал рекомендации по встроенным средствам аудита и логирования для сетевых устройств, чтобы облегчить последующую криминалистическую проверку инцидентов [81]. Такие инициативы указывают на стремление центра улучшить методы сбора и обмена доказательствами в международном масштабе.

Австралийский центр кибербезопасности продемонстрировал заметные успехи. Согласно отчету об угрозах за 2020–21 гг., ACSC получил 67 500 заявлений о киберпреступлениях и зафиксировал рост вымогательских атак на 15%. Благодаря налаженному взаимодействию с телеком-операторами, центр совместно удалил свыше 110 злонамеренных веб-сайтов, связанных с COVID-19 мошенничеством, защитив граждан в разгар пандемии. В ходе реагирования ACSC оказал поддержку по меньшей мере 1630 инцидентам разной степени серьезности за год – от консультирования пострадавших до непосредственного участия в техническом устранении последствий. Примерно 25% серьезных инцидентов затронули критические организации, и новые властные полномочия позволили ACSC напрямую вмешиваться для помощи этим объектам. Центр также активно ведет наступательные операции в киберпространстве, по заявлению правительства, киберподразделение ASD, которое тесно связано с ACSC, провело ряд наступательных кибероперации против преступных группировок, угрожающих Австралии. Кроме того, ACSC реализует киберучения, за отчетный период проведено 18 крупных учений с участием 50 организаций для повышения готовности [82]. Все это позволило Австралии укрепить свою национальную киберзащиту и более эффективно пресекать цифровые преступления, опираясь на работу ACSC как центрального звена.

Европейский Союз и Европейский центр по борьбе с киберпреступностью (далее – EC3, Европол). Страны Европы также выстроили развитую систему противодействия киберпреступности, значительную роль в которой играет Европейский Союз. Правовая база ЕС ориентирована на гармонизацию законодательств государств-членов в соответствии с лучшими международными практиками. Ключевым актом является Директива 2013/40/ЕС «О атаках на информационные системы», которая заменила Рамочное решение 2005/222/JHA и обязала все страны ЕС криминализировать хакерские атаки, создание и распространение вредоносных программ, деятельность ботнетов и прочее [83]. Дополнительно в ЕС приняты директивы, касающиеся борьбы с детской порнографией и эксплуатацией детей в интернете (2011/92/ЕС), а также с мошенничеством с платежными средствами (резолюция 2022/1227) и другие. Эти нормативные акты обеспечивают единые минимальные стандарты уголовной ответственности и процессуальных полномочий. Например, возможность изъятия компьютерных данных, транскордонного доступа к сохраненным данным и т.п. на всем пространстве Евросоюза. Параллельно, практически все страны ЕС стали участниками Будапештской конвенции Совета Европы, ее ратифицировали 27 из 28 государств ЕС, за исключением Ирландии, которая подписала, но пока не ратифицировала конвенцию [84]. Таким образом, материальное право и

процессуальные механизмы противодействия киберпреступности в Европе в значительной степени унифицированы.

В настоящее время в ЕС действует Европейский центр по борьбе с киберпреступностью при агентстве правоохранительных органов ЕС Европол. EC3 начал работу 1 января 2013 года и расположен в Гааге (Нидерланды). Это межгосударственная платформа в рамках ЕС, финансируемая из бюджета Европола и подотчетная государствам-членам Евросоюза. Центр создан по инициативе Еврокомиссии как ответ на рост трансграничной киберпреступности, выходящей за рамки возможностей отдельных стран. Штат EC3 изначально составлял 30 сотрудников, план расширения до 40 к концу 2013 годаи имел бюджет около €3,6 млн; сейчас он вырос, включая офицеров связи от разных стран. Центр возглавляется директором, подчиняющимся главе Европола. Внутренняя структура EC3 подразделяется на отделы по ключевым направлениям киберпреступности и на аналитико-технические подразделения (лаборатория цифровой криминалистики, отдел стратегического анализа и т.д.) [85].

Миссия EC3 – укреплять способность правоохранительных органов стран ЕС противодействовать киберпреступности через совместные действия. Его задача – стать центральной точкой координации борьбы с киберпреступностью в Европе. Мандат EC3 охватывает три основных области:

1) Атаки организованных криминальных групп в киберсфере, особенно преследующих финансовую выгоду, например, кражи платежных данных, банковские трояны, мошенничество.

2) Киберпреступления, причиняющие серьезный вред жертвам, прежде всего онлайн-эксплуатация детей и распространение материалов с детской порнографией.

3) Кибератаки на критическую инфраструктуру и информационные системы ЕС, сюда входят сложные хакерские атаки, диверсии против важных систем.

Таким образом, EC3 фокусируется не только на «классических» киберпреступлениях, таких как мошенничества, взломы ради денег, но и на наиболее опасных преступлениях против личности и систем жизнеобеспечения. Центр призван противодействовать и нарушать деятельность организованных сетей киберпреступников, которые несут основную ответственность за тяжкие киберпреступления в Европе [86].

EC3 не обладает собственными полномочиями следствия или ареста – эти действия остаются за национальными правоохранительными органами стран. Однако EC3 координирует расследования и операции, объединяя усилия разных государств. Он предоставляет странам-членам оперативную и аналитическую поддержку. Например, может обрабатывать большие объемы цифровых доказательств, проводить расшифровку данных или анализ сетевых логов для национальных полиций. В Европоле действует зашифрованная платформа для обмена информацией об уголовных делах, и EC3 обеспечивает через нее «secure outreach platform» для обмена стратегическими сведениями и

лучшими практиками между правоохранителями ЕС. Важнейшая функция EC3 – криминалистическая и техническая экспертиза, центр располагает собственным «Digital Forensics Lab», оснащенным современными средствами анализа носителей и вредоносных программ, где эксперты могут извлекать и обрабатывать данные с изъятых устройств, взламывать шифрование, анализировать ботнет-трафик и т.д. Европол позволяет странам, не имеющим достаточных ресурсов, использовать эти возможности EC3. Также EC3 стал площадкой для формирования совместных оперативных групп. В 2014 году на его базе создана группа J-CAT (Joint Cybercrime Action Taskforce) – постоянная команда офицеров из различных стран, включая представителей США, Великобритании, Германии и др., работающих бок о бок над наиболее сложными международными киберделами. Кроме того, EC3 активно взаимодействует не только с полицией, но и с другими субъектами, национальными центрами по противодействию киберпреступности, международными организациями (Интерпол, НАТО), частным сектором и научным сообществом. Он выстроил партнерства с ИТ-компаниями и банковским сектором, которые нередко предоставляют данные и экспертизу, например, информация от компаний о мошеннических транзакциях помогает EC3 начинать расследования. Важное направление – повышение квалификации, EC3 проводит тренинги для следователей из стран ЕС, организует совместные учебные мероприятия, выпустил ряд методических материалов, например, пособия по расследованию киберпреступлений, рекомендации по лучшим технологиям.

В своем распоряжении EC3 имеет ряд специализированных инструментов. Для анализа больших данных о киберпреступности центр использует систему «FP Cyborg», куда аккумулируются разрозненные данные расследований из всех стран ЕС, позволяя выявлять связи между делами, совпадение IP-адресов, криптовалютных кошельков и т.д. Лаборатория EC3 оснащена аппаратно-программными комплексами для взлома зашифрованных носителей, в том числе крупными вычислительными мощностями для атаки перебором паролей. В сотрудничестве с частными компаниями центр применяет сети телеметрии - данные антивирусных вендоров для отслеживания ботнетов и скоординированного их отключения. Одним из методов стало создание «летучих отрядов» экспертов, по заявлению первого руководителя EC3, центр может направлять в страну команду специалистов с мобильным оборудованием – своего рода «кибернетический спецназ» – для немедленного содействия на месте при крупном инциденте. Кроме того, EC3 развивает инновационные подходы, запланировано создание «Cyber Innovation Room» – лаборатории для испытания новых технологий расследования и моделирования сценариев кибератак. В области информационного обмена EC3 запустил ежегодный Отчет об угрозах организованной киберпреступности (IOCTA) – подробный аналитический доклад о ключевых трендах, видах атак и прогнозах, основанный на данных всех государств ЕС. Данный отчет стал авторитетным источником для выработки политики ЕС в сфере кибербезопасности [87].

Джилкишиев Р.Б.

За годы работы EC3 добился значимых успехов в совместных операциях. С его координацией проведено множество международных операций против киберпреступников. Например, в 2021 году под эгидой EC3 состоялась операция GoldDust/Quicksand – одновременные аресты в нескольких странах членов банды, распространявшей вирус-вымогатель REvil/Sodinokibi, что стало большим ударом по программам-вымогателям. Ранее в рамках Operation Talpa совместно с ФБР и 16 странами был ликвидирован крупный ботнет, причастный к рассылке вымогателей [88]. Всего EC3 отчитывается о десятках успешных операций против сетей вымогателей, торговцев данными и хакерских сервисов. В 2022 г. Европол через EC3 координировал операцию Tourniquet, в результате которой был закрыт один из крупнейших криминальных онлайн-форумов Raid Forums и блокирована его инфраструктура [89]. Эта операция объединила правоохранителей США, Великобритании, Швеции, Португалии и Румынии. Ежегодно EC3 публикует показатели, так, только за 2020 год при поддержке EC3 было арестовано более 100 киберпреступников и начато свыше 300 международных расследований, изъято криптовалюты и активов на миллионы евро. Помимо операций, EC3 поднял уровень экспертизы, более 500 сотрудников правоохранительных органов прошли обучение на курсах центра за первые пять лет. EC3 стал центром компетенций ЕС, его аналитики помогают в выработке новых законов, такие как директивы по борьбе с мошенничеством и абьюзом детей онлайн, а сам факт его существования существенно упростил обмен данными между странами. Сегодня EC3 – признанный пример эффективной межгосударственной платформы цифровой криминалистики и кибербезопасности.

Россия и государства СНГ. Российская Федерация обладает развитой законодательной и организационной системой борьбы с преступлениями в сфере информационных технологий. Уголовный кодекс РФ включает специальные статьи, в том числе ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ст. 273 УК РФ (создание, распространение и использование вредоносных программ), ст. 274 и 274.1 УК РФ (нарушение правил эксплуатации средств хранения и обработки информации, злоупотребления в сфере критической инфраструктуры) и др. Кроме того, применяются общие нормы о мошенничестве, если деяние совершено с использованием электронных средств, это рассматривается как отягчающее обстоятельство, например в ст. 159.6 УК о мошенничестве в сфере компьютерной информации. Для расследования таких преступлений в системе МВД России созданы специализированные подразделения, ранее известные как «Управление К», которые имеются в Главном управлении уголовного розыска и территориальных органах. Также ФСБ России ведет работу по пресечению кибератак, затрагивающих критическую информационную инфраструктуру и государственные информационные системы, в рамках обеспечения информационной безопасности. В 2018 году в РФ была утверждена доктрина информационной безопасности, где киберпреступность названа одним из

существенных вызовов национальной безопасности, а среди приоритетов – развитие международного сотрудничества с упором на защиту суверенитета информационного пространства.

При этом Россия не присоединилась к Будапештской конвенции о киберпреступности, официально мотивируя это несоответствием ее положений принципу государственного суверенитета. Российские представители указывают, что Конвенция позволяет иностранным правоохранительным органам действовать на территории государства, напрямую обращаться к провайдерам или сохранять данные без достаточного контроля со стороны национальных властей, что неприемлемо для РФ [90]. В результате Россия исторически воздерживалась от участия в механизмах Будапештской конвенции и даже не использовала неформальные возможности сотрудничества по ее линии. Вместо этого Россия выступила инициатором разработки нового глобального договора под эгидой ООН. Одновременно РФ активно развивает взаимодействие в рамках региональных организаций. Так, еще в 2001 году государства СНГ заключили Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, предусмотрев обмен информацией, совместные оперативные мероприятия и правовую помощь между правоохранительными органами Содружества. В 2018 году в рамках СНГ подписано новое Соглашение о сотрудничестве в борьбе с киберпреступностью, заменившее документ 2001 года с учетом обновившихся технологий и угроз [91]. Указанный договор расширил перечень совместно преследуемых деяний и установил механизм обмена электронными доказательствами между сторонами СНГ. В рамках вышеупомянутой ШОС Россия вместе с Китаем продвигает подход, акцентирующий борьбу не только с техническими киберпреступлениями, но и с преступным использованием информации, пропаганды терроризма, экстремизма, по их терминологии – «информационно-психологическими угрозами».

Отмечая международный аспект, следует добавить, что несмотря на неприсоединение к Будапештской конвенции, Россия участвует в работе Интерпола, в т.ч. его программы по киберпреступности, и направляет запросы о правовой помощи в другие страны на двусторонней основе. В структуре МВД России функционирует национальный координационный центр 24/7 (пункт связи) для взаимодействия с зарубежными коллегами по киберпреступности, который, в частности, включен в глобальную сеть контактных пунктов. Эту сеть Россия развивает преимущественно в сотрудничестве со странами СНГ и БРИКС. Тем не менее, политические разногласия заметно сказываются, сотрудничество правоохранителей РФ и западных стран затруднено, экстрадиция киберпреступников из России фактически не осуществляется, так как Конституция РФ запрещает выдачу граждан РФ иностранным государствам. С другой стороны, Россия сама активно привлекает к ответственности лиц, совершающих преступления в ее киберпространстве: так, в 2021–2022 гг. проводились резонансные операции ФСБ и МВД против группировки вымогательского ПО REvil и хакерского форума Hydra, что

Джилкишиев Р.Б.

показало готовность российских властей действовать против киберпреступников, когда их деятельность затрагивает национальные интересы РФ.

В целом, подход России и ряда государств СНГ выделяется акцентом на суверенитет, стремлением сформировать альтернативные международные режимы борьбы с киберпреступностью, вне западных институтов и одновременной активной работой на национальном уровне по совершенствованию законодательства и практики кибербезопасности.

Организация Объединенных Наций играет все более значимую роль в разработке глобальных подходов к борьбе с киберпреступностью. Хотя изначально лидирующую позицию занимали региональные организации Совет Европы и группы государств (G8/G20), в последнее десятилетие именно в рамках ООН развернулись основные переговоры о всеобъемлющем международном сотрудничестве. В системе ООН вопросами киберпреступности прежде всего занимается Управление ООН по наркотикам и преступности (далее – UNODC). С 2011 года при UNODC функционирует «Межрегиональная программа по киберпреступности», осуществляющая исследования, техническую помощь странам, обучение правоохранителей и содействие совершенствованию законодательства. В 2013 году по поручению Генеральной Ассамблеи UNODC подготовило Всеобъемлющее исследование проблемы киберпреступности, где проанализированы законодательство и кооперация более 100 государств, обозначены основные вызовы, включая отсутствие унифицированных норм, проблемы юрисдикции, сложности транскордонного доступа к данным и т.д. [92]. Данный доклад стал основой для межправительственных обсуждений.

В 2019 году по инициативе Российской Федерации Генассамблея ООН приняла резолюцию 74/247, которой была учреждена Специальная межправительственная рабочая группа Ad Hoc Committee для разработки проекта глобальной конвенции о борьбе с киберпреступностью. Несмотря на возражения ряда стран, таких как США, ЕС и др., изначально считали, что достаточно имеющихся соглашений, переговоры начались в 2020 году под эгидой ООН. В них приняли участие представители всех региональных групп – как сторонники жесткого регулирования - Россия, Китай, Иран, ряд стран Африки и Азии, так и государства, настаивавшие на узком фокусе нового договора и надежных правах человека - ЕС, Великобритания, Канада, Япония и др.. После нескольких сессий, в августе 2024 года, Комитет сообщил о достижении консенсуса по тексту Проекта Всеобъемлющей международной конвенции ООН по противодействию использованию ИКТ [93] в преступных целях. UNODC назвал это «важнейшим шагом» в борьбе с киберпреступностью на глобальном уровне. Ожидается, что финальная конвенция будет вынесена на одобрение Генассамблеи в 2024–2025 гг., после чего открыта для подписания, планируется церемония подписания в Ханое в конце 2025 года. Предполагается, что новый договор охватит широкий круг вопросов, криминализацию ключевых деяний, в значительной степени на основе

Джилкишиев Р.Б.

подходов Будапештской конвенции, но с добавлением некоторых новых составов вроде мошенничества, отмывания доходов, контентных преступлений; процессуальные меры, сбор электронных доказательств, выдача, взаимопомощь; превентивные меры, включая укрепление потенциала, обмен информацией, обучение; а также положения об уважении государственного суверенитета и международном сотрудничестве. Последние аспекты особенно отличают документ ООН от европейской Конвенции, проект ООН шире по охвату институциональных вопросов, предусматривает техническую помощь и обмен информацией между государствами, регламентирует роль центральных органов и защиту суверенных интересов [94]. Вместе с тем по ряду позиций новый текст уже сейчас вызывает обеспокоенность правозащитных организаций. В частности, критики указывают на недостаточные гарантии защиты прав человека и возможность расширительного толкования ряда положений, что может дать *«репрессивным государствам инструмент для расправы с инакомыслием под предлогом борьбы с киберпреступностью»* [95]. Например, первоначально предлагавшиеся статьи о наказуемости «экстремистских высказываний» и «распространения фейков» были частично смягчены под давлением демократических стран, однако некоторые формулировки все же оставлены на усмотрение национальных законодателей [96]. Западные государства и технологические компании выражали опасения относительно рискованности заключенного компромисса и призывали тщательно отнестись к имплементации будущей конвенции [97]. Тем не менее, сам факт перехода обсуждения киберпреступности на универсальный уровень ООН – значимое достижение. После вступления договора в силу ООН, вероятно, станет площадкой для регулярных встреч государств-участников, мониторинга выполнения обязательств и дальнейшего развития международного права в данной сфере. Уже сейчас при UNODC обсуждается создание специального механизма, комитета конференции сторон для обмена опытом и выработки рекомендаций по новой конвенции.

Помимо разработки глобального договора, система ООН задействует и другие свои структуры в противодействии киберпреступности. Так, Международный союз электросвязи (ITU) реализует программы повышения киберустойчивости и выпускает Глобальный индекс кибербезопасности, стимулируя страны развивать способности к пресечению киберпреступлений. Межполицейская организация ООН (Интерпол) (о ней ниже) сотрудничает с Советом Безопасности ООН по вопросам, где киберпреступность пересекается с терроризмом и транснациональной преступностью. Кроме того, тематикой цифровых преступлений занимаются профильные комиссии ООН – например, Комиссия по предупреждению преступности и уголовному правосудию (CCPCJ) включает киберпреступность в повестку своих сессий, а Управление по контртерроризму ООН рассматривает угрозы использования интернетом террористическими организациями.

Таким образом, ООН постепенно формирует всеобъемлющий международно-правовой режим борьбы с киберпреступностью, дополняющий

Джилкишиев Р.Б.

региональные механизмы и объединяющий как можно больше государств на основе общих принципов и стандартов.

Интерпол (Международная организация уголовной полиции) – ключевой практический механизм координации полицейских усилий против киберпреступности в глобальном масштабе. Объединяя 195 государств-членов, Интерпол обеспечивает ежедневно действующую инфраструктуру для обмена информацией и совместных действий правоохранительных органов. Базовым инструментом является защищенная коммуникационная сеть I-24/7, связывающая национальные центральные бюро Интерпола по всему миру. Через I-24/7 спецподразделения по киберпреступности разных стран могут в режиме реального времени обмениваться оперативными данными, рассылать сообщения о кибератаках, запросы на установление IP-адресов, координаты подозреваемых и т.п. Кроме того, Интерпол создал глобальную систему 24/7 контактных пунктов именно по киберпреступлениям. Данная сеть уполномоченных офицеров в более чем 120 странах, которые доступны круглосуточно для неотложных запросов, срочное сохранение цифровых доказательств, предотвращение продолжающейся атаки. Интерпол также поддерживает обширные базы данных и аналитические платформы, куда входят сведения об украденных платежных картах, известных киберпреступниках, используемых вредоносных программах, образцы цифровых следов и пр. Указанные базы доступны национальным правоохранительным органам, что облегчает расследования, позволяет связать киберинциденты в разных странах по схожим характеристикам [98].

Международная организация уголовной полиции Интерпол также учредила собственный центр, посвященный борьбе с киберпреступностью. В 2015 году в Сингапуре открыт **Глобальный комплекс инноваций Интерпола, Interpol Global Complex for Innovation (далее – IGCI)** – высокотехнологичный центр, ставший азиатской базой организации и главным узлом в сфере киберпреступности. IGCI – это межправительственное учреждение под эгидой Интерпола, обслуживающее все 195 стран-членов. В структуре IGCI действует Центр цифровых преступлений Digital Crime Centre (далее – DCC), который является одной из двух основных дирекций комплекса, вторая – Центр инноваций. DCC выступает оперативным подразделением Интерпола по расследованию киберпреступлений, под руководством директора, в первые годы пост занимал Санджай Вирмани. Штат IGCI насчитывает экспертов из разных стран, включая офицеров полиции, ИТ-специалистов, аналитиков. Финансирование идет через бюджет Интерпола и целевые взносы, в том числе от стран-хозяев, Сингапур активно поддерживал создание центра.

Глобальный комплекс Интерпола ставит целью оснастить мировую полицию инструментами и знаниями для борьбы с преступлениями XXI века. В контексте кибербезопасности DCC IGCI призван поддерживать национальные правоохранительные органы в расследовании киберпреступлений, особенно трансграничных. Его мандат – глобальный охват, центр обслуживает все

Джилкишиев Р.Б.

страны-участницы, многие из которых не обладают достаточными собственными кибервозможностями [99]. Основные функции DCC:

1) Центр экспертизы по цифровой криминалистике – IGCI содержит современную лабораторию цифровой криминалистики, где специалисты идентифицируют, извлекают и анализируют электронные доказательства с различных устройств. Данная лаборатория позволяет проводить экспертизы для сложных международных дел, по темным веб-форумам, ботнетам, криптовалютным транзакциям.

2) Оперативная поддержка расследований – по запросам национальных бюро Интерпола DCC направляет своих экспертов или консультирует удаленно, помогая преодолеть технические проблемы, отслеживание преступников, скрывающихся за анонимайзерами, или предоставление информации о вредоносных IP-адресах.

3) Координация международных операций – IGCI выступает площадкой, где собираются представители разных стран для совместных оперативных мероприятий. Например, через него идут инициативы типа глобальных «дней действий» против сетей киберпреступников.

4) Обмен информацией – центр улучшает обмен разведданными о киберугрозах между странами, используя коммуникационную сеть Интерпола (I-24/7) и специальные каналы.

5) Обучение и наращивание потенциала – IGCI проводит тренинги для специалистов полиции со всего мира, издает руководства. Так, Интерполом разработаны «Руководства для первых реагентов по цифровой криминалистике», распространяемые через IGCI с целью стандартизировать подходы к работе с электронными доказательствами на месте преступления.

Интерпол не обладает своими следственными полномочиями на территории стран – он действует посредством национальных бюро. Поэтому IGCI фокусируется на координации и вспомогательных функциях. Однако, находясь вне национальных юрисдикций, он может служить нейтральной территорией для совместной работы представителей стран, которые не всегда напрямую обмениваются информацией. DCC часто сталкивается с проблемами юрисдикций и законов, как отмечает руководство, различия в законодательствах и политические конфликты между странами затрудняют быстрый обмен данными. Центр пытается преодолеть это через формат «полиция-полиция», налаживает прямые связи оперативников, создает региональные рабочие группы для доверительного обмена разведданными. IGCI также запускает инициативы по аудиту национального киберпотенциала: по запросу страны специалисты центра проводят всесторонний обзор «national cyber review» ее способностей противодействовать киберпреступности, выявляют пробелы и рекомендуют улучшения в законодательстве, организационной структуре и техническом оснащении, что повышает уровень включенности стран, особенно развивающихся, в глобальные усилия. IGCI активно сотрудничает с частным сектором, заключаются партнерства с компаниями-разработчиками цифровых криминалистических инструментов.

Джилкишиев Р.Б.

Например, компания Cellebrite предоставила IGCI оборудование и обучение по вскрытию мобильных устройств, усилив возможности Интерпола в расследованиях цифровых доказательств [100].

Глобальный комплекс оснащен по последнему слову техники. Digital Forensics Lab имеет инструменты для анализа данных с мобильных телефонов, компьютеров, IoT-устройств; хранит обширные базы данных хеш-сумм известного контента, для детской порнографии для автоматизированного сравнения. Большое внимание уделяется малваре-аналитике, IGCI сотрудничает с антивирусными компаниями, например, лаборатория Касперского помогала наладить поиск вредоносных программ в центре [101], что дало возможность разбирать образцы вредоносов прямо в сингапурской лаборатории. Киберфьюжн-центр – центральный узел IGCI, где под одной крышей работают офицеры полиции разных стран и партнерских ИБ-компаний, обмениваясь информацией в режиме реального времени. Этот fusion-центр позволяет объединять сведения из правоохранительных источников с данными частных фирм, по угрозам финансового сектора, создавая целостную картину. Для преодоления правовых ограничений на передачу данных IGCI разработал строгие процедуры контроля: страна, передающая данные, может наложить оговорки об их использовании, и Интерпол соблюдает принципы суверенитета данных – не раскрывая информацию другим без разрешения источника [102]. В техническом арсенале центра – собственные платформы для обмена расследовательской информацией, информационная система по киберпреступлениям, где страны размещают сводки своих дел. Также Интерпол организует симуляции кибератак и учения, IGCI проводил международные учения Cyber Polygon и другие, где в режиме реального времени отрабатывается сотрудничество при глобальных атаках. В области инноваций IGCI изучает новые технологии, как их используют преступники и как они могут помочь полиции. Его Инновационный центр занимается исследованиями применения ИИ, блокчейна, анализа больших данных для нужд уголовного сыска [103].

Деятельность Интерпола через IGCI значительно усилила глобальный отпор киберпреступности. Интерпол стал главной площадкой для организации многосторонних полицейских операций против киберпреступников. Например, через его координацию проводились такие операции, как: Operation Killer Bee (2021) – против мошенников, занимавшихся компрометацией коммерческой электронной переписки (BEC-fraud) в 20+ странах, Operation Haechi (серия операций 2020–2022 гг.) – против онлайн-мошенничеств и отмывания денег в Азии и за ее пределами, Operation Lyrebird – по задержанию подозреваемого оператора Darknet-платформы по торговле данными и др. В 2020 году Интерпол и Европол запустили совместную инициативу Cyber Most Wanted, публикуя списки наиболее разыскиваемых киберпреступников, что стимулирует их поиск по всему миру. Интерпол координировал операцию против сетевого ресурса Infraud (форум киберпреступников), где были арестованы десятки людей в 14 странах. В Азии при поддержке IGCI

проведены масштабные аресты группировки кибермошенников, похитивших миллионы долларов посредством интернет-афер. В 2018 году совместно с EC3 Европола Интерпол запустил операцию Night Fury против ботнетов, заразивших десятки тысяч маршрутизаторов в Азиатско-Тихоокеанском регионе – она привела к очистке устройств и задержаниям. IGCI также стал центром знаний, выпущенные им глобальные «Руководства для цифровой криминалистики» используются полицией в разных странах, а проведенные тренинги, 90-дневные стажировки для киберинвестигаторов из Германии, Великобритании, Австралии, Нидерландов, Литвы и Украины способствовали обмену опытом и созданию личных связей между специалистами. Интерпол отмечает, что благодаря IGCI обнаружено и закрыто несколько темных веб-ресурсов, включая упомянутый RaidForums в сотрудничестве с Европолом, изъяты сотни серверов, используемых преступниками, и арестованы лидеры ряда хакерских групп. IGCI зарекомендовал себя как уникальная международная площадка, где объединяются усилия полиций всего мира, и в сфере цифровой криминалистики он играет все более существенную роль, особенно для стран, не имеющих собственных мощностей [103].

Важно подчеркнуть, что Интерпол не обладает наднациональными властными полномочиями, но служит механизмом доверия и коммуникации между правоохранительными органами. Его эффективность зависит от готовности национальных полиций взаимодействовать и делиться информацией. В контексте киберпреступности Интерпол незаменим, поскольку нередко «одна атака может включать злоумышленников из нескольких стран, инфраструктуру в разных юрисдикциях, и жертв по всему миру; глобальный охват киберпреступности требует глобального стратегического подхода». В итоговом счете, Интерпол служит оперативным звеном международного сотрудничества, дополняя формальные договоры, когда требуется быстро отреагировать на глобальную кибератаку или отследить преступника, именно каналы Интерпола позволяют это сделать с минимальными бюрократическими задержками.

Анализ мировых практик показывает, что успешная борьба с киберпреступностью требует создания специализированных национальных центров, которые объединяют технические, аналитические и организационные ресурсы для централизованного и эффективного управления кибербезопасностью. Яркими примерами таких структур являются Национальный центр кибербезопасности Великобритании (NCSC), Канадский центр кибербезопасности (CCCS), Австралийский центр кибербезопасности (ACSC) и Национальный центр интеграции кибербезопасности и коммуникаций США (NCCIC). Их опыт демонстрирует значительное повышение способности стран оперативно выявлять и реагировать на кибератаки, обеспечивать защиту критически важной инфраструктуры, проводить цифровую криминалистику и координировать действия различных ведомств и организаций.

Отмечено, что ключевой функцией таких центров является не только мониторинг и анализ угроз, но и активное взаимодействие с частным сектором, гражданским обществом и международными партнерами. Особенно эффективными оказались модели, которые предполагают интеграцию данных центров с разведывательными службами и правоохранительными органами, как это реализовано в Великобритании и Австралии. Например, NCSC Великобритании зарекомендовал себя благодаря программе активной киберзащиты, что позволило значительно снизить уязвимость государственных и коммерческих сетей перед угрозами.

В Канаде также наблюдаются значимые успехи после создания CCCS, который смог централизовать разрозненные ресурсы разных ведомств и существенно укрепить защиту критических секторов, таких как здравоохранение, финансы и телекоммуникации. Использование уникальной платформы автоматизированного анализа угроз Assemblyline значительно повысило эффективность цифровой криминалистики и оперативного реагирования на инциденты. В США, несмотря на отсутствие единого центра как отдельного юридического лица, интегрированный подход NCCIC/CISA обеспечивает глубокое и комплексное покрытие потребностей в сфере национальной кибербезопасности.

Опыт Европейского центра по борьбе с киберпреступностью (EC3) и Интерпола демонстрирует необходимость международной координации и обмена информацией для эффективного противодействия трансграничным киберугрозам. EC3 является примером успешного объединения стран для совместного расследования и цифровой криминалистики, а Интерпол через свой Глобальный комплекс инноваций (IGCI) активно развивает инфраструктуру и инструментарий для глобальной оперативной поддержки стран-членов [104].

Исходя из вышеизложенного, можно рекомендовать создание и развитие аналогичного **«Национального центра управления кибербезопасностью и цифровой криминалистики» (НЦУКЦК)** в Казахстане. Подобный центр должен иметь статус межведомственного органа с четко определенными полномочиями и ответственностью за координацию и управление кибербезопасностью страны. Необходимо предусмотреть его взаимодействие не только с государственными органами и службами безопасности, но и с частным сектором, научным сообществом и международными партнерами, опираясь на лучшие международные практики. НЦУКЦК должен объединить функции и полномочия правоохранительных и специальных государственных органов (МВД, КНБ, Агентство по финансовому мониторингу и других заинтересованных государственных органов), а также финансовых и частных цифровых организаций. Основными задачами Центра должны стать:

1. **Разработка и внедрение единой цифровой платформы обмена информацией**, на которой в реальном времени аккумулируются данные о киберинцидентах от банков, интернет-провайдеров, криптовалютных бирж, социальных сетей и операторов связи, а также от национальных и зарубежных

правоохранительных структур. Платформа должна быть построена с использованием блокчейн-технологий для обеспечения прозрачности и защиты данных, с возможностью оперативного отслеживания всех операций и транзакций.

2. **Формирование цифровой базы данных и реестра киберпреступлений**, включающего сведения о схемах мошенничества, используемых вредоносных программах, фишинговых сайтах и подозрительных аккаунтах, что позволит оперативно выявлять преступления, анализировать их тенденции и прогнозировать возникновение новых угроз.

3. **Закрепление в законодательстве РК** обязанности финансовых организаций, интернет-платформ и операторов связи незамедлительно (не позднее 24 часов) предоставлять правоохранительным органам сведения о подозрительных операциях, а также вводить обязательный мониторинг новых цифровых услуг и инструментов на предмет соответствия требованиям информационной безопасности. Данное предложение необходимо закрепить в новом законе «О противодействии киберпреступности».

4. **Создание Национальной лаборатории цифровой криминалистики** в структуре НЦУКЦК, которая займется внедрением передовых технологий расследования киберпреступлений, таких как «Big Data» аналитика, машинное обучение и искусственный интеллект для быстрой обработки и анализа цифровых следов и доказательств, что позволит существенно сократить сроки расследования и повысить процент раскрываемости.

5. **Введение института цифровых криминалистов и киберследователей** с законодательно закрепленными полномочиями по сбору, фиксации и экспертизе цифровых доказательств, а также регулярное (не реже двух раз в год) повышение квалификации сотрудников правоохранительных органов на специальных тренингах и семинарах с участием международных экспертов.

6. **Разработка и принятие межведомственного протокола**, регламентирующего порядок оперативного взаимодействия правоохранительных органов Казахстана с компетентными органами иностранных государств, включающего электронный документооборот и унифицированные форматы передачи цифровых доказательств в рамках расследования трансграничных преступлений.

Заключая данный анализ, подчеркнем, что успех в противодействии киберпреступностью сегодня невозможен без межведомственного, межсекторного и международного взаимодействия. Создание НЦУКЦК в Казахстане, построенного по лучшим мировым образцам, способно значительно повысить устойчивость страны к цифровым угрозам и обеспечить защиту ее национальных интересов в киберпространстве, что позволит нашей стране не только оперативно реагировать на возникающие угрозы, но и активно предотвращать их, обеспечивая стабильность и безопасность всего информационного пространства страны.

Джилкишиев Р.Б.

2 ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ И АЛГОРИТМЫ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ ОБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

2.1 Начало досудебного производства и обстоятельства, подлежащие доказыванию по уголовным делам об информационных технологиях и киберпреступности

Правовая система Республики Казахстан, реагируя на вызовы цифровой эпохи, постепенно внедряет институциональные и процессуальные механизмы, адаптированные под специфику киберпреступлений. Однако анализ показывает, что на практике остаются нерешенными множество аспектов, связанных с идентификацией источников цифровых угроз, определением момента возбуждения уголовного дела, а также установлением обстоятельств, подлежащих доказыванию в данной категории дел.

Особую значимость в таких делах приобретает вопрос определения основания для начала досудебного расследования, особенно с учетом специфики получения информации о совершенном деянии. Источниками сведений о противоправных действиях все чаще выступают не только заявления физических и юридических лиц, но и данные, полученные в ходе оперативно-розыскной деятельности, сообщения из средств массовой информации, результаты аудита и внутреннего мониторинга безопасности. Это требует от следователя глубокого понимания как юридической сути поступившей информации, так и ее технологического контекста, связанного с цифровыми носителями, сетевой инфраструктурой и форматами представления цифровых доказательств.

Одновременно с этим возникает необходимость в осмыслении и четкости определения обстоятельств, подлежащих доказыванию по уголовным делам об информационных технологиях. В данной категории дел приоритетное значение приобретают такие элементы, как установление механизма несанкционированного доступа, доказательство наличия умысла у обвиняемого в отношении цифрового объекта, а также причинно-следственная связь между действиями субъекта и наступившими последствиями. Отдельно необходимо подчеркнуть важность доказывания роли соучастников, вовлеченных в технологически распределенные действия, а также мотивов и цели киберпреступления, которые нередко связаны не только с корыстной, но и с идеологической или протестной направленностью.

В условиях цифровизации уголовного судопроизводства особую актуальность приобретает системный подход к организации досудебного производства и построению предмета доказывания по делам, связанным с информационными технологиями. Актуальной задачей научного и практического характера становится разработка методологической базы, позволяющей выработать оптимальные алгоритмы действий следователя, стандартизировать процесс фиксации цифровых следов, а также повысить уровень доказательной силы материалов, представляемых в суд. Углубленный

Джилкишиев Р.Б.

анализ этого вопроса позволит не только повысить эффективность борьбы с киберпреступностью, но и обеспечить соблюдение принципов законности, объективности и справедливости при осуществлении уголовного преследования в условиях современной цифровой реальности.

Киберпреступления охватывают широкий спектор противоправных деяний, совершаемых в цифровой среде (виртуальном пространстве) при помощи компьютерной техники, мобильных телефонов, прочих гаджетов и информационных технологий.

Количество киберпреступлений, совершаемых в глобальных сетях или с использованием компьютерных технологий, растет день ото дня. Кибервзломы, интернет-мошенничество, кража данных — сегодняшняя обыденность. Для понимания важности и актуальности проблемы мировой киберпреступности было проведено исследование глобальных экономических правонарушений, в котором приняли участие 78 государств. Результаты показали, что киберпреступления занимают 4-е место в мире. Как уже отмечалась неоднократно, рост численности компьютеров и интернета вызвал рост численности экономических преступлений, т.е. преступники активно осваивают новые технологии для совершения преступлений.

Действующим уголовно-процессуальным законодательством предусмотрено деление дел на различные категории с установлением для каждой из них определенных правил и процедур. Дифференцированный порядок производства также предполагает диспозитивность, предполагающую возможность пострадавшей стороны влиять на процесс (подача жалоб, выражение своего волеизъявления по ключевым вопросам, участие в процессе).

Начало досудебного расследования

Основанием для начала досудебного расследования является регистрация заявления, сообщения об уголовном правонарушении в Единый реестр досудебного расследования WEB-ЕРДР, утвержденного Приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89 (далее – Приказ ГП № 89).

Досудебное расследование противоправных деяний, совершенных в сфере компьютерной информации, может быть инициировано путем подачи пострадавшей стороной заявления о несанкционированном доступе к компьютерной информации или системам, или о краже финансовых средств. Подобные заявления могут исходить от отдельных граждан, организаций в лице первых руководителей и должностных лиц. Основаниями для начала расследования могут быть заключения контролирующих органов по итогам проведенных проверок, в ходе которых выявлены факты хищений или несанкционированного доступа. Информация о правонарушениях также может быть предоставлена службами безопасности, что также является основанием для возбуждения дела.

При этом все забывают, что согласно пункту 5 Приказа ГП № 89, первоначальная регистрация осуществляется в книгу учета информации – КУИ.

Джилкишиев Р.Б.

И лишь после проверки, при установлении наличия признаком уголовного правонарушения, осуществляется регистрация в ЕРДР.

Согласно статистическим данным за последние пять лет, в качестве заявителя по поводу компьютерных правонарушений, в основном, выступают организации, тогда как рядовые граждане обращаются гораздо реже. Одна из причин низкой активности граждан — боязнь разглашения информации личного (конфиденциального) характера, а также страх того, что их частная жизнь может стать предметом обсуждения в ходе судебного разбирательства. Поэтому крайне важно, чтобы следователем были установлены доверительные отношения и психологический контакт с гражданином.

Расследование уголовных правонарушениях в области информационных технологий и киберпреступности должно начинаться с четкого анализа произошедшего, какие конкретно данные или системы подверглись воздействию злоумышленников, следственный эксперимент – последующие допросы – дополнительные экспертизы, какова структура объекта, где возможно было совершено противоправное деяние. Следователю необходимо проанализировать условия, в которых функционирует объект, способ обработки и хранения данных; система документооборота (товарооборота); параметры оборудования и программного обеспечения, позволяющие определить способ взаимодействия между компьютерами и пользователями; уровень организация мер безопасности для защиты конфиденциальной информации; должностные инструкции сотрудников, в чьи обязанности входит обработка и хранение компьютеров и информации ставшей объектов преступного посягательства.

Обстоятельства, подлежащие доказыванию

«Для достижения объективной истины при расследовании правонарушений важнейшее значение имеет доказывание, т.е. направляемая и регулируемая уголовно-процессуальным законом в определенных формах и пределах деятельность следователя, прокурора и других органов и лиц по собиранию, исследованию и оценке доказательств в целях установления фактических обстоятельств по уголовному делу» [105, с.249].

Пункт 1 ст. 113 УПК РК регламентирует основные обстоятельства, подлежащие доказыванию:

- установление конкретного места, времени и условий совершения преступления;
- кем совершено противоправное деяние, имело ли данное лицо судимость за совершение аналогичных преступлений ранее;
- как именно было совершено преступление;
- оценка факторов, способных повлиять на степень вины обвиняемого (смягчающие и отягчающие обстоятельства);
- какие цели преследовал обвиняемый, каковы мотивы совершения преступления;
- были ли вовлечены третьи лица в преступные действия (соучастники, пособники), уровень их вовлеченности;

Джилкишиев Р.Б.

- причины и условия, которые способствовали совершению противоправного деяния.

Задачи расследования правонарушений

«Во всех случаях расследования уголовных дел установление наличия преступного события является важным начальным этапом расследования правонарушения и составляет первоочередную задачу следователя при расследовании всех без исключения категорий дел. Следователь, установив наличие преступного события, создает необходимые условия для дальнейшего ведения следствия» [106, с.44].

Одной из первостепенных задач является создание и внедрение новых методов расследования, которые помогли бы следователю своевременно выявлять и эффективно расследовать противоправные деяния в сфере информационных технологий. Успех расследования во многом зависит от применения следователем современных научных и технических методов, позволяющих проведение качественного анализа улик и выявления преступников. Эффективные методы расследования должны базироваться на научных исследованиях и анализе успешных практик, что дает возможность следователю перенимать опыт других, адаптировав его к своим нуждам. Методика расследования позволяет следователю минимизировать затраты ресурсов, а также избежать возможных ошибок в процессе расследования.

Возникновение либо усиление различного рода негативных тенденций в сфере информатизации, появление новых видов киберпреступности и изменения в структуре ранее существовавших видов правонарушений в сфере информационных технологий в сфере киберпреступности обусловливают необходимость разработки новых методик расследования правонарушений данной категории.

Одним из важных решений в данном направлении стало Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» (далее – Киберщит Казахстана), результатом которого в 2019 году стало создание Центра по борьбе с киберпреступностью Департамента криминальной полиции МВД РК (далее – Центр по борьбе с киберпреступностью) [4].

В дальнейшем данный проект получил развития уже в следующей Концепции развития цифровой экосистемы на 2022–2027 года или Киберщит-2 [107]. Так, документом предложено создать отдельные центры в направлениях защиты кричащих секторов, в частности, финансового, топливного, образовательного и медицинского, нефтегазового, транспортного, сельскохозяйственного и оборонного и т. д. Так, например, в сфере банковского обслуживания начал действовать соответствующий центр, уполномоченный собирать и анализировать информацию о проблемах в сфере информационной безопасности в соответствующем секторе; данный центр призван предупреждать банковскую систему о возможных кибератаках и уязвимых местах в информационной безопасности. Упомянутый проект в большинстве фокусируется на крупных компаниях; в отношении средних и малых

Джилкишиев Р.Б.

предприятий, также страдающих от кибератак, отмечается, что основной причиной атак на указанный бизнес, является неосведомленность владельцев относительно последствий небрежной информационной защиты. Поэтому авторами проекта предложено повысить уровень информационного образования и увеличить финансирование компаний, разрабатывающих системы защиты носителей информации [107].

Учитывая данный проект, наиболее распространенными и актуальными киберугрозами остаются фишинговые атаки и DDoS-атаки, исключающие работу предприятия и обработку запросов и т.д. [107].

Стоит отметить, что «Киберщит-2» хотя и значительно совершенствует систему киберзащиты на территории Республики Казахстан, однако нерешенным остается правовое поле, а именно процесс расследования правонарушений, которые все же были совершены в сфере информационных технологий и которые не удалось предотвратить. Проектом не предусмотрено создание отдельного специального подразделения, уполномоченного на расследование данного вида преступлений. Также открытым остается вопрос о возможном увеличении финансирования существующих правоохранительных органов по совершенствованию технических возможностей в данной сфере, а также дополнительной квалификации работников [108, p. 105].

Процесс предварительного расследования проводится строго в рамках уголовно-процессуального законодательства, что дает гарантию законности и обоснованности предпринимаемых в ходе расследования действий. Сотрудники, участвующие в данном процессе, должны обладать соответствующим образованием и навыками, включая знание современных технологий и методов расследования криминалистики. Профессионально подготовленные сотрудники, осуществляющие свою деятельность в рамках закона, более эффективно осуществляют предотвращение и выявление противозаконных действий, тем самым способствуя повышению общественной безопасности.

Как верно отметил Саруханян А. расследование преступлений представляет собой сферу деятельности следователя, выступающего в качестве основного элемента в производстве определенных процессуальных действий, регулирования и руководства [109, с. 52].

Масштабы киберпреступности возрастают пропорционально возрастающему числу пользователей Интернета. Согласно статистическим данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан за 5 лет (2021-2025 годы), соотношение зарегистрированных уголовных правонарушений главы 7 УК и направленных уголовных дел в суд не выдерживает никакой критики, так: по статье 205 за указанный период направленно 5, по статье 206 – 33, по статье 207 – 3, по статье 208 – 3 и по статье 210 – 4 дела [1].

Как уже неоднократно подчеркивалось ранее, киберпреступления — крайне специфичный вид противоправных деяний. Особенности данного вида преступлений делают их расследования более сложными в сравнении с

традиционными правонарушениями. Следователи сталкиваются с трудностями с обобщением материалов: не имея достаточного опыта, не обладая достаточными данными, правоохранительные органы не могут эффективно проводить анализ и выявить общие тенденции в киберпреступлениях. К факторам, мешающим эффективному расследованию рассматриваемой категории дел, можно отнести недостаток методических рекомендаций и недостаточная квалификация лиц, проводящих следствие. Порой следователи не обладают элементарными знаниями правильного сбора, сохранения и анализа цифровых данных, что является критически важным для раскрытия киберпреступлений.

Анализ статистических денных позволяет сделать вывод о недостаточном уровне навыков у сотрудников созданного Центра по противодействию киберпреступности, позволяющим своевременно раскрывать правонарушения, устанавливать доказательства и привлекать к ответственности виновных лиц.

Следственные ситуации

То, насколько следователь умеет правильно воспринять и оценить следственные ситуации на первоначальном этапе, может определить эффективность и успешность дальнейшего процесса расследования. Понимание и анализ следственных ситуаций имеют особую актуальность в контексте сложности киберправонарушений. Понятие «следственная ситуация» является центральным в криминалистике, поскольку это связующее звено между теоретическими знаниями и практическими действиями следователя. Данная дефиниция относится к конкретным обстоятельствам, в которых происходит противоправное деяние, а также к способу использования данных обстоятельств для сбора доказательной базы и построения дела.

В понимании профессора Джакишева Е.Г. следственная ситуация — это «положение, обстановка, которая складывается и изменяется на определенных этапах расследования на основе данных, вытекающих из материалов дела» [110, с. 343].

В настоящее время интерес к изучению следственных ситуаций имеет стойкую тенденцию роста. Сегодня мы можем говорить о развитии целого направления в криминалистике — криминалистической ситуалогии [111, с. 33]. Данное направление фиксируется на анализе конкретных обстоятельств, при которых совершаются противоправные деяния, а также на влиянии данных обстоятельств на процесс расследования. С нашей точки зрения, следственная ситуация охватывает все аспекты, имеющие отношение к расследованию преступления, в том числе факторы, которые могут оказать влияние на выдвижение версий и организацию следственных действий.

На наш взгляд, следственная ситуация — важнейший инструмент в работе следователя, позволяющий определить наиболее эффективные действия для расследования. Умение правильно анализировать следственные ситуации значительно повышает эффективность следственных действий. Особенно это актуально в отношении киберпреступлений, когда традиционные методы не всегда могут быть применены, глубокое понимание следственной ситуации

Джилкишиев Р.Б.

способствует рациональному распределению ресурсов и увеличивает вероятность раскрытия противоправного деяния.

Исходя из специфики расследования киберпреступлений, а также опубликованного опыта, представляем алгоритм расследования, представляющий собой последовательный и систематический подход к расследованию преступлений в сфере компьютерной информации. Данный алгоритм включает в себя пять основных этапов, позволяющих следователю сконцентрироваться на определенных аспектах дела, провести более детальный анализ и принять обоснованные решения на каждой стадии.

1. Установление непосредственного факта совершения преступления и его характера: сбор первичной информации о месте, времени совершения противоправного деяния, о лицах, принимавших в нем участие, а также о совершенных действиях.

2. Определение вида материальной или иной выгоды, которую преступник мог получить, совершая преступное деяние.

3. Проведение анализа методологии преступника при совершении правонарушения: установление технических средств и приемов, которые были применены для совершения преступления.

4. Определение круга лиц, принимавших участие в совершении противоправного деяния (непосредственный исполнитель, соучастники, пособники).

5. Оценка нанесенного ущерба и масштаба последствий правонарушения.

На первоначальном этапе расследования могут возникнуть следующие **основные следственные ситуации**:

1) наличие полной либо частичной информации о факте самого правонарушения, и причинах его возникновения, способе совершения правонарушения и личности пострадавшего, отсутствие сведений о лице, совершившем правонарушение, мотивы которого неясны;

2) наличие полной информации о личности лица, которому нанесен ущерб и лице, кто нанес ущерб, способе совершения преступления, мотивах правонарушения, однако подозреваемое лицо не идет на контакт со следствием и не признает свою вину;

3) наличие информации о причинах возникновения противоправного деяния, способах его совершения и сокрытия, при этом подозреваемый признает свою вину и сотрудничает со следствием.

Сложность установления момента совершения преступления, трудности идентификации лица, причастного к деянию, а также отсутствие видимых последствий сразу после атаки — все это обуславливает замедленную реакцию правоохранительных органов и увеличивает риск утраты или искажения цифровых следов. При этом действующий Уголовно-процессуальный кодекс Республики Казахстан не содержит четко очерченного механизма реагирования на инциденты в киберсреде, что снижает эффективность начальных этапов расследования.

Джилкишиев Р.Б.

Одним из основных выводов, вытекающих из анализа, является необходимость переосмысления природы поводов и оснований к возбуждению уголовного дела в данной категории. Современные формы киберпреступности — от фишинга до деструктивного воздействия на критически важную инфраструктуру — зачастую выявляются не заявителями, а в результате автоматического мониторинга, технических логов, системных сбоев или сигналов из межведомственных источников. Это требует законодательного закрепления таких источников информации, как самостоятельные и достаточные поводы для начала досудебного расследования.

Кроме того, структура предмета доказывания в киберпреступлениях должна быть существенно дополнена с учетом особенностей цифровых следов. Необходимо формализовать включение в предмет доказывания обстоятельств, касающихся идентификации IP-адресов, лог-файлов, метаданных и цифровых профилей, что потребует комплексной оценки технологической инфраструктуры, участвовавшей в совершении деяния. Недопустимо ограничиваться лишь формальными данными об имуществе, личности и мотивации — требуется доказательная реконструкция цифрового поведения субъекта. В этой связи предлагается дополнить статьи УПК нормами, регламентирующими необходимость привлечения специалиста по информационной безопасности уже на момент возбуждения дела и фиксирования цифровых следов в первоначальной форме их обнаружения.

Для повышения эффективности досудебного производства в рассматриваемой категории дел рекомендуется разработать типовые алгоритмы (регламентирующие схемы) первичного реагирования на киберинциденты. Они должны учитывать скорость распространения цифрового вредоносного воздействия и предусматривать возможность экстренной блокировки активов, фиксации удаленных логов и получения судебных санкций в ускоренном порядке. В этом контексте необходимо также реформировать систему подготовки следователей, обеспечивая их знаниями в области цифровой криминалистики, основах кибергигиены и технической работы с цифровыми носителями.

Эффективное досудебное производство по делам о киберпреступлениях требует перехода от инерционно-формализованного к адаптивно-оперативному подходу. Только своевременное признание специфики цифровой преступности на нормативном и процессуальном уровнях позволит не только обеспечить законность и результативность уголовного преследования, но и сохранить доказательства, которые с высокой вероятностью могут быть утрачены в первые же часы после совершения деяния. В этом смысле модернизация начального этапа досудебного производства является краеугольным элементом всей системы борьбы с киберпреступностью в условиях цифровой трансформации правоохранительной системы Республики Казахстан.

С учетом интенсивного роста количества и сложности преступлений, совершаемых с использованием информационных и цифровых технологий, а также международного опыта и современных стандартов расследования,

Джилкишиев Р.Б.

предлагаются следующие авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 24.05.2025 г.).

А) В главу 3 «Уголовное преследование» добавить **ст. 34-1 «Особенности уголовного преследования по делам о киберпреступлениях»,** далее добавить нижеследующие части с авторским изложением в следующей редакции:

«1. При производстве уголовного преследования по уголовным делам о преступлениях, совершенных с использованием информационно-коммуникационных технологий, орган дознания и следователь вправе использовать специализированные программно-технические комплексы для сбора и закрепления цифровых доказательств.

2. Доказательства, полученные с использованием специализированных программно-технических комплексов, должны сопровождаться подробным техническим описанием процедур получения и сохранения данных».

Предложение направлено на обеспечение допустимости и достоверности цифровых доказательств, полученных при расследовании киберпреступлений. Это также позволит унифицировать и повысить качество досудебного расследования.

Б) В главу 15 «Доказательства» добавить новую **ст. 118-1 «Цифровые доказательства»,** затем добавить 1 и 2 часть с авторским изложением в следующей редакции:

«1. Цифровыми доказательствами признаются любые электронные данные, полученные из информационных систем, компьютерных устройств, серверов, мобильных устройств, облачных сервисов, а также информация, извлеченная в результате негласного снятия информации с компьютерных систем в соответствии со статьей 245 настоящего Кодекса.

2. Порядок сбора, фиксации и использования цифровых доказательств определяется Правилами, утверждаемыми Генеральной прокуратурой Республики Казахстан совместно с уполномоченным органом в области цифрового развития».

Введение четкой дефиниции и стандартизации цифровых доказательств необходимо для обеспечения их процессуальной чистоты, что существенно повышает эффективность уголовного судопроизводства по киберпреступлениям.

В) В ст. 197 «Общие правила производства следственных действий» добавить часть 7 и внести дополнение, изложив его в следующей редакции: **«В случаях расследования преступлений в сфере информационных технологий допускается дистанционное производство следственных действий с использованием технологии видеоконференцсвязи при условии соблюдения требований идентификации участников и защиты конфиденциальности данных, полученных в ходе следственного действия».**

Данное предложение направлено на оптимизацию и ускорение расследования киберпреступлений, особенно с учетом трансграничного

Джилкишиев Р.Б.

характера таких преступлений и необходимости оперативного взаимодействия с участниками процесса, находящимися за пределами Республики Казахстан.

Г) В ст. 245 «Негласное снятие информации с компьютеров, серверов и других устройств» добавить часть 4 и внести дополнение, изложив его в следующей редакции: **«Результаты негласного снятия информации, произведенного в рамках расследования преступлений, совершенных с использованием информационных технологий, подлежат обязательному экспертному исследованию с привлечением специалистов в области кибербезопасности».**

Необходимость экспертного подтверждения результатов негласных мероприятий обусловлена сложностью технологических аспектов цифровой информации, что исключает возможность ошибок и гарантирует юридическую значимость собранных данных.

Д) Добавить новую главу **30-1 «Особенности производства по уголовным делам о киберпреступлениях»**, после чего добавить **ст. 251-1. «Особенности досудебного расследования киберпреступлений»,** далее внести нижеследующие части с авторским изложением в следующей редакции:

«1. При досудебном расследовании преступлений, совершенных в цифровом пространстве, обязательным является участие специалиста или эксперта в области информационных технологий и кибербезопасности на всех этапах сбора, анализа и оценки доказательств.

2. Следователь вправе поручать проведение технических исследований объектов цифровых преступлений специализированным экспертным учреждениям.

3. Участники уголовного процесса по делам о киберпреступлениях обеспечиваются правом получения полной информации о методах сбора и анализа цифровых данных, используемых в рамках следственных мероприятий».

Специализация расследования киберпреступлений обеспечит повышение профессионального уровня проводимых мероприятий и минимизацию риска процессуальных ошибок, связанных с техническими аспектами расследования таких преступлений.

Е) В ст. 576 «Проведение процессуальных действий путем проведения видеосвязи» добавить часть 7 и внести дополнение, изложив его в следующей редакции: **«В случаях проведения видеосвязи при расследовании трансграничных преступлений в области информационных технологий, обеспечение идентификации личности участников видеоконференции и защиты передаваемых данных осуществляется в соответствии с международными стандартами цифровой идентификации и защиты данных».**

Повышение надежности идентификации участников трансграничного процесса и защиты конфиденциальности информации необходимо для международного сотрудничества и признания собранных доказательств за рубежом.

Джилкишиев Р.Б.

Предложенные авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан создают целостную нормативную базу, способную обеспечить эффективное уголовно-процессуальное регулирование в области противодействия киберпреступлениям. Они учитывают специфику и сложность современных преступлений, совершенных в цифровом пространстве, и дают четкие ориентиры правоохранительным и судебным органам для грамотного осуществления расследования и судебного рассмотрения данных категорий уголовных дел.

Кроме того, они обеспечивают более эффективное международное сотрудничество по делам о трансграничных киберпреступлениях, вводя стандарты идентификации и защиты данных, соответствующие международным нормам, что существенно облегчит взаимодействие казахстанских правоохранительных и судебных органов с зарубежными коллегами, повысит взаимное доверие и упростит процедуру признания доказательств на международном уровне.

Таким образом, реализация указанных предложений и изменений будет способствовать формированию устойчивой и передовой уголовно-процессуальной системы, адаптированной к новым цифровым реалиям и отвечающей современным вызовам и угрозам в области информационной безопасности. Их внедрение позволит не только эффективно пресекать и расследовать киберпреступления, но и существенно укрепит доверие граждан и организаций к правоохранительной системе Республики Казахстан.

Джилкишиев Р.Б.

2.2 Типичные ситуации на первоначальном этапе расследования информационных технологий в сфере киберпреступности и алгоритм действий следователя

На начальном этапе расследования следователь сталкивается с типичными ситуациями, характеризующимися высокой степенью неопределенности, дефицитом информации и необходимостью оперативного принятия решений в условиях ограниченного времени. Специфика таких ситуаций связана, прежде всего, с неосязаемым характером цифровых следов и их высокой подверженностью уничтожению или изменению. В этой связи важнейшей задачей становится своевременная идентификация цифровых объектов, надежная фиксация цифровых доказательств и грамотное проведение первоначальных следственных действий.

Особое внимание в подразделе уделяется алгоритму действий следователя, который должен четко понимать последовательность своих шагов, начиная от момента поступления информации о преступлении и заканчивая первым комплексом мероприятий, направленных на закрепление доказательной базы. Определение данного алгоритма призвано обеспечить оперативность и эффективность расследования, минимизировать риски утраты доказательств, а также повысить качество и юридическую значимость проводимых следственных мероприятий.

Кроме того, в рамках рассматриваемого подраздела раскрываются отдельные особенности тактики проведения таких следственных действий, как осмотр места происшествия, допрос подозреваемых и свидетелей, изъятие цифровых устройств, а также экспертные исследования в сфере информационных технологий. Понимание и грамотное применение данных тактических приемов позволяет существенно оптимизировать следственную работу, ускорить получение необходимой информации и обеспечить ее надежность и допустимость в уголовном процессе.

Подробное изучение типичных ситуаций на первоначальном этапе расследования киберпреступлений, детальный анализ алгоритмов действий следователя и выявление специфических тактических приемов являются ключевыми условиями для успешного раскрытия преступлений, совершенных с использованием информационных технологий. Это обусловливает актуальность и необходимость детальной разработки данного подраздела в контексте общей методики расследования киберпреступлений.

Каждое противоправное деяние обладает типичными для него следственными ситуациями, которые могут быть взяты в качестве образца при проведении следственных действий. Данные следственные ситуации помогают следователю предугадать, какие именно действия необходимо предпринять в конкретном случае, а также являются основной для планирования расследования.

Возгрин И.А. определяет следственную ситуацию как совокупность различных детерминантов, создающих определенную «картину

Джилкишиев Р.Б.

расследования», т.е. формируют определенный контекст на определенной стадии дела [112, с. 309].

Вышеобозначенные следственные ситуации по уголовным правонарушениям в сфере информационных технологий определяют основные направления, в рамках которых необходимо проведение дальнейшего расследования. Выбор оптимальной стратегии для организации и выполнения следственных действий зависит от понимания конкретной ситуации. То есть, следственные ситуации — это, своего рода, ориентир для следователя, благодаря которому возможна разработка эффективной стратегии расследования.

Первая следственная ситуация связана с дефицитом информации и требует от следователя сосредоточения на сборе дополнительных улик и сведений о подозреваемом лице.

Г.И. Повзренюком выделены четыре этапа установления личности: «подготовительный, аналитический, сравнительный и оценочный» [113, с.23].

Идентификация преступника, особенно в случае совершения преступления насильственного характера, представляется особо сложной. Она требует тщательного подхода, так как злоумышленник может быть абсолютно непредсказуемым и крайне опасным. Это делает расследование более сложным и рискованным, а задержание преступника требует слаженной работы правоохранительных органов (различных подразделений) и использование всех доступных ресурсов, профессиональных навыков и технических средств.

Оставаться неразоблаченным преступнику предположительно помогает высокий уровень технологических знаний и навыков, которыми он обладает. Благодаря этому, злоумышленник способен применять разнообразные методы и техники для защиты своей идентичности и сокрытия следов совершенного преступления.

Для проведения эффективной работы по установлению личности злоумышленника необходимо использование средств оперативной аналитики, помогающие выявлять закономерности, распознавать подозрительные активности, а также устанавливать связи между различными правонарушениями. Все это способствует более эффективной идентификации личностей злоумышленников.

В процессе расследования должны быть установлены следующие обстоятельства:

1) Объект, на который направлено противоправное деяние. В аспекте киберпреступности это может быть информация, личностные права, конфиденциальность и общественные интересы. Зачастую преступление может затрагивать сразу несколько объектов. К примеру, перехват личной корреспонденции может нарушать одновременно и права личности, и конфиденциальность данных.

2) Определение действия или бездействия, сведения о месте, времени и обстоятельств, при которых совершено противоправное деяние.

Джилкишиев Р.Б.

3) Определение реального масштаба нанесенного ущерба (вреда). Включает как материальную (финансовый ущерб, порча оборудования и пр.), так и нематериальную составляющую (моральный вред, репутационный ущерб).

4) Сбор доказательной базы (улик), указывающей на причастность подозреваемого (обвиняемого) к совершению противоправного деяния, т.е. выявление материальных и электронных следов.

5) Идентификация всех лиц, вовлеченных в совершение противоправного деяния, включая организаторов, непосредственных исполнителей и соучастников.

6) Установление пострадавших лиц, а также нахождение лиц, которые могут обладать значимой для следствия информацией.

К объектам, относящимся к предметам следственного осмотра рассматриваемой категории дел, относятся:

1) места (помещения) с находящимися автоматизированными информационно-вычислительными системами и техническим комплексом: серверные, кабинеты с рабочими станциями, системы связи, системы заземления и пр.;

2) вычислительные устройства, используемые для обработки данных: компьютеры, серверные и т.д.;

3) коммуникационные линии, посредством которых происходит передача данных: интернет-каналы, телефонные линии;

4) машинные носители информации: флэш-накопители, жесткие диски и прочие устройства, обеспечивающие хранение информации;

5) данные в соответствующих форматах, пригодных для автоматической обработки: текстовые файлы, программные коды, базы данных;

6) программы и системы, обеспечивающие автоматизированную обработку данных, а также правил и распределения обязанностей между должностными лицами.

В криминалистике следственные версии подразделяются на три группы: 1) общие следственные версии; 2) частные следственные версии; 3) рабочие следственные версии.

Предметом общих следственных версий являются событие правонарушения, квалификация его как правонарушения, виновность определенного лица в совершении данного правонарушения. Например, в связи с происшедшим неправомерным доступом к компьютерной информации, которая содержится на компьютере и тщательно охраняется уголовным законом. Неправомерный доступ влечет собой много последствий.

При определенных условиях могут быть построены версии о причинах неправомерного доступа к компьютерной информации: проникновение к компьютеру и влезание в его систему; удаление нужной информации, обладание ею, а также распространение; неправильная работа на компьютере; неосторожное обращение с компьютером. Это общие версии.

Событие правонарушения может быть доказано, но еще не ясно, кто его совершил. По одной следственной версии его мог совершить гр-н А., по другой - гр-н Б. и т.д.

Предметом общей следственной версии может быть и вопрос о том, совершил ли определенное действие данный гражданин, и вопрос о виновности конкретного лица в совершении этого действия.

Предметом частных следственных версий обычно являются отдельные обстоятельства по делу. Так, частные версии могут быть построены для выяснения способа, при помощи которого совершено правонарушение, для установления орудия, которым совершено правонарушение [114, с. 82].

В план действий необходимо включить мероприятия, направленные на идентификацию злоумышленников. К первоначальным и неотложным следственным действиям необходимо отнести следующее:

1) Осмотр места происшествия. Позволяет получить первичные сведения о противоправном деянии. Заключается в тщательном изучении обстановки, нахождении улик, изъятии информационных носителей, которые могут содержать доказательную базу.

2) Инструктаж лиц-участников осмотра. Проводится с целью ознакомления с правилами осуществления необходимых процедур и сохранения улик в рамках действующего законодательства.

3) Выемка и осмотр средств компьютерной техники. В ходе действия изымается и анализируется оборудование (компьютерная техника, носители информации) на момент нахождения электронных следов или документации, имеющей отношение к совершению преступления.

4) Допрос заявителя или потенциальных свидетелей. Проводится с целью получения ценной криминалистически значимой информации.

5) Назначение экспертиз. Тип конкретной экспертизы назначается в зависимости от обнаруженных улик.

Все последующие действия предпринимаются, исходя из дополнительных сведений, полученных в ходе первоначальных следственных действий.

Одним из ключевых моментов является точное определение перечня последовательности следственных действий для конкретной ситуации (версии), что аналогично разработке алгоритма, который, как математическая модель, способствует систематизации подхода к решению поставленных задач [115, с. 17].

Применение алгоритмов в правоприменительной практике имеет немаловажное значение, поскольку они помогают организовать и систематизировать процесс расследования, а также повысить квалификацию экспертов. Однако каждая следственная ситуация уникальна и предполагает индивидуальный подход. По мнению Возгрина И.А., алгоритмы не следует воспринимать как жесткие и категорические инструкции. Они должны предполагать гибкость действий, позволяя следователям действовать творчески и адаптировать свои действия к конкретным обстоятельствам [116, с. 190].

Джилкишиев Р.Б.

Таким образом, правоприменительная практика предполагает сочетание систематического подхода и творческой составляющей. Данная комбинация помогает организовать эффективную работу, особенно в такой области как киберпреступность.

Во втором случае следует продолжать собирать доказательства, чтобы противодействовать отказу от признания.

Б.Б. Нургалиевым выделены следующие общие задачи противодействия: «1) сокрытие информации о событии правонарушения; 2) сокрытие информации о виновности конкретного лица в совершении правонарушения 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) дискредитация добытых доказательств; 6) оказание психологического, физического воздействия на свидетелей, потерпевшего… следователя» [117, с. 27].

К обстоятельствам, подлежащим установлению в процессе расследования, относятся:

1) Поиск необходимых доказательств (улик), подтверждающих виновность или невиновность подозреваемого лица.

2) Проверка алиби. Предполагает подтверждение/опровержение нахождения подозреваемого лица в момент совершения противоправного деяния в другом месте.

3) Выяснение фактов нарушения процедуры при задержании подозреваемого лица или при работе со свидетелями и понятыми.

4) Проверка достоверности показаний подозреваемого лица.

Наиболее вероятными следственными версиями в данных условиях являются:

1) подозреваемое лицо намеренно лжет и искажает факты с целью избежать ответственности за совершенное преступление;

2) подозреваемое лицо на самом деле не имеет никакого отношения к совершению преступления.

Правильная тактика использования психологических приемов может кардинально изменить весь ход расследования: это поможет следователю не только найти необходимые доказательства, но и избежать предвзятости в отношении подозреваемого.

Для последовательного выполнения действий по сбору доказательной базы и установления фактов и виновных необходимо применить следующий алгоритм действий:

1) Осмотр места происшествия. Позволяет осуществлять фиксацию следов и улик, оставленных преступником.

2) Назначение экспертиз. Тип конкретной экспертизы назначается в зависимости от обнаруженных улик.

3) Поиск виртуальных следов, включающий анализ электронных данных, цифровых улик, фиксация сетевой активности.

Джилкишиев Р.Б.

4) Начало процедуры расследования на основании полученной информации о противоправном деянии.

5) Задержание причастного лица к совершению преступления с целью проведения допроса и выяснения обстоятельств дела.

6) Проверка подозреваемого лица на наличие судимостей по специальным базам данных, а также на наличие возможных связей с другими преступлениями.

7) Проведение допроса свидетелей и лиц, которым причинен ущерб, позволяющий собрать максимально полную информацию об обстоятельствах дела.

8) Проведение обыска по месту жительства и работы с целью поиска криминалистически значимой информации и улик в помещениях, где она может находиться.

В третьей ситуации необходимо сосредоточиться на изучении дополнительных деталей дела с учетом имеющихся признательных показаний.

Имеющаяся информация о личности преступника позволяет следователю сконцентрироваться на сборе доказательной базы и выяснении обстоятельств совершения преступного деяния. Следователем проводится тщательный анализ материалов, имеющихся в его распоряжении на момент полноты собранных материалов, соответствию норм действующего законодательства, что обеспечивает легитимность и допустимость собранной доказательной базы в суде. В случае выяснения, что определенные аспекты не охвачены или собранная информация недостаточна, следователь предпринимает необходимые меры для ее сбора, в том числе и при помощи негласных следственных действий (далее — НСД). Использование НСД (прослушка, негласные мероприятия и пр.) может быть оправдано в случае, если это приведет к получению важных доказательств или установлению дополнительных фактов по расследуемому делу.

Алгоритм расследования представлен в следующем виде:

1) Осмотр места происшествия. Позволяет собрать криминалистически значимую информацию, улики, доказательства с целью дальнейшего установления обстоятельств дела.

2) Проведение обысков (личные, на рабочих местах, по месту жительства). Действие преследует целью сбор дополнительных доказательств, имеющих непосредственное отношение к преступлению.

3) Инструктаж специалистов, осуществляющих процедуру осмотра. Проводится с целью ознакомления с правилами осуществления необходимых процедур и сохранения улик в рамках действующего законодательства.

4) Допросы лиц со статусом «свидетель», «потерпевший», «свидетель с правом на защиту». Проводятся с целью уточнения фактов, установления мотивов и взаимосвязи между участниками.

Джилкишиев Р.Б.

5) Выемка и осмотр вещественных доказательств (в письменной форме). Позволяет извлекать, изучать и подвергать документированию полученные улики.

6) Допрос лиц, фигурирующих в документах, с целью выяснения их роли, возможной ответственности.

7) Истребование документов и нормативных актов, которые позволят понять возможные нарушения правил и законов организациями, где было совершено преступление.

8) Назначение судебных экспертиз с целью подтверждения или опровержения выдвинутых версий следствия.

9) Анализ полученной информации. Проводится с целью ревизии или проверки имеющейся информации, что может прояснить ситуацию или назначить дополнительные проверки.

Следственные действия на данном этапе носят бесконфликтный характер, т.е. без каких-либо явных конфликтных ситуаций между следственными органами и подозреваемыми. Тем не менее, в ходе судебных заседаний все же могут возникать ситуации, когда подсудимые отказываются от ранее данных показаний, обвиняя при этом органы расследования в предвзятости и применении к ним давления. Чтобы понимать поведение подсудимых, заранее предположить возможную реакцию и дать ей оценку, следователю необходимо рассматривать ситуацию с точки зрения и эмоций подсудимых. То есть, следователи и адвокаты должны брать во внимание типичные человеческие реакции, которые могут осложнять процесс получения показаний.

К обстоятельствам, подлежащим установлению, относятся:

1) Поиск доказательств, которые подтверждают либо опровергают вину подозреваемого.

2) Определение всех участников преступления (организаторы, исполнители, соучастники).

3) Установление первопричин и условий, создавших возможность для совершения преступления.

Наиболее типичными следственными версиями могут быть:

1) Подозреваемый осознал противоправность совершенных им действий и оказывает содействие следствию.

2) Подозреваемый принимает на себя вину, тем самым, оговаривая себя и покрывая соучастников, с целью получения какой-либо выгоды (материальная помощь, протекция), надеясь на получение минимального срока наказания.

3) Подозреваемый умышленно дает ложные показания, оговаривая себя, из-за запугивания со стороны соучастников, надеясь на получение определенных благ.

Наиболее логичным тактическим решением в данной следственной ситуации является уточнение следователем характера взаимоотношений подозреваемого и потерпевшей стороны с целью установления реальных мотивов и первопричин, приведших к конфликту. Также необходимо выяснить

Джилкишиев Р.Б.

наличие у подозреваемого определенных навыков и знаний, которые способствовали совершению преступления в сфере информационных технологий и киберпреступности. Это поможет сформировать верную тактику и стратегию взаимодействия с подозреваемым лицом, а также сформировать целостную картину произошедшего.

Как показывает практика, немаловажное значение имеют действия собственников информационных систем в вопросах информирования произошедшего преступления. Между указанными лицами и правоохранительными органами могут развиться следующие сценарии взаимодействия [118, с.100-101].

1) Нарушение целостности и конфиденциальности информации было обнаружено собственником информационной системы, а также выявлено лицо, виновное в совершении данных нарушений, о чем было незамедлительно заявлено в правоохранительные органы. Данная следственная ситуация — наиболее благоприятная для следствия, поскольку следственным органам представлена полная информация как о нарушении, так и о виновном лице.

2) Нарушение целостности и конфиденциальности информации было обнаружено собственником информационной системы, однако виновное лицо не было установлено, о чем было незамедлительно заявлено в правоохранительные органы. Данная следственная ситуация предполагает более низкую эффективность расследования, так как правоохранительные органы не обладают информацией о виновном.

3) Нарушение целостности и конфиденциальной информации было обнаружено правоохранительными органами в ходе проведения оперативно-розыскных мероприятий в рамках расследования другого дела. При таком положении дел следствию придется приложить больше усилий для сбора данных о нарушениях и установлении виновных лиц.

В случае наличия подозреваемого лица, первоначальной задачей следствия является фиксация следующих доказательств:

- факт изменения, уничтожения информации или неправомерного доступа к ней;
- объем нанесенного ущерба (финансовый, репутационный);
- действия, которые привели к нарушению целостности или конфиденциальности информации, т.е. причинно-следственную связь между действиями и последствиями;
- вовлеченность подозреваемого в нарушение и осознанность им совершенных преступных действий и их последствий.

В случае если злоумышленник пойман на месте совершения преступления или некоторое время позже, первоначальные следственные действия выглядят следующим образом:

1) Проведение обыска задержанного с целью поиска вещественных доказательств, находящихся при нем.

2) Проведение допроса с целью получения информации о мотивах и обстоятельствах совершения противоправного деяния. В контексте

Джилкишиев Р.Б.

киберпреступлений вопросы могут касаться способа осуществления доступа к системе, использованных инструментов и пр.

3) Проведение обыска по месту жительства с целью обнаружения дополнительных доказательств, улик и прочей криминалистически значимой информации.

Типичными следственными действиями также могут быть осмотр и фиксация состояния и работы оборудования, которое могло быть задействовано при совершении преступления (компьютерная техника, сети, сервера, носители информации); допрос очевидцев, а также лиц, ответственных за работу информационных систем, в том числе должностных лиц и собственников систем.

Выемка документов и фиксация состояния рабочего места — критически важные следственные действия.

Выемка документов подразумевает сбор и анализ документов, в которых может содержаться информация о состоянии системы в момент совершения атак или последствий вторжения.

Фиксация состояния рабочего места проводится с целью обнаружения следов действий преступника. Здесь крайне важно зафиксировать состояние устройств, использованных злоумышленником для доступа к информационной системе. Следы могут быть обнаружены также вне рабочего места — по месту жительства злоумышленника, где установлена соответствующая техника.

В случае если подозреваемый не установлен, в первую очередь следственными органами проводится работа с собственником информационной работы с целью получения сведений о произошедшем инциденте. Следователем осуществляется сбор данных с их последующей фиксацией в соответствии с процессуальными нормами. Также необходимо определить поиск места входа в систему, т.е. каким именно образом был получен доступ к системе, а также пути следования злоумышленников.

К типичным следственным версиям можно отнести следующее:

- имел место факт совершения преступления, исходя из имеющихся первичных материалов;
- преступление не было совершено, а заявитель добросовестно заблуждается;
- преступление не было совершено, но заявитель намеренно предоставил ложную информацию о факте его совершения.

Следственным органам необходимо выбрать, на что они будут направлять свои усилия, т.е. определиться с выбором цели тактического воздействия. Следственная ситуация может состоять из множества элементов (улики, подозреваемые, свидетели и пр.). Чтобы добиться наиболее эффективного результата, следователь может акцентировать свою работу на каждом из них. Для достижения целей могут быть использованы конкретные инструменты и подходы.

Джилкишиев Р.Б.

Основными следственными действиями, позволяющими получить криминалистически значимые показания от подозреваемых, свидетелей или потерпевших, являются:

- Допрос. Эффективность данного действия зависит от опыта следователя, его способности использовать различные методы для задавания вопросов и интерпретации полученных ответов.
- Очная ставка. Способствует выявлению возможных противоречий в показаниях при встрече свидетелей или подозреваемых лицом к лицу.
- Проверка показаний на месте. Предполагает возврат на место совершения преступления с целью перепроверить или уточнить показания.
- Опознание. Используется для установления подозреваемых лиц или объектов, имеющих непосредственное отношение к совершению преступления.

К общим принципам тактики проведения данных следственных действий относятся:

- понимание психологии и учет психологических аспектов общения с людьми;
- четкое понимание и определение конкретных целей и задач;
- детальное изучение личностных данных опрашиваемых;
- технико-криминалистическая подготовка следователя к проведению следственных действий;
- проведение следственных действий с использованием средств аудио-, видеозаписи.

Допрос потерпевшего и свидетелей. Качество допроса потерпевших и свидетелей является ключевым моментом в расследовании преступлений в сфере информационных технологий. Результатом некачественно проведенного следственного действия может стать неправильное восприятие ситуации, упущенные криминалистически значимые детали, получение недостоверной информации. Как уже неоднократно подчеркнуто, киберпреступления имеют свою специфику, поэтому крайне важно, чтобы следователи, привлеченные к допросу, имели достаточный объем знаний, навыков и опыта. Причем следователь должен иметь не только лишь юридическое образование, но и соответствующие знания в сфере информационных технологий, как специфическая терминология, технология и методы работы. При необходимости, в случае отсутствия у следователя достаточного опыта и знаний, к следственному действию могут быть привлечены соответствующие специалисты.

Под допросом следует понимать процесс, в ходе которого следственные или судебные органы получают сведения, имеющие отношение к расследуемому уголовному делу, от лица, обладающего криминалистически важными фактами. Допрос проводится в соответствии с правилами и нормами УПК, а информация, получаемая в ходе данного следственного действия, должна быть значимой для правильного разрешения уголовного дела [119, с. 27].

Джилкишиев Р.Б.

В случае если злоумышленник известен, основной задачей допроса является выяснение всех обстоятельств произошедшего противоправного деяния. Если же его личность не установлена, то ключевым моментом является выяснение всей необходимой информации (приметы, личностные характеристики, поведенческие особенности и пр.), которые бы облегчили поиск злоумышленника. Обычно, в первую очередь, данное следственное действие проводят в отношении заявителя (потерпевшего), а затем допрашивают свидетелей.

При допросе потерпевших и (или) свидетелей в контексте рассматриваемого вида преступлений, ставятся следующие тактические задачи, выявление элементов состава противоправного деяния, установление места, времени и обстоятельств совершения преступления, способы и мотивы совершения противоправного деяния, выяснение сопутствующих обстоятельств, сбор сведений о внешнем облике подозреваемых лиц и (или) непосредственных участников совершения преступления, определение объекта преступного посягательства, определение величины причиненного ущерба, точный список украденных вещей с указанием отличительных характеристик, установление свидетелей и иных, причастных к совершению преступления лиц [120, с. 92].

Подготовка к допросу и его эффективное проведение во многом зависит от последовательного выполнения определенных этапов. Конкретизированный порядок подготовки и проведения допроса по противоправным деяниям в сфере информационных технологий выглядит следующим образом:

1) ознакомление следователя с уже собранной доказательной базой, полученной с использованием иных методов;

2) ознакомление и изучение личностных характеристик, психологических особенностей и прочих личных данных допрашиваемого;

3) подготовка доказательств и материалов для составления более точного опросника;

4) составление структуры (плана) допроса, концентрация на ключевых вопросах и основных аспектах дела;

5) подготовка оборудования для проведения и фиксации допроса.

Осмотр места происшествия. Данное следственное действие является одним из первостепенных и неотложных. Зачастую, осмотр места происшествия осуществляется незамедлительно после сообщения о совершении противоправного деяния. Особенно это актуально и при расследовании киберпреступления, где доказательства могут быть не только физическими, но и цифровыми. Целью осмотра является обнаружение следов, подтверждающих совершение происшествия или лиц, причастных к нему.

Как показала практика, осмотр места происшествия по исследуемому составу преступления ограничивается описанием помещения, где находится техника и изъятием ее. При этом совершенно забывая о том, что существуют и способы подключения и проникновения в компьютер извне, такие как:

Джилкишиев Р.Б.

видеокамеры, считывающие устройства и др., а также нельзя исключать проникновение преступников в помещения и оставление следов в нем.

Как правило, при осмотре места происшествия акцент делается на нахождении физических улик, которые могут указать на лицо, совершившее преступление. В контексте киберпреступлений это может быть поиск документов, технических устройств, информационных носителей, следов, оставленных на клавиатуре, и прочих материальных объектов. Следы могут быть обнаружены не только в непосредственном месте совершения преступления, но и на близлежащей территории. Крайне важно составить описание окружающей обстановки, даже если материальные следы не были обнаружены. Нахождение определенных предметов, устройств может натолкнуть следователя на то, как и при помощи каких средств совершено противоправное деяние. Следует акцентировать внимание на любые предметы, оставленные подозреваемым, или от которых он избавился.

Осмотр места происшествия настолько значимый источник информации, что расследование многих видов правонарушений не может обойтись без проведения данного следственного действия. Необходимости применения приемов по воссозданию обстановки и обстоятельств происшествия для решения задач расследования при осмотре места происшествия посвящена работа Попова В.И., Бегалиева К.Е. [121, с.60-67].

Данное следственное действие имеет свои особенности при расследовании преступлений в сфере информационных технологий.

Во-первых, при расследовании рассматриваемой категории преступлений следователь не может ограничиваться лишь своим восприятием объектов. Сбор и анализ данных требует применения специализированного оборудования (программное, техническое) и инструментов.

Во-вторых, расследование преступлений в сфере информационных технологий требует от следователя не простого пассивного наблюдения за применением ввода команд при поиске улик, но и активного самостоятельного (через специалиста) взаимодействия с информационными системами, производя считывание данных из систем, вывод информации на бумажные носители или экран, выполнение программ с целью вызова реакций за соответствующие запросы и пр. Таким образом, следователь взаимодействует с киберпространством, играя проактивную роль, что способствует оперативному получению информации.

При расследовании преступлений в сфере информационных технологий от следователя требуется не только применение традиционных следственных навыков, но и глубокое понимание специфики рассматриваемого вида противоправного деяния. Таким образом, он не должен ограничиваться лишь сбором фактов, он должен осознать саму суть правонарушения. Осознание того, в чем заключается само правонарушение, может повлиять на все последующие следственные действия и принимаемые решения. Также следователь должен обладать достаточным уровнем знаний, чтобы разбираться в принципе функционирования систематизированных информационных систем.

Джилкишиев Р.Б.

Расследование преступлений в сфере информационных технологий накладывает свою специфику и на такое следственное действие как осмотр. Следственный осмотр требует особого внимания к правовым аспектам [122, с. 40]. В контексте расследования киберпреступлений это может отражаться в виде вмешательства в информационные системы и личные данные граждан или организаций. В процессе осмотра следователь может столкнуться с проблемой доступа к помещениям, где находятся автоматизированные системы, так как они могут принадлежать на праве собственности третьим лицам или организациям. Следовательно, чтобы осуществить рассматриваемое следственное действие, следователю необходимо строгое соблюдение норм законодательства, регулирующих доступ и проникновение.

Более того, в процессе осмотра следователь вынужден работать с информацией, составляющей коммерческую тайну, или персональными данными. Это, в свою очередь, вынуждает его действовать в рамках закона о защите личной информации, что может создать дополнительные правовые и этические вопросы.

Следственное действие в таких критически важных областях, как банковская сфера, телекоммуникации и энергетические системы, государственные управление может привести к материальным убыткам учреждений и их клиентов, поскольку осмотр компьютерных систем может вызвать необходимость отключения их функционирования.

Расследования преступлений в сфере компьютерной информации требуют тщательной подготовки, поскольку осмотр в указанной области проводится, как правило, однократно. Конечно, осмотр может быть проведен и несколько раз, однако его информативность будет значительно снижена, поскольку важные следы могут быть изменены или уничтожены, а количество материальных улик ограничено. Планирование осмотра предполагает не только непосредственный осмотр, но и сбор необходимой информации и ресурсов заранее, поскольку такие факторы как скорость и эффективность проведения осмотра являются ключевыми и имеют критическое значение.

Особенности осмотра места происшествия. Следственный осмотр — важный процесс, предполагающий выявление обстоятельств и фактов, значимых для дела. Одна из основных задач осмотра заключается в выяснении, совершено ли преступление в отношении компьютерной информации, т.е. верно классифицировать преступление для правильного направления расследования. Следователь должен определить, была ли компьютерная техника использована для совершения противоправного деяния или же оно само связано непосредственно с использованием компьютеров как основного объекта. Определение сущности преступления является ключевым моментом, так как от этого зависит вектор следствия, а также правомерность возбуждения уголовного дела в принципе.

При совершении компьютерных преступлений в качестве объекта посягательства выступает непосредственно система обработки информации. Это может быть персональный компьютер (далее — ПК), сети, сервера,

Джилкишиев Р.Б.

которые содержат конфиденциальную информацию т.е. данные средства образуют основу для совершения противоправного деяния. Очень часто ПК и локальные сети используются для неправомерного доступа к другим системам и компьютерам, находящимся на дальнем расстоянии друг от друга. К примеру, большинство несанкционированного доступа к защищенной информации в Пентагоне и NASA было осуществлено именно таким путем, т.е. через сеть интернет с использованием промежуточных систем — компьютеров, находящихся на разных континентах. При этом данные промежуточные системы принадлежали абсолютно сторонним фирмам, организациям и даже учебным организациям, не имеющим ничего общего с преступной деятельностью. Таким образом, можно смело утверждать, что злоумышленники в своей деятельности могут использовать инфраструктуру, принадлежащую другим лицам, без ведома последних, что в значительной степени усложняет поиск преступников и процесс расследования.

В зависимости от роли осматриваемого объекта зависят подходы, которые будут использоваться при расследовании. Если объект осмотра — конечное звено в цепочке преступления, следовательно, именно он и есть цель преступного деяния. В таком случае необходимо установить пользователя данного объекта, лиц, имеющих доступ к нему или информации, хранящейся на нем, а также определить способы, при помощи которых используются результаты автоматизированной обработки информации в этом объекте. Если же осматриваемый объект — промежуточное звено, необходимо, прежде всего, установить наличие связей (информационных, технологических) с другими объектами в киберпространстве, а, во-вторых, определить, при каких условиях возникли и поддерживаются данные связи [115, с. 30].

Использование различных технических средств следователем повышает эффективность расследования преступлений в области компьютерных технологий. Это могут быть компьютеры, планшеты, видеокамеры, фотоаппараты и пр. При их помощи осуществляется фиксация объектов, мест, доказательств, важных и имеющих значение для следствия. Это актуально особенно, когда осуществить процедуру изъятия не представляется возможным (графическое изображение, надписи и прочие визуальные элементы). В случае, если преступление происходит в интернете в конкретный момент времени, зафиксировать его возможно при помощи снимков экрана (скриншотов). Скриншоты могут использоваться с целью фиксации и сохранения сообщений, изображений, различных веб-страниц, чатов, т.е. информации, которая может быть подвержена изменению или удалению после совершения преступления.

Если преступление совершено при помощи сети интернет, следственными органами может быть направлен соответствующий запрос в Интерпол, так как поскольку преступление имеет транснациональный характер, информация о злоумышленниках может находиться в юрисдикции другого государства. Варианты информации, которая может быть направлена в ответ на данный запрос, выглядят следующим образом:

Джилкишиев Р.Б.

- предоставлены сетевые адреса, имена доменов, серверов. Данная информация позволяет установить, сайты и сервисы, через которые осуществлялись преступные деяния. Информация о доменах и IP-адресах поможет отслеживать активность пользователей;

- предоставлено содержание протоколов и логических файлов. Могут содержать записи о действиях пользователей в сети: время входа и нахождения в интернете, посещенные страницы и пр., что может помочь в установлении хронологии событий и нахождении злоумышленников;

- предоставлена информация о провайдерах и дистрибьютерах услуг. Позволяет определить места нахождения пользователей, выявить лиц, которые ответственны за распространение заведомо ложных сведений или сведений, порочащих честь и достоинство.

Допрос подозреваемого. Данное следственное действие необходимо проводить как можно скорее, после непосредственного задержания подозреваемого. Задержка в допросе может дать злоумышленнику дополнительное время для построения линии защиты или подготовки выгодных для себя объяснений, что может значительно усложнить работу следственных органов и затруднить установление истины. Следователю стоит заблаговременно ознакомиться с материалами дела, что позволит ему сформулировать правильные вопросы, уточнить детали. Это может помочь правильно понять обстановку и выявить возможные противоречия в показаниях подозреваемого. Также следует учесть, что допрос подозреваемого необходимо проводить после допроса свидетелей или потерпевших, так как это дает возможность выявить ключевые моменты, способные подтвердить или опровергнуть показания подозреваемого лица [122, с. 40].

В процессе допроса следователю важно соблюдать правовые, этические и моральные нормы. Следственные органы обязаны действовать исключительно в рамках закона, т.е. все тактические методы и приемы, а также их комбинации, должны соответствовать уголовно-процессуальному законодательству. Следователю необходимо избегать действий, которые могут быть восприняты как манипуляция или психологическое давление, или насилие.

Процедуру опроса подозреваемого следует проводить тогда, когда следственные органы располагают очевидными доказательствами причастности данного лица к совершению противоправного деяния, за исключением случаев, когда злоумышленник пойман с поличным. То есть следователь должен иметь достаточно информации, полученной в ходе проведения следственных действий, например, показания свидетелей, потерпевших и пр. На допросе следователь должен выяснить следующие моменты:

1) Обстоятельства, при которых подозреваемый оказался на месте совершения преступления (когда, с кем, каким образом). Это позволяет дать оценку его роли в совершении преступления, а также возможное алиби.

2) Чем подозреваемый был занят до начала совершения преступления. Дает понимание возможных мотивов, а также поведения в момент непосредственного совершения противоправного деяния.

3) Что заставило подозреваемого пойти на совершение преступления. Также может понять мотивацию подозреваемого, дает понять, было ли преступление спровоцировано.

4) Знал ли подозреваемый потерпевшего до совершения преступления. Дает понимание о существовании возможных конфликтов между потерпевшим и подозреваемым.

5) Степень отношения между потерпевшим и злоумышленником. Может помочь в оценке мотивов преступления.

6) Уточнение взаимоотношений, в случае если они были враждебные, в чем конкретно это выражалось. Может выявить информацию о возможном конфликте, приведшем к совершению преступления.

7) Психологическое и эмоциональное состояние подозреваемого в момент совершения преступления. Помогает понять действия подозреваемого в момент совершения преступления.

8) Физическое состояние подозреваемого (алкогольное, наркотическое опьянение. Помогает объяснить поведение подозреваемого.

Результаты данного следственного действия могут различаться, исходя из ряда факторов: признание или уклонение от признания, наличие собранной доказательной базы (веские, слабы доказательства). Если подозреваемый сотрудничает со следствием, давая правдивые показания, задача следователя заключается в получении максимально полной информации о произошедшем событии.

В случае нежелания подозреваемого идти на контакт, когда он продолжает отрицать свою вину, следователю необходимо предъявить имеющуюся в его расположении доказательную базу.

В случаях конфликтных ситуаций, эффективным тактическим приемом со стороны следователя будет приглашение для участия в допросе специалиста в области информационно-коммуникационных технологий. Привлечение подобного специалиста особенно полезно, когда доказательства связаны с технологическими аспектами и существует необходимость объяснения сложных технических моментов. Чтобы доказать ошибочность утверждений подозреваемого, следователем могут быть предоставлены следующие материалы:

а) протокол осмотра места происшествия, содержащаяся информация в котором может с успехом опровергнуть ложные показания подозреваемого лица;

б) свидетельские показания очевидцев;

в) протоколы допросов потерпевшего и свидетелей, содержащие информацию, позволяющую раскрыть несоответствия в показаниях;

г) изъятые при обыске технические средства, при помощи которых совершено преступление (могут побудить подозреваемого признаться в содеянном);

д) протоколы очных ставок соучастников, информация в которых противоречива;

Джилкишиев Р.Б.

е) экспертные заключения, дающие дополнительную аргументацию.

Представленные материалы могут выступать не только в качестве доказательств, но как инструмент, побуждающий к даче правдивых показаний подозреваемым.

Совершение преступлений в сфере информационных технологий сопряжено с высокой степенью профессионализма и использованием специфических знаний преступниками. Следователю необходимо установить, каким образом подозреваемый приобрел соответствующие навыки и знания. Запросы могут касаться места обучения (институты, специализированные курсы, специализированные учебные заведения), трудовой деятельности, круга общения, характеристик с места жительства и работы. Полученная информация может дать разъяснения, как подозреваемый мог совершить киберпреступление. Понимание круга общения подозреваемого дает представление об интересах подозреваемого, его наклонностях, привычках. Представленные характеристики дают возможность получить ценные данные об образе жизни подозреваемого, его социальных контактах, поведении, а также оценочные суждения его окружения.

Немаловажным является выяснение уголовного прошлого подозреваемого, привлекался ли он к административной, уголовной ответственности, особенно в контексте совершения преступлений в сфере информационных технологий. Это крайне важно для понимания опыта подозреваемого в сфере киберправонарушений: информация, где, когда и за что был привлечен подозреваемый, может помочь сформировать образ преступника, а также выявить предрасположенность к совершению преступлений.

Немаловажным следственным действием является проведение очной ставки, главной целью которого является достижение большей ясности и согласованности в доказательствах, а также выявление истины через уточнения и допущения.

Осмотр предметов. В контексте расследования киберпреступлений это является важной процедурой, способствующей сбору доказательной базы, установлению фактов, которые имеют отношение к совершению преступления. Как правило, осмотру подвергаются различные традиционные и электронные носители информации: письма, записки, электронные письма, сообщения из чатов, информация с сайтов, записи телефонных передач, разговоров.

Полное изъятие предметов правонарушения с подробным отчетом способствует проведению глубокого анализа данных, находящихся на устройствах, и является наилучшим вариантом при проведении осмотра предметов.

При изъятии информационных файлов (пароли, журналы доступа, настройки конфигурации систем, вирусы, модифицированные программы) в обязательном порядке необходимо учитывать их специфику. Изъятие должно сопровождаться тщательным протоколированием с учетом следующих моментов:

Джилкишиев Р.Б.

- дата и время;
- ФИО участников операции;
- описание каждого файла в контексте его значения для расследования.

При изъятии необходимо получить и сохранить информацию по всем атрибутам:

- дату создания и модификации, позволяющей установить хронологию событий;
- владельца файла, у которого есть доступ файла;
- размер файла;
- место хранения.

Таким образом, при изъятии информационных файлов необходимо быть предельно внимательным к деталям, а также точности соблюдения процедур. Это позволит обеспечить целостность и достоверность доказательств, а также законность и состоятельность расследования.

Злоумышленники, совершившие преступление в сфере компьютерных технологий, могут предпринять быстрые действия для удаления или зашифровки данных для сокрытия своих преступных действий. При помощи всего лишь пары команд возможно уничтожение больших объемов информации, в том числе на жестких дисках, флэш-картах или других носителях. Это может поставить дальнейшее расследование под угрозу. Таким образом, неотложность следственного осмотра является критически важным моментом.

Главенствующую роль в проведении следственного осмотра должна быть закреплена за следователем. Именно он несет ответственность за весь процесс, включая принятие решений и обеспечение правильности, тщательности и качественности выполнения всех необходимых процедур.

К проведению осмотра могут привлекаться прочие лица, как понятые, эксперты, работники дознания, представители прокуратуры. Количество участников напрямую зависит от сложности дела, разнообразия улик и необходимости проведения специализированного анализа.

Как уже отмечалось ранее, следственный осмотр требует наличия четкого плана, учитывающего все детали предстоящих действий. Помимо фиксации традиционных следов (отпечатки пальцев, микрочастицы и пр.), пристальное внимание необходимо уделять устройствам, которые могут содержать данные и которые могут быть источником получения улик (жесткие диски, флэш-накопители, иные виды магнитных носителей). Здесь необходимо также помнить, что объекты компьютерной информации имеют свою специфику и внутренние структуры, состоящие, зачастую, из множества взаимосвязанных компонентов. Осмотр предполагает фиксацию основных элементов устройства, их конфигурацию, взаимосвязи и соединения. Необходимо понимать, что в отличие от традиционных улик (оружие, наркотики и пр.), информация не имеет столь однозначных характеристики и требует более детального описания функционала и анализа, т.е. подготовка должна включать не только понимание объектов, но и их функциональность.

Джилкишиев Р.Б.

В качестве примера приведем некоторые детали расследования одного из уголовных дел в сфере информационных технологий, а именно подделка денежных знаков с использованием компьютерной и периферийной техники. В ходе следственного действия произведен осмотр персонального компьютера и струйного принтера, при этом протокол следственного осмотра содержал поверхностное документирование на основе традиционных характеристик, как «металлический объект прямоугольной формы, выкрашенный в белый цвет», «фрагмент списка файла с изображением денежных купюр», «файлы графического редактора, способного создавать, модифицировать и распечатывать графические изображения». На основе данного описания, следствие сделало вывод, что именно данный компьютер был использован для изготовления поддельных купюр. Однако следствием не были учтены все технические аспекты и нюансы. Более того, обвиняемые показали, что изображения были распечатаны на другом персональном компьютере и в другом месте, а осматриваемый компьютер был просто местом хранения, а не местом совершения преступления, а графический редактор являлся лишь инструментом проверки целостности файлов [117]. Этот случай наглядно иллюстрирует, что следствию необходимо учитывать не только физические характеристики устройств, но и их занятость в процессах, поскольку неверная интерпретация информации и игнорирование иных возможностей использования устройств могут привести следствие к необоснованным и ложным выводам и ошибочным обвинениям.

Данный пример также демонстрирует, что к неправильным выводам может привести недостаточное понимание динамики работы вычислительного средства, т.е. простая фиксация физических характеристик будет недостаточной. Подробное описание технических средств, занесенное в протокол, должно включать и ограничиваться такими моментами, как порядок работы осматриваемого устройства, каким именно образом оно функционирует и какие процессы в нем происходят; с какой основной целью используется устройство; каким образом устройство может быть использовано для совершения преступления. Для определения же правильного назначения, описания функций, действий, которые могут совершаться при помощи данного устройства, необходима оценка квалифицированного специалиста, способного определить, могло ли данное устройство использоваться при совершении конкретного противоправного деяния. В случае участия в смотре подозреваемых и свидетелей, их пояснения также должны быть запротоколированы.

Обыск — это одно из оперативных следственных действий, проводимых по месту работы или жительства подозреваемого. Как и следственный осмотр, данное действие направлено на выявление доказательств. Следовательно, основной целью обыска является обнаружение объектов, содержащих информацию, связанную с правонарушением (персональные компьютеры, носители информации, документы и. пр.). Объекты, которые представляют интерес для следствия, при наличии основания могут быть изъяты. Изъятию

Джилкишиев Р.Б.

подлежат устройства, программы, документы, предметы, имеющие отношение к совершению преступления, прямо или косвенно подтверждающие совершение преступления. Все изъятое должно быть в обязательном порядке приобщено к делу. Исходя из специфики киберпреступлений, в рассматриваемом следственном действии могут принимать участие специалисты в области информационно-коммуникационных технологий. Их основная задача — оказать профессиональную помощь при изъятии и проведении анализа технических устройств и данных с целью понимания, каким образом они могли быть использованы в преступных действиях.

Обыск может быть первичным или повторным. Первичный или первоначальный обыск — это обыск, проводимый с целью выявления и изъятия информации и объектов, которые имеют непосредственную связь с преступлением. Повторный обыск в контексте рассматриваемого вида преступлений, как правило, не проводится, ввиду его низкой эффективности. При проведении обыска в рамках расследования традиционных преступлений повторный обыск проводится в случаях появления новой информации о материальных объектах, которые не были обнаружены при первичном осмотре. При расследовании же киберпреступлений, первоочередное значение имеет информация, хранящаяся на материальном объекте, и которая может быть удалена или изменена при помощи стандартных средств или посредством внешних воздействий (электромагнитное воздействие). «Традиционная информация» при расследовании традиционного преступления может сохраняться в своем первоначальном виде достаточно долго (следы крови, физические улики). Информация же, связанная с совершением киберпреступления, при каждом новом использовании материального объекта подвергается риску изменения или уничтожения. Тем не менее, несмотря на нецелесообразность проведения повторного обыска (в большинстве случаев), существуют исключения. Повторный обыск может оказаться эффективным в случае, когда после первичного обыска материальный объект не работал и к нему был ограничен доступ третьих лиц. В таком случае, с определенной долей вероятности, данные могут оставаться в неизменном виде, что делает повторный обыск оправданным [113, с. 50].

Одной из распространенных проблем, с которой сталкивается следователь при расследовании рассматриваемого вида преступления — огромный объем данных, представленных в различных форматах. Это значительно затрудняет их оценку, а также требует наличия специальных знаний для понимания и проведения анализа. Также, довольно часто, следователь просто не способен самостоятельно оценить важность найденного, так как не имеет достаточно навыков работы с информационными технологиями. Исходя из всего вышеперечисленного, следователями часто принимаются решения об изъятии всех носителей, которые, возможно, могут содержать криминалистически значимые данные. Имея определенный практический опыт, некоторые следователи действуют проактивно и изымают не только отдельные материальные объекты и их компоненты, но и целые

Джилкишиев Р.Б.

системные блоки. Мы считаем данные действия целесообразными, поскольку таким образом можно обеспечить защиту системного блока от потенциальных проблем, связанных с совместимостью материнской платы и процессора, а также позволить осуществить более детальный и глубокий анализ, так как системный блок предоставляет доступ ко всем устройствам (дисководы, компакт-диски и пр.) [106, с.44].

Порядок проведения обыска предполагает присутствие понятых, задача которых подтвердить законность действия следственных органов и удостоверить факты, вскрывшиеся (обнаруженные) во время следственного действия. Следователь обязан проводить обыск в присутствии лица, у которого данный обыск проводится. В случае его отсутствия при обыске присутствуют его совершеннолетние члены семьи. Если обеспечить вышеуказанные категории не предоставляется возможным, необходимо пригласить представителей ЖЭКа, эксплуатационной организации или органа местного самоуправления с целью соблюдения законности и контроля за действием следственных органов. В случае проведения обыска в помещениях, принадлежащих учреждениям (предприятиям, организациям), в обязательном порядке необходимо обеспечить присутствие их представителей.

Критически важным является привлечение эксперта (специалиста) в области компьютерной безопасности в случае наличия затруднений технического характера, когда следователь не может преодолеть их самостоятельно. Это может быть наличие пароля или нежелание лица, у которого происходит обыск, сообщать данный пароль [123, с. 12-16].

При проведении рассматриваемого следственного действия следователь может остановиться лишь на изъятии добровольно предоставленных предметов и информации. Данная практика более актуальна именно для расследования киберпреступлений, когда следователь сталкивается с данными, хранящимися в цифровом формате, или когда информация может быть легко предоставлена. Здесь важно четкое определение целей, с которыми проводится обыск.

Данная ситуация, когда следователь изымает лишь добровольно предоставленные материальные объекты или информацию, делает обыск схожим с процедурой выемки, которая подразумевает поиск или изъятие конкретных предметов. В то время как обыск представляет собой более емкое следственное действие.

В рамках расследования киберпреступлений следователь может столкнуться с новыми объектами и местами производства выемок. К ним можно отнести не только физические носители информации, но и электронную информацию, которая может храниться на удаленных серверах или облачных хранилищах. Работа с таким форматом требует от следователя дополнительных знаний и навыков для верной интерпретации полученных результатов и обеспечения законности в процессе изъятия.

Следующий этап следственных действий предполагает допрос подозреваемых лиц, обвиняемых лиц, проведение очных ставок, опознание, а также, при необходимости, назначение соответствующих экспертиз [124].

Джилкишиев Р.Б.

Назначение судебных экспертиз. Одним из важных доказательств по делам о правонарушении в сфере информационных технологий и киберпреступности, является заключение эксперта.

В рамках расследования киберпреступлений могут назначаться следующие виды экспертиз:

- *Технико-криминалистическая* (в отношении документов). Позволяет выявлять факты частичного добавления, удаления информации в документе, что может указывать на фальсификацию.

- *Трасологическая.* Проводится в случае обнаружения таких следов, как отпечатки пальцев, рук, ног, обуви, частицы одежды [125, с. 24].

- *Компьютерно-техническая*. Дает возможность установить личность создателя документа или источника информации. В качестве объектов экспертизы рассматриваются файлы в графическом и текстовом формате, графические изображения, где анализу подвергаются метаданные, а также содержание (аудио-, видеофайлы, записи разговоров и прочий мультимедийный контент, различные носители информации). Данный вид экспертизы может быть назначен в случаях подделки документов, несанкционированного доступа к информации и прочих случаях, требующих проведения анализа данных. Компьютерно-техническая экспертиза позволяет провести анализ аномальной сетевой активности и время проведения атак. При проведении экспертизы ключевое значение имеют лог-файлы, содержащие записи всех интернет-соединений, запросов к компьютеру жертвы, в том числе IP-адреса, с которых поступали запросы. После анализа экспертами лог-файлов задача следователя заключается в идентификации владельцев IP-адресов. В рамках данного следственного действия следователь может столкнуться с проблемами динамических IP-адресов, которые могут принадлежать большому числу клиентов. Также экспертом может проводиться анализ устройств на предмет наличия вредоносного ПО (вирусы, трояны и пр.). При обнаружении подозрительных приложений экспертом проводится их декомплирование с целью дальнейшего изучения внутреннего кода. Посредством анализа возможно выяснение IP-адреса, куда вредоносное программы отправляют компрометированную информацию [126].

- С*удебно-фоноскопическая*. Проведение данного вида экспертизы актуально при предоставлении в качестве доказательств аудиозаписей или фонограмм. Основные вопросы касаются определения принадлежности голоса подозреваемому, расшифровки неразборчивых фрагментов, установки точного текста, установления шумов и определения их источников, оценки модификации голоса, определения пола, возраста, психо-социологического профиля, эмоционального состояния, возможного монтажа. В случае проведения экспертизы текста предоставляется оригинал полного издания или его копия. При анализе цифрового документа предоставляется соответствующая ссылка на данный документ. Экспертиза интернет-контента требует предоставления ссылки на персональный сайт или ресурс. В случае экспертизы чатов (блог) необходимо работать как с печатной, так и

Джилкишиев Р.Б.

электронной версиями, поскольку гиперссылки и контекст могут играть ключевую роль. Если объектом выступает веб-сайт, необходима его архивная копия с указанием даты ее создания. Работа эксперта в данном случае связана непосредственно с интернет-пространством, поскольку он должен видеть актуальную информацию и структуру.

- *Судебно-психологическая*. Назначается в случае, если возникают сомнения в осознанности действий подозреваемого, особенно не достигшего порога совершеннолетия, без явных признаков серьезных психических расстройств. В случае отсутствия серьезных психических расстройств, психопатологических состояний, экспертиза может быть назначена с целью выяснения умственного развития и определения психологических характеристик. Данный вид экспертизы помогает установить степень осознанности действий преступника и возможности контроля своих действий.

Для определения места нахождения подозреваемого, следователем проводятся оперативно-розыскные мероприятия. Данные для поиска могут быть получены в результате анализа IP-адресов, лог-файлов и прочих полученных улик. Следующим следственным действием после установления места нахождения является проведение обыска по адресу проживания подозреваемого, в ходе которого проводится изъятие материальных объектов и иные доказательства, свидетельствующие о совершении преступления или опровергающие вину подозреваемого. В случае необходимости проводится допрос свидетелей или экспертов, а также назначаются необходимые экспертизы. На каждом этапе следственных действий следователь имеет возможность выбора стратегии и тактики поведения в зависимости от обстоятельств дела. Эффективность расследования зависит от того, насколько правильно были спланированы и организованы начальные следственные действия [127, с. 16].

Одним из ярких примеров использования компьютерных технологий явилось уголовное дело в отношении Омарова А.О., Дастарова Б.Е. и других по признакам преступлений, предусмотренных ст. ст. 208 ч.3 п.п. 1,2, 210 ч.3 п.п. 1,2 УК, осужденных приговором суда №2 Бостандыкского района города Алматы от 24 января 2017 года к различным срокам лишения свободы.

По обстоятельствам уголовного дела: Омаров А. и Дастаров Б., работающие системными администраторами на предприятии и имеющие опыт работы в сфере информационных технологий и бухгалтерского учета, организовали устойчивую организованную группу, с целью хищения чужого имущества путем неправомерного доступа к конфиденциальной информации юридических и физических лиц.

Преступный умысел злоумышленников состоял в создании вредоносных программ и дальнейшего их распространения с целью неправомерного доступа и завладения охраняемой законом информации.

Рассылка электронных писем осуществлялась от имени Генеральной прокуратуры, Налогового комитета, Министерства финансов, Комитета государственных доходов Министерства финансов и различных служб

Джилкишиев Р.Б.

поддержки 1С бухгалтерии. Рассылаемые электронные письма содержали подложный обратный электронный адрес, текст, побуждающий пользователя загрузить и установить модифицированный программный продукт по прилагаемой к письму ссылке.

После запуска и установки пользователем модифицированного программного продукта Омаров А. и Дастаров Б. получали неправомерный удаленный доступ к хранящимся данным на электронных носителях и возможность контроля, а также управления зараженным компьютером.

Преступное сообщество, имея неправомерный доступ к компьютерной информации физических и юридических лиц, умышленно и неправомерно завладели охраняемых законом информациями, в частности, логинами, паролями учетных записей социальных сетей, электронной почты, системой «банк-клиент», системами «интернет-банкинга» и т.д. Кроме того, имели возможность получать изображения от веб-камер, установленных на зараженных компьютерах.

Используя полученные возможности, осуществляли незаконные перечисления денежных средств со счетов юридических и физических лиц, на заранее подготовленные расчетные счета третьих лиц.

В результате анализа содержания подраздела, посвященного типичным ситуациям на первоначальном этапе расследования киберпреступлений и алгоритмам действий следователя, установлено, что эффективность расследования в данной сфере во многом определяется оперативностью и методологической точностью первых следственных действий. Особенность цифровой среды, как объекта уголовного преследования, заключается в ее высокой изменчивости, виртуальности следов и потребности в немедленном реагировании на угрозу утраты доказательной информации. Следственные органы, сталкиваясь с киберпреступлением, в большинстве случаев оказываются в условиях высокой информационной неопределенности, что требует от них не только точных правовых знаний, но и уверенного владения техническими средствами и криминалистическими алгоритмами.

Выявленные типичные ситуации, в том числе фиксация фактов несанкционированного доступа, выявление источников вредоносных программ, анализ логов сетевой активности, идентификация пользователей, скрывающих свою личность, требуют внедрения четко структурированных тактических моделей поведения следователя. Представленные алгоритмы действий, ориентированные на последовательную фиксацию цифровых следов, изъятие электронных носителей, взаимодействие с интернет-провайдерами и банковскими учреждениями, должны рассматриваться как основа современной криминалистической методики в условиях цифровой трансформации общества.

По итогам анализа можно заключить, что действующая следственная практика в Республике Казахстан еще не в полной мере адаптирована к специфике расследования правонарушений, совершаемых в цифровом пространстве. Вызывает озабоченность отсутствие единых методических рекомендаций, недостаточный уровень технической оснащенности

Джилкишиев Р.Б.

подразделений, специализирующихся на расследовании киберпреступлений, а также ограниченный круг специалистов, способных квалифицированно проводить осмотр цифровых объектов и анализировать информацию в формате электронных данных. Данные обстоятельства снижают качество первоначальных следственных действий и нередко приводят к потере критически важной информации.

В качестве предложения по улучшению следственной практики в данной сфере целесообразно разработать и утвердить на уровне Министерства внутренних дел и Генеральной прокуратуры Республики Казахстан официальную инструкцию (методические рекомендации) по алгоритму действий следователя при выявлении, фиксации и анализе цифровых следов на первичном этапе расследования. Данный документ должен предусматривать стандартизированные формы взаимодействия с телекоммуникационными операторами, банками, хостинг-провайдерами и другими структурами, вовлеченными в функционирование цифровой инфраструктуры.

Успешное противодействие киберпреступности невозможно без пересмотра традиционных тактических подходов и внедрения современных цифровых инструментов в следственную деятельность. Эффективность расследования зависит от того, насколько быстро и грамотно будет организовано реагирование на преступление в киберпространстве, насколько полно и корректно будут зафиксированы и интерпретированы цифровые следы. Предлагаемые меры направлены на повышение качества работы следственных органов, укрепление доказательной базы и обеспечение надлежащей правовой защиты интересов государства и граждан в условиях цифровой эпохи.

Современные вызовы в сфере цифровых технологий и информационной безопасности требуют принципиального пересмотра подходов к проведению судебно-экспертных исследований в Казахстане. Усиление угроз со стороны киберпреступности делает актуальным создание надежной нормативной основы, способной регулировать судебно-экспертную деятельность в области цифровой криминалистики. Это обуславливает необходимость внесения целого ряда нововведений в Закон Республики Казахстан от 10 февраля 2017 года №44-VI «О судебно-экспертной деятельности» (с изменениями по состоянию на 03.09.2023 г.).

В связи с этим мы предлагаем научно обоснованные дополнения и изменения, направленные на модернизацию законодательства с учетом передового международного опыта и современных стандартов. Приведенные нововведения включают закрепление понятийного аппарата, касающегося цифровых криминалистических экспертиз, детализацию объектов и методов исследования цифровых доказательств, а также определение квалификационных требований к судебным экспертам, специализирующимся в сфере информационных технологий.

Введение предложенных изменений позволит существенно повысить качество и эффективность судебно-экспертных исследований, обеспечить надлежащий уровень защиты прав и законных интересов граждан, организаций

Джилкишиев Р.Б.

и государства при расследовании компьютерных и иных киберпреступлений. Кроме того, это создаст условия для широкого внедрения современных технических и методологических средств, необходимых для успешной реализации экспертной деятельности в условиях цифровизации правовой среды.

А) **В ст. 1 «Разъяснение некоторых понятий, содержащихся в настоящем Законе» добавить** п. 16) и внести авторское понятие «**цифровая криминалистическая экспертиза»,** изложив его в следующей редакции: **«цифровая криминалистическая экспертиза – вид судебной экспертизы, основанный на применении специальных знаний и технических средств для выявления, анализа, интерпретации и документирования цифровых доказательств, извлеченных из компьютерных систем, сетевых структур, мобильных устройств и других электронных носителей информации».**

Отсутствие четкого понятия цифровой криминалистической экспертизы в законе затрудняет ее институционализацию и ограничение от смежных видов исследований. Введение термина позволит легализовать данную сферу как самостоятельную экспертную специализацию.

Б) **В ст. 4 «Содержание судебно-экспертной деятельности» добавить** пункт 6) и внести дополнение, изложив его в следующей редакции: «**организация и проведение судебных экспертиз в области цифровой криминалистики и информационной безопасности, включая сбор, анализ и интерпретацию цифровых доказательств, извлеченных из электронных источников».**

Данное дополнение необходимо, так как оно направлено на расширение содержания судебно-экспертной деятельности с учетом современных вызовов, связанных с расследованием киберпреступлений.

В) Включить в ст. 12 «**Компетенция Министерства юстиции Республики Казахстан»** новый подпункт 10-1) и внести дополнение, изложив его в следующей редакции: **«разработка и утверждение перечня экспертных специальностей и методик, используемых при производстве цифровых криминалистических экспертиз, а также стандартов безопасности и процедур обращения с цифровыми доказательствами».**

Введение единой регуляции цифровой экспертизы и создание перечня признанных методов обеспечат правовую допустимость таких доказательств в суде и устойчивость к оспариванию.

Г) **В ст. 4 «Содержание судебно-экспертной деятельности» добавить** п. 6) и внести дополнение, изложив его в следующей редакции: «**организация и проведение судебных экспертиз в области цифровой криминалистики и информационной безопасности, включая сбор, анализ и интерпретацию цифровых доказательств, извлеченных из электронных источников».**

Данное дополнение необходимо, так как оно направлено на расширение содержания судебно-экспертной деятельности с учетом современных вызовов, связанных с расследованием киберпреступлений.

Джилкишиев Р.Б.

Д) Добавить в ст. 19 **«Судебный эксперт»** п. 1-1 и внести дополнение, изложив его в следующей редакции: **«Судебным экспертом в области цифровых криминалистических экспертиз может быть лицо, имеющее высшее техническое образование в области информационной безопасности, программирования или кибербезопасности, прошедшее специальную подготовку и получившее квалификационное свидетельство (лицензию)».**

В п. 2 «Лица, указанные в подпунктах 1) и 2) пункта 1 настоящей статьи, должны состоять в гражданстве Республики Казахстан», соответственно, внести изменение, дополнив и изложив его в следующей редакции: **«Лица, указанные в подпунктах 1) и 2) пункта 1 и 1-1 настоящей статьи, должны состоять в гражданстве Республики Казахстан».**

Четкая квалификация и лицензирования для экспертов по цифровым следам позволит отбирать специалистов с надлежащими техническими знаниями и гарантировать научную обоснованность экспертиз.

Е) Добавить в ст. 32 «Объекты судебной экспертизы» новый п. 2-1 и внести авторское дополнение, изложив его в следующей редакции: **«К объектам цифровой криминалистической экспертизы относятся электронные устройства, их компоненты (жесткие, мягкие, CD и DVD диски, флеш-накопители, SIM-карты и др.), данные в облачных хранилищах, сетевой трафик, лог-файлы, данные с мессенджеров, соцсетей, почтовых и платежных систем, а также программное обеспечение».**

Формализованное определение объектов позволит избежать споров об их допустимости и укрепить доказательственную базу по делам о киберпреступлениях.

Предложенные авторские изменения в Закон Республики Казахстан «О судебно-экспертной деятельности» отражают необходимость своевременного законодательного реагирования на вызовы цифровой эпохи. Эти инициативы формируют правовую среду, способствующую созданию качественно новой практики судебно-экспертных исследований в сфере киберпреступлений, и закладывают основу для устойчивого развития экспертной деятельности в цифровом пространстве.

Нововведения, затрагивающие как квалификационные требования к специалистам, так и методическое обеспечение цифровых криминалистических экспертиз, создадут прочный фундамент для повышения уровня доверия к заключениям экспертов. Четко сформулированные стандарты и подходы к сбору, хранению и анализу цифровых доказательств позволят минимизировать риск ошибок и обеспечат соблюдение прав участников судебных процессов.

Реализация предложенных изменений также откроет дополнительные возможности для интеграции казахстанской экспертной практики с международными стандартами. В долгосрочной перспективе это усилит позиции Республики Казахстан в области международного сотрудничества и

Джилкишиев Р.Б.

повысит эффективность трансграничного взаимодействия при расследовании преступлений в цифровой среде.

Таким образом, принятие данных предложений позволит не только решить текущие проблемы судебно-экспертной деятельности, но и обеспечить ее устойчивость и эффективность в условиях непрерывного развития информационных технологий и цифровой криминалистики.

Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.
Джилкишиев Р.Б.

2.3 Последующий этап расследования уголовных дел о правонарушениях, в сфере информационных технологий и киберпреступности

Расследование преступлений в сфере информационной безопасности часто сопряжено с трудностями, связанными с пониманием самой сущности преступления, механизма его совершения, а также установлением виновного лица. В ходе расследования может быть дана неверная трактовка событий, преступление может быть неправильно классифицировано и неверно определен способ совершения преступления.

Первый этап расследования связан со сбором различной информации с целью проведения дальнейшего анализа для определения сущности правонарушения и злоумышленника, совершившего данное правонарушение. На втором этапе расследования имеющаяся доказательная база используется для проведения углубленного анализа и определения решений обнаруженных проблем. Проблемы, с которыми следователь может сталкиваться на первом этапе, касаются идентификации заходов и методов преступника. Поэтому собранная доказательная база, имеющаяся в наличии у следователя к моменту начала следующего этапа следствия, дает возможность более точно ответить на поставленные вопросы и предпринять соответствующие оперативные решения.

Таким образом, справиться с большинством проблем на первом этапе позволяют правильно организованные следственные действия и качественно проведенный анализ собранных данных.

Последующий этап характеризуется возможностью доступа к большому объему информации, собранной на предыдущем этапе (цифровые улики, свидетельские показания, документы и пр.). Собранные данные систематизированы, отличаются более четкой структурой, что позволяет упростить проведение их анализа. Доказательная база может быть собрана из различных источников, что позволяет видеть общую картину дела с разных сторон.

На первоначальных этапах расследования следователь может лишь строить рабочие гипотезы, различные версии событий, руководствуясь своей собственной интуицией. Собранные доказательства и более четкое понимание ситуации позволяют следователю перейти к более логичному и последовательному подходу, включающему формирование четких выводов и построения логических структур. То есть следователь может формировать выводы, опираясь не только на предположения, но и на фактические данные. Более структурированное рассмотрение дела позволяет устанавливать причинно-следственные связи и выстраивать последовательность событий.

Последующий этап расследования характеризуется планомерным и систематическим сбором доказательств и должен строиться не на случайных или интуитивных подходах, а на четких методах, в основе которых логика и доказательства. Основная направленность этапа — идентификация подозреваемого лица, доказывание его вины. Здесь ключевым моментом

Джилкишиев Р.Б.

является не только сбор новых, но и детальный анализ уже существующих доказательств [128, с. 261].

Таким образом, при традиционной структуре проведения этапов расследования основной акцент делается на сбор и оценку доказательств. Отправной точкой для дальнейшего расследования являются уже собранные доказательства, имеющиеся в распоряжении следователя. На основании подобных данных следователь должен стремиться к обнаружению новых источников информации с целью их дальнейшего анализа и установления важных фактов и ключевых обстоятельств дела. На всем протяжении этапа необходимо действовать организованно и целенаправленно, т.е. проводить развернутое, последовательное и методичное доказывание. Во главу угла должна ставиться логика и убедительные доказательства, что позволит сформировать ясную и обоснованную картину происходящего [129, с. 100-101].

Методы и тактика, используемые следователем на последующем этапе, могут отличаться от тех, которые были выбраны на первоначальном, поскольку меняются задачи и объем исходных данных, а также следственная ситуация. Следственные органы должны быть готовы к адаптации к таким изменениям и корректировать свои методы работы, исходя из вновь открывшихся обстоятельств. Использование шаблонного метода является неэффективным, поскольку каждый случай уникален, гибкость мышления и способность к анализу каждого нового аспекта дела имеет немаловажное значение.

Таким образом, процесс расследования — это, скорее, творческий процесс, требующий от следователя креативности, применение же схематизма может привести к ошибкам [130, с.23]. Частная криминалистическая методика не должна ограничивать инициативные действия следователя в его стремлении использовать эвристический поиск. Тем не менее, стоить помнить, что она сформировалась на основе многолетнего опыта и практики. Отсюда следует вывод, что сочетание творческого подхода и методического обоснования позволит эффективно решать задачи, стоящие перед следствием, и достигать наилучших результатов.

Конечно, каждый этап расследования характеризуется типичными для него проблемами. Если на начальном этапе — это трудности, связанные с получением первоначальных улик и информации, то на более позднем, по мере продвижения расследования, возникают более сложные проблемы, имеющие конфликтный характер, когда следствию противодействуют участники уголовного процесса. Прежде всего, оно может исходить от подозреваемых и обвиняемых, поскольку они не заинтересованы в раскрытии дела, так как полученная информация может быть использована против них. В случаях расследования дел с организованной преступностью это может создать дополнительные проблемы, поскольку сообщники, находящиеся на свободе, могут также оказывать противодействие следствию. Все это значительно усложняет процесс получения доказательств, поэтому следователь должен быть готов к сложным взаимодействиям с участниками дела и применению более сложных методов расследования [131, с.205].

Джилкишиев Р.Б.

Когда обвиняемый определен, это делает его центральной фигурой в расследовании, т.е. все следственные действия, в том числе и негласные, сосредотачиваются вокруг него, направлены на изучение его личности и получение новой информации не только об инкриминируемом им преступлении, но и выявлении других противоправных деяний. Главная задача на данном этапе — выяснение всех деталей преступления и установление виновности каждого участника дела. Следователь должен:

- выявить обстоятельства совершения каждой части преступления;
- оценить роль и степень вины каждого лица, проходящего по делу;
- предъявить обвинение и организовать допросы лиц со статусом «обвиняемый»;
- сделать сравнительный анализ показаний с другими доказательствами в деле;
- провести анализ всех собранных доказательств с целью устранения выявленных противоречий.

В случае необходимости, следователем проводится работа по поиску новых доказательств и выявлению смягчающих или отягчающих обстоятельств. В своей работе следователь должен учитывать типичные ситуации и проблемы, имеющие место на данном этапе расследования. Это означает, что следователь должен быть готов к различным развитиям обстоятельств и вызовам.

Мы абсолютно разделяем точку зрения Ахпанова А.Н. и Кусаинова Ш.К., по словам которых «Обвиняемый в соответствии с принципом презумпции невиновности считается невиновным до тех пор, пока его виновность не доказана в установленном порядке и юридически не зафиксирована, согласно статье 77 Конституции Республики Казахстан, обвинительным приговором суда, вступившим в законную силу. В данной ситуации в общей правосубъектности гражданина ограничиваются права и возлагаются обязанности только в пределах, определенных задачами и интересами предварительного следствия» [132, с. 60-61].

Таким образом, следственные действия должны быть сконцентрированы не только на подтверждении фактов совершения противоправного деяния, но и на определении всех его аспектов и эпизодов. Комплекс следственных действий должен содержать следующие мероприятия:

1) поиск всех участников преступной деятельности, включая сообщников, а также лиц, имеющих прямое или косвенное отношение к совершению преступления;
2) установление полного объема преступной деятельности;
3) оценка ущерба, который нанесен совершением преступления;
4) проведение анализа всех обстоятельств, приведших к совершению противоправного деяния.

Эффективность следственных действий последующего этапа зависит от качества собранных доказательств на первоначальном этапе [133, с.43-44].

Данному этапу присущи следующие следственные ситуации:

1) обвиняемый полностью признает свою вину;

Джилкишиев Р.Б.

2) обвиняемый отрицает свою вину;

3) из всех установленных соучастников лишь некоторые признали вину;

4) все установленные соучастники отрицают вину за совершенное преступление;

5) все установленные соучастники признают свою вину в полном объеме;

6) установлены все соучастники по рассматриваемому делу, но у следствия появилась информация о совершении других преступлений.

Наиболее часто встречающимися ситуациями являются ситуации под номером 1) и 2), поскольку, как показывает практика, большинство преступлений совершаются одним человеком. В этом случае процесс расследования может либо упроститься, либо усложниться, исходя из позиции, которой придерживается обвиняемый.

Признание обвиняемым своей вины значительно облегчает следственные действия, так как следователь может сконцентрировать свои усилия на подтверждении всех обстоятельств преступления и сборе дополнительной доказательной базы.

Как верно отмечено Бегалиевым Е.Н., установление доверительных взаимоотношений между следователем и обвиняемым — залог успеха открытого и плодотворного допроса при условии невыхода за профессиональные рамки и уголовно-процессуального законодательства [134, с. 5-8].

Здесь основополагающей задачей является не только сбор доказательств, но и их качественная проверка и оценка.

В случае если обвиняемый признает свою вину, но у следователя нет достаточных доказательств, следственные действия должны быть направлены на фиксацию полученных от обвиняемого сведений, а также на дальнейший сбор криминалистически значимой информации, подтверждающей совершение подозреваемым лицом преступлений.

Когда обвиняемый отрицает причастность к совершению преступления, как правило, он заявляет о своем алиби, создавая специфическую ситуацию для следствия. Зачастую такая ситуация возникает в случае, если с момента совершения преступления и задержания подозреваемого лица прошло достаточно много времени. Данный факт может значительно затруднить проверку алиби в связи с трудностями в поисках свидетелей или доказательств. Недостаток информации у обвиняемого также может повлиять на стратегию его защиты. В таком случае следователю необходимо направить свои усилия на сбор и анализ доказательств, которые могут подтвердить или опровергнуть алиби обвиняемого, а также проверить состоятельность выдвигаемых им доводов. Исходя из полученных от обвиняемого показаний, следователь должен выстроить логическую модель, которая демонстрирует условия, в которых обвиняемый мог находиться в момент совершения преступления. Такая модель дает следователю возможность понимания реальности и правдоподобности выдвинутых доводов об алиби. Также на основе данной модели следователь

Джилкишиев Р.Б.

изучает и выводит возможные следствия, которые облегчат дальнейшее расследование.

Из следственных действий, проводимых на этом этапе расследования, рассмотрим лишь некоторые, имеющие наибольшие особенности в тактике их проведения по делам данной категории.

В ходе проведения расследования нередко возникает необходимость в проверке объективной возможности того или иного обстоятельства, явления в определенных условиях. Например, мог ли свидетель, находясь в определенном месте, видеть или слышать то, что происходило на месте совершения правонарушения; можно ли проникнуть в помещение, где совершено данное правонарушение; может ли быть организована перевозка различных материалов, связанных с расследуемым делом (листовки, записи разговоров, передач и пр.) С целью выяснения вышеобозначенного, следователем могут быть проведены следственные эксперименты, представляющие специальное следственное действие, направленное на стимуляцию условий, при которых могли произойти события.

Проверка и уточнение показаний на месте является важным элементом уголовного процесса и самостоятельным следственным действием, регулируемым ст. 257 УПК.

Данное следственное действие проводится с целью выяснения новых обстоятельств, имеющих отношение к преступлению. Процесс предполагает проверку и уточнение ранее предоставленных показаний от свидетелей, потерпевших или обвиняемых с целью определения их достоверности и точности. В случае противоречивости показаний проверка на месте может прояснить ситуацию, а также привести к обнаружению новых данных, не учтенных ранее или не известных следствию.

Делается это путем вербального воспроизведения допрашиваемого на месте той обстановки, которая имела место ранее, а также путем демонстрации действий лицом, показания которого проверяются, указания им на предметы и документы, воспроизведения показаний и дачи ответов на поставленные вопросы.

К прочим тактическим задачам можно отнести следующие:

1) уточнение ранее известных фактов, добавление новых, что позволяет лучше понять ситуацию в целом;

2) поиск новой информации, ранее не известной следствию;

3) нахождение новых вещественных доказательств (носителей информации), ранее не задействованных в деле;

4) выявление противоречий в ранее полученных показаниях, указывающих на ложность и неправдоподобность некоторых свидетельств;

5) проверка версии совершения преступления одним лицом;

6) уточнение изменений, произошедших в период со времени окончания преступного события до момента проверки показаний;

7) оценка степени психологической устойчивости и последовательности к приверженности обвиняемого своих показаний.

Джилкишиев Р.Б.

Данное следственное действие особо значимо, когда в его результате обнаружен новый, ранее не известный факт, новый эпизод, новые пострадавшие или другие важные обстоятельства.

В процесс проверки могут быть обнаружены новые вещественные доказательства, которые были спрятаны или о которых знало лишь лицо, которое дает показания. Если при проверке ранее не упомянутых показаний следователем подтвердится их правдивость, это является свидетельством их правдивости.

Действие по проверке и уточнению показаний на месте имеет ряд особенностей:

- выход на место происшествия требует согласия подозреваемых или обвиняемых, так как согласно действующему законодательству, они могут отказаться от участия в данном следственном действии;

- согласие также требуется от свидетелей и потерпевших, особенно это касается тех случаев, когда есть реальный риск причинения им душевных страданий или угроз здоровью;

- следователю следует заранее посетить место происшествия, пройти тот же маршрут, что и лицо, чьи показания проверяются. Это поможет ему лучше понять обстановку, оценить окружение, максимально приблизить обстановку к реальным условиям, при которых было совершено преступление, а также определить направление следственного действия.

Следственный эксперимент проводится в целях: проверки возможности совершения определенных действий в определенных условиях, что также дает возможность проверить правдивость показаний обвиняемого (подозреваемого); проверки использования тех инструментов, аппаратуры и материалов, которые были обнаружены и изъяты при расследовании и т.п. (ст. 258 УПК).

В рамках расследования одного из уголовных дел по распространению вредоносных программ посредством сети интернет обвиняемый создал псевдосайт, мимикрирующий под законный, и разместил там вредоносную программу-тестер («тестирования проблем 2010 года»), выглядящую как легитимную. При заходе на данный сайт данная программа скачивается пользователями, не подозревающими, что в ее запуске могут происходить опасные действия. В результате происходила несанкционированная отправка учетных имен и паролей пользователей на заранее определенный электронный адрес, а также менялись файлы настройки операционной системы, что крайне затрудняло обнаружение и удаление вредоносного ПО. Особенностью полученных показаний потерпевших стало то, что при схожести посещенного сайта (дизайн, структура), ими были указаны разные электронные адреса, на которых, по мнению потерпевших, находился данный сайт. Исходя из данного факта, можно предположить следующее:

- несмотря на различные адреса, потерпевшие могли видеть одну и ту же вредоносную программу, доступную по разным ссылкам или доменам, чему способствовало использование зеркал или фальсификация сайта;

Джилкишиев Р.Б.

- было использовано неограниченное количество доменов с целью сокрытия деятельности.

При проведении следственного эксперимента было осуществлено исследование сайтов, указанных потерпевшими в качестве мест размещения вредоносного ПО. Проведенные следственные действия подтвердили существование данных сайтов, а также нашла подтверждение и информация о размещении на них вредоносной программы. Данные подтвержденные факты явились основанием для дальнейшего расследования. Лица, участвующие в эксперименте, имели возможность скачать и сохранить размещенную вредоносную программу. Это явилось одним из ключевых моментов, поскольку наличие физического образца программы позволило провести исследования в дальнейшем, а также назначить соответствующие экспертизы. Тем не менее, следователи и участники эксперимента не смогли в полной мере оценить назначение программы и ее свойств, так как они не обладали специальными познаниями и навыками. Детальное исследование предполагает назначение компьютерно-технической экспертизы, в рамках которой специалисты имеют возможность проведения анализа структуры и функционала программы с целью понимания, действительно ли обнаруженное вредоносное ПО является именно тем, информация о котором запротоколирована в деле.

Воспроизведение обстановки и обстоятельств события при проведении следственного эксперимента надлежит осуществлять в условиях, максимально приближенных к тем, которые имели место при совершении правонарушений, в сфере информационных технологий и киберпреступности. При его проведении должны быть использованы те же материалы и инструменты, которыми пользовался преступник, или инструменты и материалы, аналогичные использованным.

Основаниями проведения следственного эксперимента являются сведения, подтверждающие необходимость проверки или уточнения определенных фактов и обстоятельств события.

Классификация следственных экспериментов, в зависимости от опытных действий и целей, выглядит следующим образом:

1) Следственный эксперимент, направленный на проверку восприятия фактов. Например, можно ли заметить определенные документы или информацию в определенных условиях (нарушение безопасности).

2) Следственный эксперимент, направленный на оценку возможности совершения определенных действий, например, проверка методов фишинга.

3) Следственный эксперимент, направленный на проверку возможности наступления какого-либо события (получение спама, переход по фишинговой ссылке).

4) Следственный эксперимент, направленный на проверку возможности умещения данных в заданном хранилище (диск, база данных).

5) Следственный эксперимент, направленный на выяснение последовательности совершения событий.

Джилкишиев Р.Б.

6) Следственный эксперимент, направленный на проверку механизма образования следов с целью оценки методов и способов образования определенных доказательств.

Таким образом, различные виды следственных экспериментов позволяют провести исследование различных аспектов расследуемых событий, начиная от проверки возможности их совершения до анализа следообразования.

Процедура проведения следственного эксперимента начинается с заслушивания в краткой форме показаний участников, касающихся обстоятельств произошедшего события. Это может быть подозреваемый, потерпевший, обвиняемый или свидетель. В ходе следственного эксперимента участникам предлагается ценить соответствие обстановки, в которой проводится эксперимент, изначальным условиям, в которых происходило событие. Следует подчеркнуть, что это крайне важный момент, поскольку от точности воспроизведения оригинальной обстановки во многом зависит точность проведения эксперимента. В случае выявления неточностей в воссозданной обстановке участники могут заявить следователю о данных отличиях. В таком случае следователь должен исправить обстановку и продолжить проведение следственного эксперимента.

Ключевую роль в проведении следственного эксперимент играет следователь. Все опытные действия проводятся по его указанию. Также следователь разрабатывает детальный план проведения эксперимента, определяя порядок проведения и последовательность опытных действий. За следователем закрепляется право внесения корректив в процесс эксперимента, обеспечивая гибкость его проведения и адаптивность следственного процесса. В ходе проведения рассматриваемого следственного действия следователь должен обеспечить прозрачность процесса, выражающийся в информированности всех участников о происходящем. Все проводимые в ходе эксперимента действия подлежат обязательной фиксации. Все выявленные несостыковки, замечания или комментарии подлежат протоколированию и обсуждению.

В случае необходимости следователем могут привлекаться эксперты для помощи в проведении анализа результатов или когда следствие нуждается в проведении сложных опытных действий. Если в совершении события принимали участие несколько лиц, во избежание влияния участников на показания друг друга, следователь проверяет действия каждого из них поочередно (отдельно). В случае, когда необходимо проверить действия лиц, которые отсутствуют на момент проведения следственного эксперимента, следователь может заменить их на других людей, имеющих схожие физические данные.

Фиксация следственного эксперимента осуществляется при помощи составления протокола. Документ должен содержать детальное, пошаговое описание процесса рассматриваемого следственного действия, условия его проведения, а также результаты. В качестве дополнительных средств фиксации могут выступать фототаблицы, скриншоты, графики, таблицы, схемы, аудио-,

видеофиксация. Все перечисленные материалы являются неотъемлемой частью протокола и служат дополнительным подтверждением хода и результата следственного эксперимента.

Следственный эксперимент — одно из доказательств, следовательно, он должен подлежать оценке. Оценка может включать следующие критерии:

- Допустимость. Связана с соблюдением всех необходимых законодательных норм, определяющих порядок и основание для проведения следственного эксперимента.

- Относимость. Определяет значимость информации, полученной в ходе эксперимента, для уголовного дела.

- Достоверность. Оценивается на уровне внутренних убеждений следователя. Следователем оценивается согласованность полученных показаний свидетелей с информацией, полученной в ходе эксперимента или на основании наличия прочих улик.

По результатам проведенного следственного эксперимента может быть проведена повторная экспертиза для сравнительного исследования предметов правонарушений, в сфере информационных технологий и киберпреступности.

Важное значение в процессе расследования приобретает установление обстоятельств, способствовавших совершению преступления [135, с. 15-16].

В соответствии со ст. 287 УПК, дополнительная экспертиза назначается при недостаточной ясности или полноте заключения, а также возникновении необходимости решения дополнительных вопросов, связанных с предыдущим исследованием, где его производство может быть поручено тому же или иному эксперту.

Экспертиза может быть назначена по инициативе участников процесса, защищающих свои или представляемые права и интересы.

Участники процесса, защищающие свои или представляемые права и интересы, в письменном виде представляют органу, ведущему уголовный процесс, вопросы, по которым, по их мнению, должно быть дано заключение эксперта, указывают объекты исследования, а также называют лицо, которое может быть приглашено в качестве эксперта.

Орган, ведущий уголовный процесс, не вправе отказать в назначении экспертизы, за исключением случаев, когда вопросы, представленные на ее разрешение, не относятся к уголовному делу или предмету судебной экспертизы.

Повторная экспертиза назначается для исследования тех же объектов и решения тех же вопросов в случаях, когда предыдущее заключение эксперта недостаточно обосновано, либо его выводы вызывают сомнение, либо были существенно нарушены процессуальные нормы о назначении и производстве экспертизы.

Обязательным является приведение в постановлении о назначении повторной экспертизы мотивов несогласия с результатами предыдущей экспертизы.

Джилкишиев Р.Б.

Производство повторной экспертизы может быть поручено комиссии экспертов. Эксперты, проводившие предыдущую экспертизу, могут присутствовать при производстве повторной экспертизы и давать комиссии пояснения, однако в экспертном исследовании и составлении заключения они не участвуют.

При поручении производства дополнительной и повторной экспертиз эксперту (экспертам) должны быть представлены заключения предыдущих экспертиз.

Дополнительная и повторная экспертизы назначаются и проводятся с соблюдением требований статей 270, 272 – 284 УПК.

Если вторая или последующая по счету экспертиза назначается по нескольким основаниям, одни из которых относятся к дополнительной экспертизе, а другие – к повторной, такая экспертиза производится по правилам производства повторной.

В соответствии со ст. 281 УПК, производство экспертизы осуществляется экспертом единолично либо комиссией экспертов. При этом комиссионная экспертиза назначается в случаях необходимости производства сложных экспертных исследований и проводится не менее чем двумя экспертами одной специальности.

Для производства судебно-психиатрической экспертизы по вопросу о вменяемости назначается не менее трех экспертов.

При производстве комиссионной судебной экспертизы каждый из судебных экспертов независимо и самостоятельно проводит судебно-экспертное исследование в полном объеме. Члены экспертной комиссии совместно анализируют полученные результаты и, придя к общему мнению, подписывают заключение либо сообщение о невозможности дать заключение.

Согласно ст. 282 УПК РК, может быть назначена комплексная экспертиза, когда для установления обстоятельства, имеющего значение для дела, необходимы исследования на основе разных отраслей знаний, и проводится экспертами различных специальностей в пределах своей компетенции. Комплексная экспертиза может проводиться одним экспертом в случае, если он имеет право производства исследований по различным экспертным специальностям.

В заключении комплексной экспертизы должно быть указано, какие исследования, в каком объеме провел каждый эксперт и к каким выводам он пришел. Каждый эксперт подписывает ту часть заключения, в которой содержатся эти исследования.

На основе результатов исследований, проведенных каждым из экспертов, ими формулируется общий вывод (выводы) об обстоятельстве, для установления которого экспертиза была назначена. Общий вывод (выводы) формулируют и подписывают только эксперты, компетентные в оценке полученных результатов. Если основанием окончательного вывода комиссии или части ее являются факты, установленные одним из экспертов (отдельными экспертами), то об этом должно быть указано в заключении [136, с.35-44].

Джилкишиев Р.Б.

В случае разногласий между экспертами каждый из них или часть экспертов дает отдельное заключение либо эксперт, мнение которого расходится с выводами остальных членов комиссии, формулирует его в заключении отдельно.

В соответствии с действующим законодательством, а именно ч.1 ст. 282 УПК РК, экспертиза может проводиться одним экспертом (при условии достаточной квалификации). В данном случае речь идет о комплексной моноэкспертизе, при которой экспертом оцениваются различные аспекты одного и того же события или доказательства из нескольких областей. Преимуществом данного вида экспертизы является то, что один эксперт способен лучше и глубже связать все элементы, беря за основу единую концепцию [137].

Пунктом 11 Постановления Суда РК № 16 от 26.11.2004 года «О судебной экспертизе по уголовным делам» установлено, что заключение эксперта, несмотря на его важность, не может считаться единственным или наиболее важным доказательством. Таким образом, все полученные в ходе следствия доказательства должны оцениваться на равных условиях и в полной мере. Экспертное заключение не должно рассматриваться как окончательное: полученные результаты должны подвергаться детальному анализу и сопоставлению с другими доказательствами. Только так можно сформулировать обоснованные выводы. Оценка доказательств может быть связана с речевыми произведениями (текста записей, заявлений участников процесса и пр.), что требует применения особого подхода, включающего проведение лингвистического анализа, способного учитывать определенный контекст и речевые особенности языка.

Вовлечение лингвистов может иметь положительное влияние на следственный процесс и благоприятно сказаться на ходе дела, так как они могут помочь правильно интерпретировать и проанализировать речевые доказательства. Считаем, что было бы целесообразным (по аналогии со ст. 488 УПК РК с участием психолога) включить специалистов в области лингвистики в уголовные дела, особенно, где речь идет о несовершеннолетних [138, с. 15].

Очная ставка. Очная ставка представляет собой процесс, в ходе которого лица, дающие показания, встречаются друг с другом с целью прояснения несостыковок и противоречий в данных ими показаниях (ст. 218 УПК). Основная задача проведения очной ставки — выяснение истины в случаях наличия существенных противоречий в свидетельских показаниях. Тактические методы проведения очной ставки зависят от конкретных обстоятельств дела и личностных особенностей ее участников. Данное следственное действие должно основываться на четко разработанном плане. При этом следователь должен отдавать себе отчет, что допрашиваемые лица (подозреваемый, обвиняемый) могут намеренно искажать факты, несмотря на довольно хорошую память на события, связанные с правонарушением. Однако определенные противоречия могут возникать не из-за желания намеренного

Джилкишиев Р.Б.

искажения реальных событий, а являются результатом ошибочного восприятия событий или недостатка информации.

Правом инициировать проведение очной ставки обладает следователь, а также участники досудебного расследования, в том числе и подозреваемые (обвиняемые) путем подачи соответствующего ходатайства. При этом необходимо понимать, что проведение очной ставки — процедура не обязательная. То есть следователь имеет право ее провести, но не обязан. Таким образом, решение о целесообразности и необходимости проведения очной ставки принимается следователем в каждом конкретном случае.

Критериями определения существенности противоречий в свидетельских показаниях являются наличие взаимоисключающих показаний, данных в отношении одних и тех же фактов, либо значительные расхождения при описании таких моментов, как дата, место и обстоятельства событий. Степень существенности противоречий оценивается индивидуально для каждого расследуемого дела, в зависимости от их значимости и влияния на полноту, всесторонность и объективность расследования. В то же время согласно ст. ст. 113, 510, 531 УПК РК, в любом случае существенными признаются все противоречия, касающиеся ключевых обстоятельств, которые подлежат доказыванию.

Производство очной ставки не всегда способно разрешить противоречия между показаниями участников: частники могут просто повторить ранее предоставленную информацию, не изменяя ее; допрашиваемые лица могут отказаться от ранее предоставленных показаний или полностью изменить их; участники могут предоставить ложную информацию; один из участников, обладая меньшим уровнем психологической стабильности, может находиться под влиянием другого участника, особенно если последний дает ложные показания; участники могут отказаться от дачи каких-либо показаний. В случае сомнения эффективности следователем может быть инициирован повторный или дополнительный допрос, что дает возможность более глубоко и детально изучить показания лица, предположительно дающего ложные сведения. Следователь должен предпринять попытку выяснить причины, побудившие лицо дать недостоверные показания с целью разоблачения или убеждения к даче правдивых показаний. Если достоверность показаний вызвана заблуждением лица (ложные воспоминания, непонимание произошедших событий), следователю необходимо выяснить причины, побудившие дачу недостоверных сведений.

Очная ставка характеризуется отсутствием четкого перечня участников. Законодательство не предусматривает определенного списка участников, которые могут участвовать в процедуре допроса, т.е. УПК не ограничивает категории, но его нормы подразумевают возможность проведения данного следственного действия с участием определенных лиц. Так, очная ставка может проводиться только между потерпевшими, подозреваемыми и свидетелями при любых сочетаниях [139, с. 9]. К участникам очной ставки не могут быть отнесены эксперты и специалисты, хотя в отношении них может быть

Джилкишиев Р.Б.

осуществлено производство иного следственного действия как допрос. Исключение экспертов и специалистов объясняется спецификой их допроса, поскольку он касается вопросов, непосредственно имеющих отношение к экспертной деятельности. То есть, они не являются сторонами, чьи показания могут непосредственно пересекаться друг с другом (ст. 285 УПК).

Как уже обозначено выше, проведение процедуры очной ставки требует составления детального плана. В первую очередь, необходимо определить четкий круг участников. Кроме потерпевших и обвиняемых (подозреваемых), в процессе может быть предусмотрено участие следующих лиц:

1) Сторона защиты. Присутствие защитника обязательно, если хотя бы один из участников является подозреваемым, а также существуют обстоятельства, предусмотренные ст. 67 УПК.

2) Представитель потерпевшего. Может участвовать в случае наличия среди участников процесса потерпевшего лица. В случаях, предусмотренных нормами ч. 2 ст. 76 УПК, участие законного представителя является обязательным.

3) Сторонние специалисты. Участие обязательно, если хотя бы один из участников (свидетель или потерпевший) — лицо, не достигшее возраста совершеннолетия. Для детей, не достигших 14-летнего возраста, в обязательном порядке требуется участие педагога или (и) психолога; для подростков в возрастной категории 14-18 лет — по усмотрению следователя. Законные представители несовершеннолетнего потерпевшего участвуют в очной ставке в обязательном порядке.

4) Переводчик. В случае незнания языка одним из участников процесса присутствие переводчика обязательно.

5) Присутствие врача. Если один из участников имеет психическое или иное тяжкое заболевание, очная ставка проводится с разрешения лечащего врача и в его присутствии. Данное требование регламентируется нормами ч. 8 ст. 201 УПК РК.

Правильная организация очной ставки не только обеспечивает законность проведения данного следственного действия, но и справедливость судебного разбирательства.

С целью получения дополнительной экспертной информации и разъяснения определенных обстоятельств и специализированной терминологии в ходе следственных действий могут быть приглашены такие специалисты как бухгалтер, программист и пр. Основная цель приглашения подобных специалистов — обеспечение ясности, помощь в интерпретации показаний, особенно если в них присутствуют несоответствия.

Подготовка и порядок проведения очной ставки строго регламентированы. Как правило, участники очной ставки ранее уже проходили процедуру допроса, поэтому они не предоставляют какие-либо анкетные данные (ч. 1 ст. 110 УПК). Перед началом проведения данного следственного действия участникам напоминаются их права и обязанности, а также разъясняется порядок проведения данного следственного действия с

Джилкишиев Р.Б.

обязательной фиксацией в протоколе. Привлеченным специалистам разъясняется уголовная ответственность за предоставление ложного экспертного заключения, переводчик уведомляется об уголовной ответственности за заведомо ложный перевод (ст. 421 УК). Свидетели и потерпевшие, которым на момент очной ставки исполнилось полных 16 лет, предупреждаются об уголовной ответственности в случае отказа от дачи показаний (ст. 421) или дачу заведомо ложных показаний (ст. 420 УК). Также им разъясняется право отказа от дачи показаний, направленных против себя, близких родственников, в отношении второго супруга, а также против доверяющихся священнослужителям в процессе исповеди (ст. 28 УПК). В отношении лиц, имеющих право на свидетельский иммунитет (п. 3 ч. 2 ст. 78 УПК): медиаторы, священнослужители, сторона защиты и пр., может быть проведена процедура допроса лишь с письменного разрешения лиц, чьи права и сведения защищались. Если указанная категория лиц желает дать показания, несмотря на свидетельский иммунитет, они предупреждаются об уголовной ответственности за дачу ложных показаний (ст. 420 УК). В случае наличия отношений между допрашиваемыми лицами необходимо выяснить, какого рода эти отношения. В случае выявления неприязни, необходимо выяснить первопричины их возникновения, время их возникновения и в чем они заключаются. Если участники очной ставки находятся в родственных отношениях, выявляется степень родства. Данный порядок предусмотрен во избежание нарушений прав участников, обеспечения правовой защиты для всех сторон без исключения.

Основная цель очной ставки — выяснение противоречий в полученных показаниях двух или более допрашиваемых по отношению к одинаковым фактам (обстоятельствам), а также предоставление следствию четких фактов для дальнейшего расследования и принятия решения. Следователь, как лицо, проводящее предварительное следствие, должен придерживаться определенной процедуры. Так, в первую очередь, дать показания предлагается лицу, чьи показания считаются более правдивыми. Показания даются поочередно по тем же обстоятельствам, которые уже обсуждались на предыдущих допросах. Если противоречия имеются по нескольким обстоятельствам, свидетелю предлагается сначала дать показания по одному из них, далее выслушивается мнение второго участника, если есть необходимость, следователь может задать уточняющие вопросы. Затем необходимо продолжить рассмотрение следующего обстоятельства. Такой подход обеспечивает структурированность выяснения фактов, не перегружая углубленный анализ одновременно несколькими вопросами.

Показания каждого допрашиваемого подлежат обязательному занесению в протокол, что позволяет осуществить их фиксацию с привязкой к конкретному времени и избежать искажений. Согласие фиксации показаний подтверждается подписанием протокола каждым участником очной ставки. После первичной дачи показаний следователь может задавать детализирующие

или уточняющие вопросы с целью получения более полного представления о событиях.

Очная ставка проводится лишь при наличии определенных условий. К ним относятся:

1) Следственное действие проводится исключительно между двумя лицами. Данный формат способствует эффективному сравнению полученных показаний и выяснению противоречий.

2) Участники очной ставки ранее уже подвергались процедуре допроса в рамках расследования дела. Ранее сформированные показания являются отправной точкой для сравнения и анализа.

3) На начало очной ставки существуют значительные (существенные) противоречия в показаниях участников. В случае отсутствия таковых проведение очной ставки является нецелесообразным. В противном случае данный следственный процесс теряет свою суть и будет преследовать лишь цель подтверждения или закрепления ранее полученных показаний, что может привести к искусственному «перегрузу» объема доказательств и злоупотреблению процессуальными инструментами.

Лица, участвующие в рассматриваемом следственном действии, имеют право задавать друг другу вопросы с целью уточнения деталей своих показаний, выказывания сомнений. Вопросы могут задаваться с разрешения лица, осуществляющего производство по делу. Он имеет право отклонять вопросы, не относящиеся к сути дела, имеющие наводящий характер [140, с. 32]. Данный подход, с одной стороны, позволяет поддерживать диалог межу участниками следственного действия, с другой стороны, процесс контролируется следователем во избежание допущения злоупотреблений.

В ходе очной ставки могут быть использованы вещественные доказательства (справки из учреждений, записи, документы и пр.). Их применение целесообразно не только с точки зрения разрешения противоречий, но и при других ситуациях, когда важно установить ключевые детали, такие как дата или время произошедшего события (время доступа в интернет). Так, в случае, если показания допрашиваемых имеют отношение к конкретным временным рамкам или действиям, предоставление справок могут подтвердить или опровергнуть эти данные. Перед тем, как данные вещественные доказательства будут предъявлены, следователю необходимо убедиться, что данные о времени и дате не изменились, в противном случае это может повлиять на правильность выводов следствия. Вещественные доказательства необходимо предъявлять лишь после того, как допрашиваемые предоставили свои показания. Это позволяет проанализировать соответствие предоставленных показаний, а также обеспечить процессуальную законность.

Помимо вещественных доказательств могут быть представлены и другие виды доказательств, образовавшихся вследствие проведения следственного эксперимента или освидетельствования. Разнообразие предъявляемых доказательств способствует более полному и объективному пониманию ситуации. Тем не менее, следует подчеркнуть, что использование доказательств

Джилкишиев Р.Б.

необходимо осуществлять, исходя из тактической целесообразности, т.е. следователь должен оценить, какие доказательства и в каком объеме должны быть предоставлены, так как неправильные действия могут негативно сказаться на ходе действия дела. Таким образом, следователю необходимо найти «золотую середину»: найти истину, соблюдя при этом баланс между раскрытием информации и защитой процесса от возможных манипуляций или провокаций [141, с. 153].

В ходе проведения очной ставки оглашению подлежать не только ранее данные показания участников, но также и записи этих показаний (аудио-, видеоформат). Делается это для повышения точности и надежности предоставляемых показаний. Оглашению показаний предшествует фиксация в протоколе всего происходящего на очной ставке, с последующим письменным заверением всеми допрашиваемыми во избежание возможности внесения в них изменений или отказа от них после оглашения. В случае отказа участника очной ставки от дачи показаний, оглашение ранее данных показаний запрещается. Такой формат дает гарантию того, что участник не будет поставлен в невыгодное положение из-за ранее данных показаний, которых он больше не придерживается [142, с. 161].

Протокол проведения очной ставки представляет собой важнейший документ, в котором фиксируются все детали проведения следственного действия. Вводная часть документа должна содержать сведения о месте и дате, времени проведения следственного действия, его длительности вплоть до минуты. Также указывается, кто проводит очную ставку, полные фамилии, имена и отчества участников (допрашиваемых) с указанием их процессуального статуса. Так как лица, принимающие участие в очной ставке, были допрошены ранее, их анкетные данные указываются в сокращенном объеме (ФИО и процессуальное положение).

При присутствии иных лиц (эксперты, адвокаты) указывается их ФИО и их процессуальный статус. Необходимо отметить, что фиксации также подлежит разъяснение прав и обязанностей. Таким образом, четкая структурированность протокола обеспечивает прозрачность и законность проводимого следственного действия.

Протокол очной ставки должен содержать отражение определенных данных при использовании научно-технических средств и фиксируемых показаний, что имеет немаловажное значение с точки зрения законности, объективности следственных действий, а также обеспечения защиты прав участников следственного действия:

1) Любое использование научно-технических средств предполагает обязательное уведомление участников с занесением в протокол.

2) Подлежат документированию технические характеристики средств: вид, модель, носитель информации и пр.

3) Фиксируется время начала и окончания записи.

4) Подлежит указанию, в каких условиях и каким образом происходило использование научно-технических средств.

Джилкишиев Р.Б.

Описательная часть протокола используется для документирования ключевых моментов следственного действия. В обязательном порядке здесь указывается следующее:

1) Наличие связи между участниками, ее тип.

2) Показания участников следственного действия в порядке их предоставления.

3) Вопросы, задаваемые следователем, и предоставляемые на них ответы участников.

4) Вопросы, полученные от участников (с разрешения следователя).

5) Вопросы, полученные от прочих присутствующих лиц (адвокаты, эксперты, специалисты).

6) Фиксация фактов ранее оглашенных показаний участников, влияние данных действий на процесс.

7) Факт предъявления следователем вещественных доказательств. При предоставлении аудио-, видеодоказательств необходимо зафиксировать их длительность, время начала и окончания записи, реакцию участников на предъявленные доказательства (замечания, ходатайства). При прерывании записи указывается ее причина.

Таким образом, документирование всех вышеперечисленных элементов способствует организации проведения максимально прозрачного и полного следственного действия, а также выступает гарантом того, что все важные детали будут учтены в полной мере и смогут использоваться для анализа на последующих этапах следствия или в суде.

Ознакомление с протоколом — завершающий этап следственного действия. Данная процедура дает участникам возможность проверки точности зафиксированных показаний. До предъявления протокола для ознакомления следователь в обязательном порядке уведомляет участников об их правах, в том числе вносить замечания, требовать внесения поправок и дополнений. Далее каждому участнику предлагается подписать свои показания с обязательным парафированием каждой страницы протокола. Подписи участников подтверждают точность данных показаний. Если в процессе рассматриваемого следственного действия воспроизводились аудио-, видеозаписи, они в обязательном порядке должны быть воспроизведены для участников с указанием времени воспроизведения с точностью до минуты, что также парафируется участниками. Дополнения, замечания, исправления или возражения участников также добавляются в протокол с последующим заверением подписями. В случае если участниками вписываются какие-либо слова либо зачеркиваются уже внесенные, в обязательном порядке в конце протокола (перед подписями) вносятся сведения о таких исправлениях (ч. 4 ст. 123 УПК). Таким образом, процедура подписания протокола и парафирование его страниц дает гарантии, что участники согласны с подписанными данными.

В случае отказа одним из участников подписания протокола, следователь должен сделать соответствующую отметку об этом, заверив ее свой подписью. В соответствии с ч.ч. 7 и 9 ст. 123 УПК РК, участник, отказавший в подписании

Джилкишиев Р.Б.

протокола, вправе объяснить причину своего отказа также с занесением в протокол. Если участник, в силу своих физических недостатков, не может самостоятельно прочитать или подписать протокол, это может сделать его защитник или доверенное лицо (ч.10 ст. 123 УПК). путем зачитывания вслух (обязательно должна быть сделана отметка об этом). Однако перед непосредственным зачитыванием от участника необходимо получить согласие на такое действие. В данном случае подписание протокола также осуществляется защитником или другим доверенным лицом от его имени.

В соответствии с требованиями ч. 7 ст. 199 УПК РК, к подписанию протокола допускается не только следователь, но и все лица-участники следственного действия. Смысл данной нормы состоит в том, что подписание протокола не только должностным лицом, ведущим следственное действие, но и допрашиваемыми обеспечивает прозрачность и легитимность процесса, а также позволяет фиксировать учет мнений и позиций всех вовлеченных сторон.

Заключительный этап характеризуется подведением итогов, выявлением и исправлением ошибок, допущенных в ходе расследования, а также дальнейшим формулированием процессуальных решений. К дальнейшим процессуальным шагам относятся:

- Направление уголовного дела прокурору. После завершения работы следователя и передачи всех собранных доказательств прокурору, последний проводит анализ переданных документов. В случае если объем доказательной базы достаточен, прокурор готовит обвинительный акт для дальнейшей передачи его в суд для рассмотрения дела по существу.

- Постановление о прекращении уголовного дела или направлении в суд для применения принудительных медицинских мер. В случае если обвиняемый нуждается в принудительной медицинской помощи (психическое расстройство), дело направляется в суд для применения мер медицинского характера, т.е. уголовное наказание заменяется принудительным лечением.

- Постановление о прекращении уголовного дела и уголовного преследования. Влечет не только полное прекращение уголовного дела, но и преследование лица. В качестве основания выступает отсутствие состава преступления, истечение сроков давности или примирение сторон.

Основным является акт, содержащий выводы (итоги) расследования уголовного дела.

В последнее десятилетие в Казахстане произошли большие изменения. Резко изменившиеся социально-политические и экономические условия жизни казахстанского общества, неподготовленный переход к рыночной экономике, обвальный рост преступности, коррумпированность многих чиновников в органах власти и управления, распространение мошенничества и других злоупотреблений в кредитно-финансовой сфере и предпринимательстве, неэффективность в новых условиях ряда действовавших старых норм уголовного и уголовно-процессуального законодательства отмечались многими социологами и юристами.

Джилкишиев Р.Б.

Новые условия жизни общества требуют обновления действующего законодательства.

В данных условиях необходимо усилить проведение правовой пропаганды и иных мероприятий, основная цель которых - воспитание у социума высокого уровня правосознания и убежденности в недопустимости причинения ущерба. Это могут быть как профилактические мероприятия, так и образовательные программы [143, с. 206].

Мы убеждены, что правонарушения в сфере информации и связи, а также киберпреступления могут быть причиной целью совершения более тяжких преступлений против личности. То есть предотвращение непосредственно самих преступлений в сфере информационных технологий может привести к сокращению общего числа тяжких уголовных преступлений. Следует особо подчеркнуть, что нормы уголовного права, регламентирующие расследование киберпреступлений, это нормы с двойной превенцией, направленные не только на предотвращение непосредственного совершения киберпреступлений, но и на снижение уровня насилия и преступности в целом.

Правовое воспитание в обязательном порядке должно учитывать индикаторы целевой аудитории: возраст, образование, род деятельности, социальные характеристики, географические, этнические, культурные особенности, психологические факторы, степень правовой осведомленности и заинтересованности. Таким образом, правовое воспитание должно иметь целенаправленный характер и адаптировано под различные группы населения.

Здесь хочется отметить важность средств массовой информации в правовом воспитании. Однако не все публикуемые в СМИ материалы соответствуют необходимым требованиям, что в значительной степени снижает эффективность правового просвещения.

Так, СМИ достаточно часто публикуют об инцидентах, связанных с киберпреступлениями, тем не менее, дальнейшие действия ограничиваются лишь порицанием. То есть осуждая преступления, средства массовой информации не раскрывают конкретные правовые последствия совершения преступлений в сфере информационных технологий или действия, предпринятые в качестве ответных мер на их совершение. Подобные действия могут создавать впечатление, что рассматриваемый вид преступлений остается безнаказанным.

Практика ведения уголовных дел в данной сфере свидетельствует о наличии коллизий и пробелов, в частности, на стадии получения цифровых доказательств и взаимодействия со следственными судами и банками второго уровня.

Первостепенной проблемой остается отсутствие единообразного подхода к вопросу получения видеоматериалов, зафиксированных камерами банкоматов. Банковские учреждения второго уровня в ряде случаев требуют предоставления отдельного постановления следственного суда, санкционирующего доступ к изображению лица, осуществлявшего снятие средств. В то же время следственные суды, ссылаясь на правовую природу

Джилкишиев Р.Б.

таких материалов как не требующих специальной санкции, зачастую отказывают в ее выдаче, ссылаясь на нецелесообразность или избыточность подобного запроса. Такая неоднородность правоприменения приводит к задержкам в установлении личности предполагаемых правонарушителей, затрудняет идентификацию соучастников и препятствует эффективному проведению следственных действий.

Второй острой проблемой является запрет со стороны следственных судов на санкционирование в одном постановлении процессуальных действий в отношении нескольких лиц, даже если эти лица прямо связаны между собой в рамках одного уголовного производства. Действующие положения статей 253, 254 и 256 УПК РК не содержат запрета на вынесение одного постановления в отношении нескольких субъектов, однако сложившаяся судебная практика требует оформления отдельного постановления по каждому лицу. Это приводит к значительным временным и организационным издержкам. Пример: если денежные средства, полученные преступным путем, переводятся злоумышленниками в течение короткого промежутка времени (5–10 минут) на десятки счетов, то следственные органы вынуждены готовить и согласовывать до нескольких десятков индивидуальных судебных постановлений, каждое из которых требует отдельного рассмотрения и получения ответа от финансовых учреждений. Такая практика затягивает расследование на месяцы, что создает риски утраты следов преступной деятельности и делает невозможным своевременную блокировку активов.

Третьим затруднением является правовая неопределенность в вопросе возврата потерпевшему денежных средств, находящихся на уже заблокированных счетах, ранее использованных злоумышленниками. На практике такие средства подлежат возврату только после установления подозреваемого лица и принятия по делу соответствующего процессуального решения. Отсутствие нормативно закрепленного механизма оперативного возврата средств значительно снижает доверие граждан к правоохранительной системе и создает ситуацию юридической беззащитности для потерпевших.

Таким образом, вышеуказанные правоприменительные проблемы на сегодняшний день не урегулированы на общереспубликанском уровне, что негативно отражается на качестве досудебного производства по делам, связанным с мошенничеством в сфере информационных технологий. Их устранение требует нормативного и институционального вмешательства со стороны высших органов правосудия и надзора, в частности Верховного Суда, Генеральной прокуратуры и Министерства внутренних дел Республики Казахстан, с целью унификации судебной практики, внесения изменений в уголовно-процессуальное законодательство и разработки единых методических рекомендаций для следственных и судебных органов. Только такой комплексный подход позволит обеспечить эффективность уголовного преследования в условиях стремительной цифровизации преступной среды.

В связи с вышеизложенным мы предлагаем ввести авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан от 4

Джилкишиев Р.Б.

июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 24.05.2025 г.).

В ст. 253 «Выемка» добавить нумерацию в виде части «**1»** без изменения текста: **«**Выемка производится с целью изъятия определенных предметов и документов, имеющих значение для дела, и, если точно известно, где и у кого они находятся, а также имущества, подлежащего конфискации**».** Далее добавить часть 2 и внести дополнение, изложив его в следующей редакции: **«Допускается проведение выемки информации, составляющей банковскую тайну, в отношении нескольких банковских счетов в рамках одного постановления следственного судьи, если данные счета объединены единым эпизодом преступления, рассматриваемого в пределах одного уголовного дела».**

Указанное дополнение направлено на устранение избыточной процессуальной нагрузки, возникающей при расследовании интернет-мошенничеств, когда для каждого счета, на который были перечислены похищенные денежные средства, требуется отдельное постановление суда. Это приводит к необоснованной потере времени и затрудняет оперативное пресечение преступной деятельности. Введение нормы, допускающей коллективную выемку по одному постановлению, в случае логической и фактической связи между счетами, обеспечит оперативность и процессуальную эффективность следственных действий, не нарушая прав субъектов, чьи счета фигурируют в материалах дела.

Также в ст. 253 «Выемка» добавить часть 3 и внести дополнение, изложив его в следующей редакции: **«При расследовании преступлений, связанных с незаконным оборотом денежных средств, полученных посредством информационно-коммуникационных технологий, допускается производство выемки видео- и фотоматериалов, зафиксированных техническими средствами банков второго уровня (в том числе банкоматами), без обязательного судебного санкционирования, при наличии возбужденного уголовного дела и официального запроса органа уголовного преследования».**

Данное нововведение призвано устранить неоднородность правоприменительной практики, сложившейся в отношении получения изображений лиц, снимающих деньги в банкоматах после совершения интернет-мошенничества. Некоторые следственные суды отказывают в выдаче санкций, ссылаясь на общедоступность информации, в то время как банки требуют постановление. Закрепление права следственных органов на получение таких данных без предварительного судебного постановления, при наличии уголовного дела, позволит ускорить процесс идентификации лиц, вовлеченных в преступную деятельность, и предотвратит утрату ценных доказательств, особенно в условиях ограниченного времени хранения записей.

В Закон Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 24.05.2025 г.) внести дополнение в ст. 50

Джилкишиев Р.Б.

«Банковская тайна», ч. 4 и добавить п. 13-1), изложив его в следующей редакции: **«предоставление органам уголовного преследования запрашиваемых сведений о банковских операциях и лицах, производящих операции, в течение не более 48 часов с момента получения запроса без судебной санкции, если данный запрос производится в рамках зарегистрированного уголовного дела о мошенничестве с использованием информационных технологий и сетей».**

Предлагаемые изменения позволят правоохранительным органам значительно сократить время на получение необходимой информации о движении денежных средств по банковским счетам и упростят процесс идентификации преступников и их пособников. Сокращение бюрократических процедур позволит повысить раскрываемость преступлений, оперативно возвращать средства потерпевшим и значительно усилит эффективность борьбы с интернет-мошенничеством.

В целях повышения безопасности и предотвращения мошеннических действий при выдаче онлайн-кредитов предлагается ввести обязательный период ожидания между подачей заявки и перечислением денежных средств. Согласно предлагаемым изменениям, онлайн-кредитование должно осуществляться с временным промежутком не менее 24 часов после подачи заявки. Данная мера необходима для обеспечения возможности сотрудникам кредитных организаций провести дополнительную проверку информации и идентификацию возможных признаков мошенничества.

В течение указанного обязательного периода сотрудники банков и микрокредитных организаций должны провести индивидуальную консультацию с заявителем посредством телефонной или видеосвязи. Основной задачей консультации является подтверждение личности клиента, его намерений и проверка отсутствия признаков вовлеченности клиента в мошеннические схемы. При этом необходимо вести обязательный протокол таких консультаций, который будет храниться в информационной системе финансовой организации.

Дополнительно предлагается ограничить возможность выдачи крупных сумм в формате онлайн-кредитования. Кредиты на сумму, превышающую один миллион тенге, должны предоставляться исключительно через личное обращение клиента в отделения банков и микрокредитных организаций. Введение такого ограничения обусловлено необходимостью минимизации рисков, связанных с крупными финансовыми потерями, вызванными действиями мошенников.

Личная процедура оформления кредита на крупные суммы предполагает обязательную идентификацию клиента с использованием документов, удостоверяющих личность. При этом заявитель в присутствии сотрудника должен заполнить соответствующую заявку, указав целевое назначение кредита. Дополнительно сотрудник обязан разъяснить клиенту потенциальные мошеннические схемы, с которыми сталкиваются граждане при получении кредитных средств.

Джилкишиев Р.Б.

Ожидается, что внедрение предложенных изменений существенно сократит количество случаев мошенничества, повысит защищенность финансовых интересов граждан и укрепит доверие населения к кредитным учреждениям. Для успешного внедрения данных предложений необходимо внесение соответствующих изменений в нормативные правовые акты Республики Казахстан, регулирующие деятельность финансовых организаций, а также активное участие Национального банка и Агентства Республики Казахстан по регулированию и развитию финансового рынка.

На основе анализа закона Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 24.05.2025 г.) предлагаются следующие конкретные изменения и дополнения, направленные на предотвращение случаев мошенничества при получении онлайн-кредитов.

А) В ст. 34 «Банковская заемная операция» добавить авторское изменение ч. 3-3, изложив его в следующей редакции: **«Выдача онлайн-кредитов физическим лицам осуществляется банками и микрокредитными организациями не ранее чем через 24 часа с момента подачи онлайн-заявки. В указанный период сотрудники кредитных организаций обязаны провести дополнительную проверку информации и провести консультацию с заявителем, направленную на выявление признаков мошенничества и подтверждение намерений клиента в отношении целевого использования кредита».**

Данное дополнение вводится с целью обязательной проверки получателей онлайн-кредитов, что позволит снизить риск мошенничества. Обязательный период ожидания в 24 часа позволит сотрудникам банков и микрокредитных организаций детально изучить каждую заявку и своевременно обнаружить признаки возможного обмана, предотвращая финансовые потери граждан.

Б) Также в указанную статью дополнить ч.3-4, изложив его в следующей редакции: **«Кредиты на сумму от 1 миллиона тенге и выше выдаются физическим лицам только при личном обращении клиента в отделение банка или микрокредитную организацию. Выдача таких кредитов в онлайн-формате запрещается».**

Указанное дополнение направлено на уменьшение рисков при крупных финансовых операциях, проводимых дистанционно. Введение ограничения на выдачу значительных сумм онлайн-кредитов требует обязательного личного присутствия клиента, что существенно снижает вероятность обмана и обеспечивает надежную идентификацию и подтверждение намерений клиента.

В) В ст. 31 «Общие требования к операциям, проводимым банками» далее внести дополнение ч. 2-2) с авторским изложением в следующей редакции: **«Банки обязаны вести протоколы консультаций, проводимых в период проверки онлайн-заявок на кредиты, с обязательной регистрацией результатов проверки на предмет признаков мошеннических действий.**

Джилкишиев Р.Б.

Указанные протоколы хранятся не менее трех лет и предоставляются правоохранительным органам по официальному запросу».

Введение обязательного протоколирования проверок и консультаций при выдаче онлайн-кредитов обеспечит дополнительную защиту интересов клиентов и упростит взаимодействие с правоохранительными органами при расследовании случаев мошенничества.

Эти изменения позволят повысить безопасность финансовых операций и обеспечить правовую защиту граждан Республики Казахстан в условиях стремительно развивающихся цифровых технологий.

Современные наркопреступники все чаще используют бесконтактные схемы сбыта наркотиков, привлекая так называемых «закладчиков» – лиц, которые тайно размещают дозы в укромных местах для последующей передачи покупателям. Такая модель распространения реализуется посредством интернета, оплата за «товар» производится через электронные платежи, включая криптовалюты, после чего покупателю сообщаются координаты тайника с наркотическим средством. Отмечается стремительный рост доли наркосделок, совершаемых через социальные мессенджеры (Telegram, WhatsApp) и даркнет, особенно при распространении синтетических наркотиков. Доставка нередко осуществляется курьерами под видом сервисов доставки еды и других товаров. Данные тенденции требуют выработки новой стратегической линии борьбы с наркопреступностью, учитывающей цифровой характер деятельности закладчиков и обеспечивающей всестороннее противодействие этому опасному явлению.

Предлагаемые ниже научные положения обладает существенной практической значимостью, разработанные рекомендации могут быть внедрены как в виде нормативных правовых актов, так и через пилотные проекты и цифровые решения.

Результаты исследования могут лечь в основу совершенствования законодательства РК. Необходимо уточнить уголовно-правовые нормы, вводя понятия, отражающие специфику бесконтактного сбыта (например, квалифицировать организацию «наркотайников» как отягчающее обстоятельство). Уже предприняты важные шаги, так, с января 2025 года в Казахстане ужесточена ответственность за производство и сбыт наркотиков и одновременно смягчены санкции для исполнителей низового звена. В частности, для впервые осужденных курьеров-закладчиков без отягчающих обстоятельств верхний предел наказания снижен с 10 до 8 лет лишения свободы, учитывая, что такие лица часто не участвуют непосредственно в производстве наркотиков и используются преступными группами как расходное звено. Дальнейшее развитие нормативной базы может включать утверждение ведомственных инструкций по взаимодействию полиции и интернет-провайдеров, регулирование порядка мониторинга мессенджеров (Telegram, WhatsApp) и даркнета в рамках оперативно-розыскной деятельности, а также улучшение механизмов конфискации имущества, полученного от

Джилкишиев Р.Б.

дистанционной торговли наркотиками (например, средств на электронных кошельках).

Практическое внедрение предполагает создание специализированных цифровых платформ в помощь правоохранительной системе.

Во-первых, это единая информационная система (национальная база данных) инцидентов, связанных с наркозакладками, интегрированная с геоинформационными сервисами, такая платформа позволит отслеживать географию распространения закладок, типовые места тайников, оперативно информировать территориальные органы о выявленных случаях.

Во-вторых, целесообразно разработать онлайн-портал или мобильное приложение для населения с удобным интерфейсом, куда граждане смогут анонимно сообщать об обнаруженных подозрительных свертках или о лицах, ведущих себя подозрительно, например, роющихся в земле во дворах и парках. Такой портал должен напрямую передавать информацию в полицию и автоматически фиксировать координаты, что ускорит реакцию.

В-третьих, необходима внутренняя аналитическая платформа для киберполиции, использующая технологии искусственного интеллекта для мониторинга открытых источников, социальных сетей (Telegram, WhatsApp) и даркнета на наличие предложений о продаже наркотиков, с возможностью автоматической передачи выявленных данных оперативникам. Совокупность этих цифровых решений значительно повысит эффективность работы и облегчит обмен данными между субъектами борьбы.

Достижение поставленных целей обеспечивается использованием современных способов и методов, ориентированных на специфику деятельности закладчиков. Предлагается следующая совокупность методических подходов:

1. **Интеллектуальный анализ цифровых следов.** Применение методов Big Data и машинного обучения для обработки больших массивов данных, связанных с деятельностью наркосетей. Анализ охватывает переработку информации из соцсетей, мессенджеров, форумов даркнета, а также данных, изъятых у задержанных устройств (смартфонов, ноутбуков). С помощью интеллектуальных алгоритмов выявляются скрытые закономерности – например, типичные лингвистические маркеры переписки наркодилеров, повторяющиеся GPS-координаты, временные шаблоны размещения закладок. Данный метод позволяет прогнозировать потенциальные точки закладок и идентифицировать ранее неизвестных сообщников, повышая проактивность противодействия.

2. **Автоматическое отслеживание по метаданным**, использование технических средств для трассировки метаданных в телекоммуникационных и финансовых сетях. Например, анализ данных сотовой связи (CDR – записи соединений) для выявления подозрительных передвижений, закладчики часто перемещаются хаотично по городу, посещая множество адресов за короткий период. Автоматизированные системы могут помечать абонентов, чья геолокационная активность соответствует подобным паттернам. Аналогично

Джилкишиев Р.Б.

анализируются метаданные платежных систем, частые переводы небольших сумм на разнообразные электронные кошельки, указывающие на возможные расчеты за наркотики. Метаданные не раскрывают содержимое сообщения или цель платежа, но их корреляционный анализ поможет сузить круг подозреваемых для последующей работы оперативников.

3. **Мониторинг даркнета и сетевых площадок.** Постоянное наблюдение за скрытыми онлайн-рынками сбыта наркотиков и сообществами закладчиков. Правоохранительные органы Казахстана уже практикуют работу под прикрытием на таких ресурсах, оперативные агенты выступают покупателями или продавцами в социальных сетях и даркнете для выявления преступных групп. Предлагается расширить данный метод с использованием специального программного обеспечения, способного сканировать известные форумы, торговые площадки в «Tor-сети» и даже закрытые чаты мессенджеров. Выявленная информация, такая как объявления о «товаре», отзывы покупателей, криптокошельки продавцов, анализируется и используется для документирования преступной деятельности. Дополнительно, развитие национальной кибербезопасности через программу «Киберщит» способствует пресечению онлайн-наркоторговли путем привлечения лучших ИТ-специалистов и внедрения современных технологий киберразведки. Мониторинг мессенджеров и даркнета, подкрепленный международным сотрудничеством, обмен данными с правоохранителями других стран, совместные операции, перекроет каналы транзита информации и средств, жизненно важные для деятельности закладчиков.

4. **Работа с населением.** Активное вовлечение общества как метода противодействия. Без поддержки граждан победить распространение наркотиков крайне сложно, поэтому необходимо наладить двустороннюю связь между населением и правоохранителями. Этот метод включает широкое информирование населения о признаках деятельности закладчиков (через СМИ, социальные сети, уличную социальную рекламу), создание доверительных каналов для сообщений (горячие линии, чаты участковых инспекторов, упомянутое выше приложение для граждан). Предлагается поощрять создание добровольных молодежных отрядов или инициатив, по аналогии с движением «Антидилер» в некоторых странах, члены которых помогают выявлять и устранять граффити-рекламу наркотиков на зданиях, информируют полицию о найденных тайниках, участвуют в профилактических мероприятиях в школах. Партисипативные подходы повышают уровень бдительности в обществе, местные жители, зная о проблеме, более склонны сообщать о подозрительной активности во дворах или подъездах, что значительно расширяет возможности органов правопорядка. Таким образом, формируется среда общественного нетерпимого отношения к наркобизнесу.

Реализация указанного комплекса мер и инициатив позволит сформировать в Казахстане стратегическое направление борьбы с наркопреступностью, ориентированное на современные вызовы цифровой эпохи. Предложенная стратегия отличается научной новизной и целостностью

Джилкишиев Р.Б.

подхода, она объединяет правовые реформы, высокотехнологичные инструменты аналитики и активное участие общества для противодействия именно бесконтактным методам сбыта наркотиков. В отличие от традиционных подходов, сконцентрированных преимущественно на силовом пресечении, данное направление акцентирует опережающее выявление угроз и комплексную профилактику, что существенно повышает эффективность борьбы. В результате внедрения предложенных положений ожидается снижение уровня активности закладчиков и связанных с ними наркопреступлений, повышение раскрываемости подобных преступлений, а также укрепление общего правопорядка и безопасности граждан. Такая стратегия может стать модельной не только для Казахстана, но и для других государств, столкнувшихся с проблемой наркотрафика через закладки, демонстрируя новый уровень интеграции усилий государства и общества в противодействии наркоугрозе.

Джилкишиев Р.Б.

ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования необходимо сделать выводы по полученным результатом диссертационной работы:

1. На основе проведенного анализа современного состояния противодействия киберпреступности в Республике Казахстан, а также мировой практики, можно сделать ряд фундаментальных выводов, отражающих текущие вызовы и перспективы данной сферы.

Анализ выявил, что за последние годы значительно увеличилось число зарегистрированных киберпреступлений, причем основную долю составляют интернет-мошенничества. В частности, статистика последних пяти лет демонстрирует постоянный рост правонарушений в области информационных технологий, а также свидетельствует о высоком уровне латентности подобных преступлений. Значительный объем преступлений остается нераскрытым, что связано как с техническими сложностями расследования, так и с пробелами в нормативно-правовой базе и недостаточной подготовленностью специалистов правоохранительных органов.

На наш взгляд, необходимо разработать и принять в нашей стране новый закон «О противодействии киберпреступности» по аналогии с модельным законом «О противодействии киберпреступности» разработанным и утвержденным Межпарламентской Ассамблея государств-участников СНГ [22]. Необходимость данного закона в Казахстане вызвана стремительным ростом числа преступлений в цифровой сфере, которые представляют серьезную угрозу правам граждан, устойчивости экономики и национальной безопасности. Актуальность данного закона определяется не только увеличением общего количества киберпреступлений, их число за последние годы возросло более чем в 40 раз, но и низкой эффективностью их раскрываемости в рамках действующего законодательства, которое фрагментарно и не всегда соответствует международным стандартам и реалиям цифровой экономики.

Одной из главных рекомендаций, вытекающих из проведенного исследования, является необходимость постоянного и системного повышения квалификации сотрудников правоохранительных органов. Целесообразно создать специализированные образовательные программы на основе международного опыта, внедрять в учебный процесс технологии цифрового расследования, такие как искусственный интеллект и аналитические системы обработки больших данных. Дополнительно необходимо развивать специальные подразделения, оснащенные передовыми техническими средствами, и формировать экспертные группы, занимающиеся разработкой и внедрением инновационных методов противодействия киберпреступности.

С учетом выявленных особенностей и тенденций необходимо активно развивать методы профилактики киберпреступлений, включая просветительскую работу с населением, волонтерскую деятельность и общественные инициативы, направленные на повышение уровня цифровой грамотности граждан.

Джилкишиев Р.Б.

2. На основании глубокого анализа отечественной и зарубежной практики, а также с учетом опыта правоприменения, предлагается внести следующие авторские изменения и дополнения в Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 19.05.2025 г.)

А) В ст. 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций» добавить пункт 4) и внести дополнение, изложив его в следующей редакции:

«Те же действия, совершенные с использованием технологий искусственного интеллекта или с применением специальных программных средств, позволяющих осуществлять массовый автоматизированный подбор паролей или обход систем идентификации и защиты информации, -

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет».

Б) Добавить **ст. 213-1 «Незаконное использование цифровых персональных данных»,** далее добавить нижеследующие части с авторским изложением в следующей редакции: **«1. Сбор, хранение, распространение или незаконное использование цифровых персональных данных без согласия лица, если эти действия повлекли значительный ущерб, -**

наказываются штрафом в размере до двух тысяч месячных расчетных показателей или исправительными работами на срок до двух лет.

3. Те же действия, совершенные группой лиц по предварительному сговору, либо с использованием служебного положения, либо повлекшие тяжкие последствия, -

наказываются лишением свободы на срок до пяти лет с лишением права занимать определенные должности на срок до трех лет».

В) В ст. 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» добавить часть 4 новым квалифицирующим признаком и внести дополнение, изложив его в следующей редакции:

«Деяния, предусмотренные частями первой-третьей настоящей статьи, совершенные с целью дестабилизации работы объектов критической информационной инфраструктуры, -

наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества или без таковой».

Г) Добавить **ст. 212-1 «Цифровое мошенничество»,** далее внести дополнение в виде нижеследующих частей с авторским изложением в следующей редакции:

«1. Мошенничество с использованием информационных технологий, включая обман или злоупотребление доверием пользователей интернета, цифровых платформ, систем электронных платежей, -

Джилкишиев Р.Б.

наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо ограничением или лишением свободы на срок до четырех лет.

8. Те же деяния, совершенные организованной группой, либо причинившие особо крупный ущерб, наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества».

Исключить п. 4) путем обмана или злоупотребления доверием пользователя информационной системы, в ст.190 **Мошенничество, ч.** 2. Мошенничество, совершенное...

Д) В ст. 53 «Обстоятельства, смягчающие уголовную ответственность и наказание» Общей части УК добавить пункт 12) и внести дополнение, изложив его в следующей редакции: **активное содействие расследованию преступлений в сфере информационных технологий, повлекшее раскрытие преступления, возмещение причиненного ущерба или предотвращение дальнейших негативных последствий.**

Таким образом, предложенные авторские изменения в Уголовный кодекс РК и дополнения призваны существенно повысить эффективность правоприменительной практики Республики Казахстан в области противодействия киберугрозам, усилить защиту прав и законных интересов граждан и организаций, а также обеспечить стабильность национальной информационной безопасности страны.

3. Анализ теории и практического материала позволяет выделить следующие первопричины и условия совершения киберпреступлений:

- недостаточность (отсутствие) защитных механизмов объектов, подверженных правонарушениям;
- чересчур мягкое наказание за совершение киберпреступлений, что значительно снижает степень страха потенциальных злоумышленников;
- невозможность полного контроля способов передачи информации.

Рост числа киберпреступлений, а также техническая сложность их совершения вызвали и определенное увеличение внимания к данной проблеме в криминалистической литературе. Однако здесь отсутствует единство в определениях, т.е. на данный момент нет единого подхода к определению дефиниции «криминалистическая характеристика правонарушений в сфере информационных технологий», что в значительной степени затрудняет формирование единой теории и разработку эффективных методов расследования.

Вышеобозначенные причины, а также условия совершения киберпреступлений обладают общим (универсальным) характером и применимы для многих видов объектов, которые могут быть подвержены правонарушениям в сфере информационных технологий, т.е. они имеют широкое распространение, не ограничиваясь лишь отдельными случаями. Устранение данных причин возможно только при выработке системного комплексного подхода, реализуемого на государственном уровне, что может включать совершенствование законодательства, усиление мер безопасности,

Джилкишиев Р.Б.

повышение уровня образования и осведомленности конечных пользователей. Только посредством реформирования можно улучшить ситуацию и добиться значительных изменений в ситуации с киберпреступлениями.

С целью повышения эффективности расследования преступлений в сфере информационных технологий предлагается внедрение специализированного программно-аналитического комплекса (далее – СПАК), обеспечивающего автоматизированный сбор, анализ и хранение цифровых доказательств с применением искусственного интеллекта. СПАК позволит систематизировать данные, ускорить формирование экспертных заключений и улучшить межведомственное взаимодействие. Его внедрение на базе Центра судебных экспертиз и перспективно — в рамках Национального центра кибербезопасности, обеспечит сокращение сроков расследований, повышение квалификации специалистов и повышение качества цифровой криминалистики в Казахстане. Также имеется альтернатива: в будущем СПАК можно будет применять в ранее нами предложенном новом Национальном центре управления кибербезопасностью и цифровой криминалистики.

4. Анализ мировых практик показывает, что успешная борьба с киберпреступностью требует создания специализированных национальных центров, которые объединяют технические, аналитические и организационные ресурсы для централизованного и эффективного управления кибербезопасностью. Яркими примерами таких структур являются Национальный центр кибербезопасности Великобритании (NCSC), Канадский центр кибербезопасности (CCCS), Австралийский центр кибербезопасности (ACSC) и Национальный центр интеграции кибербезопасности и коммуникаций США (NCCIC). Их опыт демонстрирует значительное повышение способности стран оперативно выявлять и реагировать на кибератаки, обеспечивать защиту критически важной инфраструктуры, проводить цифровую криминалистику и координировать действия различных ведомств и организаций.

Исходя из вышеизложенного, можно рекомендовать создание и развитие аналогичного **«Национального центра управления кибербезопасностью и цифровой криминалистики» (НЦУКЦК)** в Казахстане. Центр будет объединять усилия правоохранительных и специальных государственных органов (МВД, КНБ, Агентство по финансовому мониторингу и других заинтересованных государственных органов), частного сектора и международных партнеров, обеспечивая обмен информацией о киберинцидентах через единую цифровую платформу на основе блокчейн-технологий. Среди ключевых функций – формирование базы киберпреступлений, оперативный обмен данными, развитие цифровой криминалистики с использованием «ИИ» и «Big Data», создание института киберследователей, а также установление механизмов международного сотрудничества. Законодательное обеспечение предлагается реализовать через принятие специального закона «О противодействии киберпреступности».

Джилкишиев Р.Б.

5. С учетом интенсивного роста количества и сложности преступлений, совершаемых с использованием информационных и цифровых технологий, а также международного опыта и современных стандартов расследования, предлагаются следующие авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 24.05.2025 г.).

А) В главу 3 «Уголовное преследование» добавить **ст. 34-1 «Особенности уголовного преследования по делам о киберпреступлениях»,** далее добавить нижеследующие части с авторским изложением в следующей редакции:

«1. При производстве уголовного преследования по уголовным делам о преступлениях, совершенных с использованием информационно-коммуникационных технологий, орган дознания и следователь вправе использовать специализированные программно-технические комплексы для сбора и закрепления цифровых доказательств.

3. Доказательства, полученные с использованием специализированных программно-технических комплексов, должны сопровождаться подробным техническим описанием процедур получения и сохранения данных».

Предложение направлено на обеспечение допустимости и достоверности цифровых доказательств, получаемых при расследовании киберпреступлений. Это также позволит унифицировать и повысить качество досудебного расследования.

Б) В главу 15 «Доказательства» добавить новую **ст. 118-1 «Цифровые доказательства»,** затем добавить 1 и 2 часть с авторским изложением в следующей редакции:

«1. Цифровыми доказательствами признаются любые электронные данные, полученные из информационных систем, компьютерных устройств, серверов, мобильных устройств, облачных сервисов, а также информация, извлеченная в результате негласного снятия информации с компьютерных систем в соответствии со статьей 245 настоящего Кодекса.

3. Порядок сбора, фиксации и использования цифровых доказательств определяется Правилами, утверждаемыми Генеральной прокуратурой Республики Казахстан совместно с уполномоченным органом в области цифрового развития».

Введение четкой дефиниции и стандартизации цифровых доказательств необходимо для обеспечения их процессуальной чистоты, что существенно повышает эффективность уголовного судопроизводства по киберпреступлениям.

В) В ст. 197 «Общие правила производства следственных действий» добавить часть 7 и внести дополнение, изложив его в следующей редакции: **«В случаях расследования преступлений в сфере информационных технологий допускается дистанционное производство следственных действий с использованием технологии видеоконференцсвязи при условии**

Джилкишиев Р.Б.

соблюдения требований идентификации участников и защиты конфиденциальности данных, полученных в ходе следственного действия».

Данное предложение направлено на оптимизацию и ускорение расследования киберпреступлений, особенно с учетом трансграничного характера таких преступлений и необходимости оперативного взаимодействия с участниками процесса, находящимися за пределами Республики Казахстан.

Г) В ст. 245 «Негласное снятие информации с компьютеров, серверов и других устройств» добавить часть 4 и внести дополнение, изложив его в следующей редакции: **«Результаты негласного снятия информации, произведенного в рамках расследования преступлений, совершенных с использованием информационных технологий, подлежат обязательному экспертному исследованию с привлечением специалистов в области кибербезопасности».**

Необходимость экспертного подтверждения результатов негласных мероприятий обусловлена сложностью технологических аспектов цифровой информации, что исключает возможность ошибок и гарантирует юридическую значимость собранных данных.

Д) Добавить новую главу **30-1 «Особенности производства по уголовным делам о киберпреступлениях»**, после чего добавить **ст.251-1. «Особенности досудебного расследования киберпреступлений»**, далее внести нижеследующие части авторским изложением в следующей редакции:

«1. При досудебном расследовании преступлений, совершенных в цифровом пространстве, обязательным является участие специалиста или эксперта в области информационных технологий и кибербезопасности на всех этапах сбора, анализа и оценки доказательств.

4. Следователь вправе поручать проведение технических исследований объектов цифровых преступлений специализированным экспертным учреждениям.

5. Участники уголовного процесса по делам о киберпреступлениях обеспечиваются правом получения полной информации о методах сбора и анализа цифровых данных, используемых в рамках следственных мероприятий».

Специализация расследования киберпреступлений обеспечит повышение профессионального уровня проводимых мероприятий и минимизацию риска процессуальных ошибок, связанных с техническими аспектами расследования таких преступлений.

Е) В ст. 576 «Проведение процессуальных действий путем проведения видеосвязи» добавить часть 7 и внести дополнение, изложив его в следующей редакции: **«В случаях проведения видеосвязи при расследовании трансграничных преступлений в области информационных технологий, обеспечение идентификации личности участников видеоконференции и защиты передаваемых данных осуществляется в соответствии с международными стандартами цифровой идентификации и защиты данных».**

Джилкишиев Р.Б.

Повышение надежности идентификации участников трансграничного процесса и защиты конфиденциальности информации необходимо для международного сотрудничества и признания собранных доказательств за рубежом.

Предложенные авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан создают целостную нормативную базу, способную обеспечить эффективное уголовно-процессуальное регулирование в области противодействия киберпреступлениям. Они учитывают специфику и сложность современных преступлений, совершенных в цифровом пространстве, и дают четкие ориентиры правоохранительным и судебным органам для грамотного осуществления расследования и судебного рассмотрения данных категорий уголовных дел.

6. По итогам анализа можно заключить, что действующая следственная практика в Республике Казахстан еще не в полной мере адаптирована к специфике расследования правонарушений, совершаемых в цифровом пространстве. Вызывает озабоченность отсутствие единых методических рекомендаций, недостаточный уровень технической оснащенности подразделений, специализирующихся на расследовании киберпреступлений, а также ограниченный круг специалистов, способных квалифицированно проводить осмотр цифровых объектов и анализировать информацию в формате электронных данных. Данные обстоятельства снижают качество первоначальных следственных действий и нередко приводят к потере критически важной информации.

В качестве предложения по улучшению следственной практики в данной сфере целесообразно разработать и утвердить на уровне Министерства внутренних дел и Генеральной прокуратуры Республики Казахстан официальную инструкцию (методические рекомендации) по алгоритму действий следователя при выявлении, фиксации и анализе цифровых следов на первичном этапе расследования. Данный документ должен предусматривать стандартизированные формы взаимодействия с телекоммуникационными операторами, банками, хостинг-провайдерами и другими структурами, вовлеченными в функционирование цифровой инфраструктуры.

Современные вызовы в сфере цифровых технологий и информационной безопасности требуют принципиального пересмотра подходов к проведению судебно-экспертных исследований в Казахстане. Усиление угроз со стороны киберпреступности делает актуальным создание надежной нормативной основы, способной регулировать судебно-экспертную деятельность в области цифровой криминалистики. Это обуславливает необходимость внесения целого ряда нововведений в Закон Республики Казахстан от 10 февраля 2017 года № 44-VI «О судебно-экспертной деятельности» (с изменениями по состоянию на 03.09.2023 г.).

В связи с этим мы предлагаем научно обоснованные дополнения и изменения, направленные на модернизацию законодательства с учетом

Джилкишиев Р.Б.

передового международного опыта и современных стандартов. Приведенные нововведения включают закрепление понятийного аппарата, касающегося цифровых криминалистических экспертиз, детализацию объектов и методов исследования цифровых доказательств, а также определение квалификационных требований к судебным экспертам, специализирующимся в сфере информационных технологий.

Введение предложенных изменений позволит существенно повысить качество и эффективность судебно-экспертных исследований, обеспечить надлежащий уровень защиты прав и законных интересов граждан, организаций и государства при расследовании компьютерных и иных киберпреступлений. Кроме того, это создаст условия для широкого внедрения современных технических и методологических средств, необходимых для успешной реализации экспертной деятельности в условиях цифровизации правовой среды.

А) **В ст. 1 «Разъяснение некоторых понятий, содержащихся в настоящем Законе» добавить** п. 16) и внести авторское понятие «**цифровая криминалистическая экспертиза»,** изложив его в следующей редакции: **«цифровая криминалистическая экспертиза – вид судебной экспертизы, основанный на применении специальных знаний и технических средств для выявления, анализа, интерпретации и документирования цифровых доказательств, извлеченных из компьютерных систем, сетевых структур, мобильных устройств и других электронных носителей информации».**

Отсутствие четкого понятия цифровой криминалистической экспертизы в законе затрудняет ее институционализацию и ограничение от смежных видов исследований. Введение термина позволит легализовать данную сферу как самостоятельную экспертную специализацию.

Б) **В ст. 4 «Содержание судебно-экспертной деятельности» добавить** пункт 6) и внести дополнение, изложив его в следующей редакции: «**организация и проведение судебных экспертиз в области цифровой криминалистики и информационной безопасности, включая сбор, анализ и интерпретацию цифровых доказательств, извлеченных из электронных источников».**

Данное дополнение необходимо, так как оно направлено на расширение содержания судебно-экспертной деятельности с учетом современных вызовов, связанных с расследованием киберпреступлений.

В) Включить в ст. 12 «**Компетенция Министерства юстиции Республики Казахстан»** новый подпункт 10-1) и внести дополнение, изложив его в следующей редакции: **«разработка и утверждение перечня экспертных специальностей и методик, используемых при производстве цифровых криминалистических экспертиз, а также стандартов безопасности и процедур обращения с цифровыми доказательствами».**

Введение единой регуляции цифровой экспертизы и создание перечня признанных методов обеспечат правовую допустимость таких доказательств в суде и устойчивость к оспариванию.

Джилкишиев Р.Б.

Г) **В ст. 4 «Содержание судебно-экспертной деятельности» добавить** п. 6) и внести дополнение, изложив его в следующей редакции: «**организация и проведение судебных экспертиз в области цифровой криминалистики и информационной безопасности, включая сбор, анализ и интерпретацию цифровых доказательств, извлеченных из электронных источников».**

Данное дополнение необходимо, так как оно направлено на расширение содержания судебно-экспертной деятельности с учетом современных вызовов, связанных с расследованием киберпреступлений.

Д) Добавить в ст. 19 **«Судебный эксперт»** п. 1-1 и внести дополнение, изложив его в следующей редакции: **«Судебным экспертом в области цифровых криминалистических экспертиз может быть лицо, имеющее высшее техническое образование в области информационной безопасности, программирования или кибербезопасности, прошедшее специальную подготовку и получившее квалификационное свидетельство (лицензию)».**

В п. 2 «Лица, указанные в подпунктах 1) и 2) пункта 1 настоящей статьи, должны состоять в гражданстве Республики Казахстан» соответственно внести изменение, дополнив и изложив его в следующей редакции: **«Лица, указанные в подпунктах 1) и 2) пункта 1 и 1-1 настоящей статьи, должны состоять в гражданстве Республики Казахстан».**

Четкая квалификация и лицензирование для экспертов по цифровым следам позволит отбирать специалистов с надлежащими техническими знаниями и гарантировать научную обоснованность экспертиз.

Е) Добавить в ст. 32 «Объекты судебной экспертизы» новый п. 2-1 и внести авторское дополнение, изложив его в следующей редакции: **«К объектам цифровой криминалистической экспертизы относятся электронные устройства, их компоненты (жесткие, мягкие, CD и DVD диски, флеш-накопители, SIM-карты и др.), данные в облачных хранилищах, сетевой трафик, лог-файлы, данные с мессенджеров, соцсетей, почтовых и платежных систем, а также программное обеспечение».**

7. Мы предлагаем ввести авторские изменения и дополнения в Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 24.05.2025 г.).

В ст. 253 «Выемка» добавить нумерацию в виде части «**1»** без изменения текста: **«**Выемка производится с целью изъятия определенных предметов и документов, имеющих значение для дела, и, если точно известно, где и у кого они находятся, а также имущества, подлежащего конфискации**».** Далее добавить часть 2 и внести дополнение, изложив его в следующей редакции: **«Допускается проведение выемки информации, составляющей банковскую тайну, в отношении нескольких банковских счетов в рамках одного постановления следственного судьи, если данные счета объединены единым эпизодом преступления, рассматриваемого в пределах одного уголовного дела».**

Джилкишиев Р.Б.

Указанное дополнение направлено на устранение избыточной процессуальной нагрузки, возникающей при расследовании интернет-мошенничеств, когда для каждого счета, на который были перечислены похищенные денежные средства, требуется отдельное постановление суда. Это приводит к необоснованной потере времени и затрудняет оперативное пресечение преступной деятельности. Введение нормы, допускающей коллективную выемку по одному постановлению, в случае логической и фактической связи между счетами, обеспечит оперативность и процессуальную эффективность следственных действий, не нарушая прав субъектов, чьи счета фигурируют в материалах дела.

Также в ст. 253 «Выемка» добавить часть 3 и внести дополнение, изложив его в следующей редакции: **«При расследовании преступлений, связанных с незаконным оборотом денежных средств, полученных посредством информационно-коммуникационных технологий, допускается производство выемки видео- и фотоматериалов, зафиксированных техническими средствами банков второго уровня (в том числе банкоматами), без обязательного судебного санкционирования, при наличии возбужденного уголовного дела и официального запроса органа уголовного преследования».**

Данное нововведение призвано устранить неоднородность правоприменительной практики, сложившейся в отношении получения изображений лиц, снимающих деньги в банкоматах после совершения интернет-мошенничества. Некоторые следственные суды отказывают в выдаче санкций, ссылаясь на общедоступность информации, в то время как банки требуют постановление. Закрепление права следственных органов на получение таких данных без предварительного судебного постановления, при наличии уголовного дела, позволит ускорить процесс идентификации лиц, вовлеченных в преступную деятельность, и предотвратит утрату ценных доказательств, особенно в условиях ограниченного времени хранения записей.

В Закон Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 24.05.2025 г.) внести дополнения в ст. 50 «Банковская тайна», ч. 4 и добавить п. 13-1), изложив его в следующей редакции: **«предоставление органам уголовного преследования запрашиваемые сведения о банковских операциях и лицах, производящих операции, в течение не более 48 часов с момента получения запроса без судебной санкции, если данный запрос производится в рамках зарегистрированного уголовного дела о мошенничестве с использованием информационных технологий и сетей».**

Предлагаемые изменения позволят правоохранительным органам значительно сократить время на получение необходимой информации о движении денежных средств по банковским счетам и упростят процесс идентификации преступников и их пособников. Сокращение бюрократических процедур позволит повысить раскрываемость преступлений, оперативно

Джилкишиев Р.Б.

возвращать средства потерпевшим и значительно усилит эффективность борьбы с интернет-мошенничеством.

На основе анализа закона Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 24.05.2025 г.) предлагаются следующие конкретные изменения и дополнения, направленные на предотвращение случаев мошенничества при получении онлайн-кредитов.

А) В ст. 34 «Банковская заемная операция» добавить авторское изменение ч. 3-3, изложив его в следующей редакции: **«Выдача онлайн-кредитов физическим лицам осуществляется банками и микрокредитными организациями не ранее чем через 24 часа с момента подачи онлайн-заявки. В указанный период сотрудники кредитных организаций обязаны провести дополнительную проверку информации и провести консультацию с заявителем, направленную на выявление признаков мошенничества и подтверждение намерений клиента в отношении целевого использования кредита».**

Данное дополнение вводится с целью обязательной проверки получателей онлайн-кредитов, что позволит снизить риск мошенничества. Обязательный период ожидания в 24 часа позволит сотрудникам банков и микрокредитных организаций детально изучить каждую заявку и своевременно обнаружить признаки возможного обмана, предотвращая финансовые потери граждан.

Б) Также в указанную статью дополнить ч.3-4, изложив его в следующей редакции: **«Кредиты на сумму от 1 миллиона тенге и выше выдаются физическим лицам только при личном обращении клиента в отделение банка или микрокредитной организации. Выдача таких кредитов в онлайн-формате запрещается».**

Указанное дополнение направлено на уменьшение рисков при крупных финансовых операциях, проводимых дистанционно. Введение ограничения на выдачу значительных сумм онлайн-кредитов требует обязательного личного присутствия клиента, что существенно снижает вероятность обмана и обеспечивает надежную идентификацию и подтверждение намерений клиента.

В) В ст. 31 «Общие требования к операциям, проводимым банками» далее внести дополнение ч. 2-2) с авторским изложением в следующей редакции: **«Банки обязаны вести протоколы консультаций, проводимых в период проверки онлайн-заявок на кредиты, с обязательной регистрацией результатов проверки на предмет признаков мошеннических действий. Указанные протоколы хранятся не менее трех лет и предоставляются правоохранительным органам по официальному запросу».**

Введение обязательного протоколирования проверок и консультаций при выдаче онлайн-кредитов обеспечит дополнительную защиту интересов клиентов и упростит взаимодействие с правоохранительными органами при расследовании случаев мошенничества.

Джилкишиев Р.Б.

Джилкишиев Р.Б.

В условиях стремительного роста бесконтактного сбыта наркотиков через интернет, мессенджеры и даркнет, предлагается сформировать в Казахстане стратегию противодействия цифровым формам наркопреступности, акцентируя внимание на закладчиках. Ключевые меры включают: совершенствование законодательства с введением специальных квалифицирующих признаков, создание цифровых платформ для мониторинга и обмена данными, а также внедрение интеллектуальных систем анализа цифровых следов и метаданных. Предусматривается активное вовлечение общества, разработка мобильных приложений для сообщений о закладках, расширение оперативной деятельности в даркнете и использование ИИ для выявления преступных схем. Комплексный подход обеспечит снижение наркоугроз и повышение эффективности правоохранительной деятельности.

Джилкишиев Р.Б.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Статистические сведения из отчетности 1-М за 2019-2023 гг. / Правовая статистика. [Электронный ресурс] – Режим доступа: https://qamqor.gov.kz/crimestat/statistics (дата обращения: 10.09.2024).

2. Исаев А.А. Применение специальных познаний для квалификации преступлений. – Алматы: Мектеп, 1997 – 234 с.

3. Что такое киберпреступность? [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 11.09.2024).

4. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): Постановление Правительства Республики Казахстан от 30 июня 2017 года №407. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 14.09.2024).

5. Об утверждении Концепции обеспечения общественной безопасности в партнерстве с обществом на 2024 – 2028 годы (в сфере профилактики правонарушений): Постановление Правительства Республики Казахстан от 29 декабря 2023 года №1233. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P2300001233 (дата обращения: 14.09.2024).

6. Невоструева А.Ф. Единое информационно-коммуникационное пространство: теория и реальность // Дискуссия. - 2012. - №10. – С. 106-109.

7. Computer Hardware, Software, and Networks. [Electronic resource] – Access mode: https://open.ocolearnok.org/informationsystems/chapter/chapter-2-computer-hardware-software-and-networks/ (date of access: 20.09.2024).

8. Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: дисс… канд. юрид. наук: 12.00.08 – Краснодар, 2001. – 216 с.

9. Революционные изменения в промышленности. [Электронный ресурс] – Режим доступа: https://issek.hse.ru/trendletter/news/196231394.html (дата обращения: 26.09.2024).

10. Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: Сб. матер. межд. конф. 1–2 марта 2001 г. – Алматы: Интернет трейнинг центр, 2001. – С.34.

11. Аскербекова Д.Т. Юридический анализ правонарушений в сфере информационных технологий в Республике Казахстан // Проблемы Науки. - 2015. - №9 (39). https://cyberleninka.ru/article/n/yuridicheskiy-analiz-pravonarusheniy-v-sfere-informatsionnyh-tehnologiy-v-respublike-kazahstan/viewer (дата обращения: 27.09.2024).

12. Исполнимо ли международное законодательство и договоры в киберпространстве. [Электронный ресурс] – Режим доступа: https://digital.report/dogovoryi-v-kiberprostranstve/ (дата обращения: 08.10.2024).

Джилкишиев Р.Б.

13. Нугманова А.Т. Частная жизнь граждан под наблюдением высоких технологий // Вестник Университета им. Д. Кунаева. – 2005. – № 2(15). – С. 34-39.

14. Нугманова (Завотпаева) А.Т. Преступления в сфере высоких информационных технологий: теория и практика их расследования на первоначальном этапе. Дисс... канд. юрид. наук. - Караганда, 2007. – 165 с.

15. Департамент криминальной полиции МВД РК. [Электронный ресурс] – Режим доступа: https://www.gov.kz/memleket/entities/qriim/about/structure/departments/activity/355/1?lang=ru (дата обращения: 10.10.2024).

16. О некоторых вопросах Агентства Республики Казахстан по финансовому мониторингу: Указ Президента Республики Казахстан от 20 февраля 2021 года № 515. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/U2100000515 (дата обращения: 13.10.2024).

17. Серия университетских модулей: киберпреступность. [Электронный ресурс] – Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/teaching-guide/executive-summary.html (дата обращения: 16.10.2024).

18. Convention on Cybercrime, Budapest, 2001 / Official web-site of Council of Europe. [Electronic resource] – Access mode: http://conventions.coe.int./Treaty/en/Treaties/Html/185.htm (date of access: 20.10.2024).

19. Об утверждении Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Указ Президента Республики Казахстан от 25 июня 2002 года №897. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/U020000897_ (дата обращения: 22.10.2024).

20. Лоскутов И.Ю. Генеральный директор ТОО «Компания «ЮрИнфо» Доклад на межд.-практ. конф. «Актуальные вопросы развития уголовного законодательства в рамках разработки нового Уголовного кодекса РК» (Алматы, 20 сентября 2012 года). https://online.zakon.kz/Document/?doc_id=38772636&pos=1827;-55#pos=1827;-55 (дата обращения: 25.10.2024).

21. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: Закон Республики Казахстан от 9 декабря 2019 года № 277-VI ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1900000277 (дата обращения: 27.10.2024).

22. Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств от 14 апреля 2023 года №55-20 О модельном законе «О противодействии киберпреступности» (Санкт-Петербург) [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=32027765 (дата обращения: 02.11.2024).

Джилкишиев Р.Б.

23. Бутусова Л.Н. К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. – 2016. - №2. - С. 48-52.

24. Казанцев В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов. [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=30050590&pos=8;-47#pos=8;-47 (дата обращения: 05.11.2024).

25. Кабжанов А.Т. Криминологические аспекты информационной преступности [Текст] / Кабжанов А.Т., Ахметбеков Д. // Теоретико-правовые и правоприменительные вопросы совершенствования законодательства Республики Казахстан в условиях четвертой промышленной революции: Мат-лы межд. научн.-практ. on-line конф., 10-12 апреля 2018 года – С. 100-106. https://rep.keu.kz/bitstream/123456789/315/1/%d0%9a%d0%b0%d0%b1%d0%b6%d0%b0%d0%bd%d0%be%d0%b2.pdf (дата обращения: 11.11.2024).

26. Об информатизации: Закон Республики Казахстан от 24 ноября 2015 года №418-V ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 14.11.2024).

27. О связи: Закон Республики Казахстан от 5 июля 2004 года №567. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z040000567_ (дата обращения: 18.11.2024).

28. О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 года №94-V. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 22.11.2024).

29. Уголовный кодекс Республики Казахстан: Кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 23.11.2024).

30. Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан: под общ.ред. Генерального Прокурора РК Даулбаева А.К. – Алматы: Жеті жарғы, 2015. – 504 с.

31. О доступе к информации: Закон Республики Казахстан от 16 ноября 2015 года №401-V ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000401 (дата обращения: 26.11.2024).

32. Коробеев А.И. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации / А.И. Коробеев, Р.И. Дремлюга, Я.О. Кучина // Всероссийский криминологический журнал. – 2019. – Т.13. - №3. – С. 416-425. – DOI:10.17150/2500- 4255.2019.13(3).416-425.

33. Курбатова М.С. Облачные сервисы хранения данных как объект преступного посягательства в современном мире // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по мат-лам научн.-практ. конф., г. Москва, 11.11.2020 г.: Университет прокуратуры Российской Федерации; МФЮА. – М., 2021. – С. 115-120.

34. Темиржанова Л.А., Абулгазина А.Ж. Проблемы обеспечения информационной безопасности правоохранительных структур и противодействие киберпреступлениям, киберхищениям (национальный и

Джилкишиев Р.Б.

зарубежный опыт) // Совершенствование методов противодействия отдельным формам хищения: Сборник межд. научно-практ. конф., 16-17 ноября 2017 года: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2017. – С. 43-51.

35. Яшков С.А. Проблемы квалификации преступлений, связанных с неправомерным доступом к компьютерной информации: отдельный аспект // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по мат-лам научн.-практ. конф., г. Москва, 11.11.2020 г.: Университет прокуратуры Российской Федерации; МФЮА. – М.: 2021. – С. 28-32.

36. Рубцов И.И. Криминалистическая характеристика преступлений как элемент частных методик расследования: Автореф. дисс. канд. юрид. наук. Спб. - С 2001. – 23 с.

37. Баев О.Я., Гуняев В.А., Матусовский Г.А. и др. Расследование отдельных видов преступлений. - Воронеж, 1986. – 193 с.

38. Коршукова О.Н. Уголовно-процессуальные и криминалистические проблемы уголовного преследования: дисс. …докт. юрид. наук: 12.00.09. – М., 2006. – 418 с.

39. Нукенов М.О. Проблемы борьбы с коррупционной преступностью (уголовно-правовые, криминологические и криминалистические аспекты): дисс. … докт. юрид. наук: 12.00.08. 12.00.09. – Алматы, 2005. – 306 с.

40. Радаев В.В. Криминалистическая характеристика преступлений и ее использование в следственной практике: лекция. – Волгоград: ВСШ МВД СССР, 1987. – 24 с.

41. Коновалова В.Е., Колесниченко А.Н. Криминалистическая характеристика преступлений: сб. науч. тр. – М.: Наука, 1984. – 106 с.

42. Сергунов А.В. Расследование хищений денежных средств при производстве строительных работ: лекция. – Хабаровск: Хабаровская высшая школа МВД СССР, 1990. – 24 с.

43. Куклин В.И., Куклин В.В. Криминалистическая методика: учебное пособие. – Тверь: изд-во Тверского гос. ун-та, 1992. – 84 с.

44. Еркенов С.Е. Взаимодействие правоохранительных органов стран СНГ при раскрытии и расследовании транснациональных преступлений: автореф. … докт. юрид. наук: 12.00.09 – М., 2000. – 47 с.

45. Мозговых Г.А. Криминалистическая характеристика преступлений и ее значение в методике расследования // Вестник КазГУ: серия юридическая. – Алматы, 2000. – № 4 (17). – С. 124-136.

46. Бегалиев Е.Н. Расследование преступлений, совершаемых путем подделки материальных объектов. – Алматы: Дайк-Пресс, 2008, – 364 с.

47. Дашян М.С. Право информационных магистралей (Law of information highways): Вопросы правового регулирования в сфере Интернет. - М: «Волтерс Клувер», 2007. – 275 с.

48. Криминалистика: Учебник / Под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М.: Юридическая литература, 1993. – 592 с.

Джилкишиев Р.Б.

49. Васильев А.Н.; Виноградов И.В.; Ратинов А.Р.; Розенблит С.Я.; Селиванов Н.А.; Ураков Л.И. Осмотр места происшествия: пособие для прокурорско-следственных работников. – М.: Госюриздат, 1960. – 377 с.

50. Быховский И.Е. Осмотр места происшествия. – М.: Юрид.лит., 1973. – 224 с.

51. Моисеенков В.А. Суета вокруг Роберта или Моррис-сын и все, все, все ... // КомпьютерПресс. - 1991. - № 11. – С. 7-20.

52. Повезнюк Г.И. Судебная экспертиза (подготовка и назначение в уголовном и гражданском процессах). Изд. второе, переработ. и доп. – Алматы: Аян Эдет, 2001. – 208 с.

53. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоиздат, 1994. – 400 с.

54. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991. – 160 с.

55. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. Б.П. Смагоринского – М.: Право и Закон, 1996. – 182 с.

56. Хоффман Л. Дж. Современные методы защиты информации. Пер. с англ. М.С. Казарова, М.К. Размахнина / Под ред. В.А. Герасименко. – М.: Сов. Радио, 1980. – 263 с.

57. Дремлюга Р.И. Субкультура хакеров и другие факторы компьютерной преступности // Криминологический журнал Байкальского государственного университета экономики и права. – 2008. – № 4. – С.22-26.

58. Аубакиров А., Ким Э. Криминалистическая экспертиза материалов и веществ: учебное пособие. – Алматы: ВШП «Әділет», 2001. – 222 с.

59. Шевченко Б.И. Научные основы современной трасеологии. Под ред. Зицер Е.У. — М., 1947. – 54 с.

60. Уголовное право. Часть общая. Часть особенная: Учебник для вузов / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. 4-е изд., испр. и доп. – М.: Юриспруденция, 2007. – 751 с.

61. Безруков Н.Н. Компьютерная вирусология: справочное руководство. – Киев: Украинская советская энциклопедия, 1991. – 416 с.

62. National Cyber Force Transforms country's cyber capabilities to protect UK [Electronic resource] – Access mode: https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk (date of access: 10.01.2025).

63. The role of the National Cyber Security Centre (NCSC) [Electronic resource] – Access mode: https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc (date of access: 15.01.2025).

64. We’re the Government Communications Headquarters – otherwise known as GCHQ [Electronic resource] – Access mode: https://www.gchq-careers.co.uk/about-us.html (date of access: 21.01.2025).

65. Cybersecurity in the UK, [Electronic resource] – Access mode: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf (date of access: 24.01.2025).

Джилкишиев Р.Б.

66. FBI, CISA, and UK NCSC Release Guidance on Digital Forensics and Protective Monitoring for Network Devices [Electronic resource] – Access mode: https://www.hstoday.us/subject-matter-areas/cybersecurity/fbi-cisa-and-uk-ncsc-release-guidance-on-digital-forensics-and-protective-monitoring-for-network-devices/ (date of access: 27.01.2025).

67. The NCSC Early Warning Service - an Overview [Electronic resource] – Access mode: https://ciisf.org/blog/the-ncsc-early-warning-service-an-overview (date of access: 30.01.2025).

68. America's Cyber Defense Agency [Electronic resource] – Access mode: https://www.cisa.gov/ (date of access: 03.02.2025).

69. Detangling the Web: A Screenshot of U.S. Government Cyber Activity [Electronic resource] – Access mode: https://ndupress.ndu.edu/Media/News/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/ (date of access: 05.02.2025).

70. Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems [Electronic resource] – Access mode: https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf (date of access: 15.02.2025).

71. Insane Incident Incursion Recursion: Mastering Incident Response Reporting Regulations [Electronic resource] – Access mode: https://www.sans.org/blog/insane-incident-incursion-recursion-mastering-incident-response-reporting-regulations/ (date of access: 19.02.2025).

72. National Security and Intelligence Committee of Parliamentarians Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack [Electronic resource] – Access mode: https://nsicop-cpsnr.ca/reports/rp-2022-02-14/00-en-introduction.html (date of access: 21.02.2025).

73. Canadian Centre for Cyber Security [Electronic resource] – Access mode: https://www.cse-cst.gc.ca/en/information-and-resources/announcements/canadian-centre-cyber-security (date of access: 23.02.2025).

74. About the Cyber Centre [Electronic resource] – Access mode: https://www.cyber.gc.ca/en/about-cyber-centre (date of access: 25.02.2025).

75. National Cyber Threat Assessment 2018 [Electronic resource] – Access mode: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018 (date of access: 01.03.2025).

76. National Cyber Threat Assessment 2023-2024 [Electronic resource] – Access mode: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024?utm_source=chatgpt.com (date of access: 04.03.2025).

77. Australian Cyber Security Centre [Electronic resource] – Access mode: https://en.wikipedia.org/wiki/Australian_Cyber_Security_Centre (date of access: 09.03.2025).

Джилкишиев Р.Б.

78. Australian Cyber Security Centre [Electronic resource] – Access mode: https://www.insupport.com.au/post/what-is-the-acsc-australian-cyber-security-centre (date of access: 12.03.2025).

79. Australia's Cyber Security Strategy 2020 [Electronic resource] – Access mode: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (date of access: 15.03.2025).

80. Cyber Security Strategies of Non-Corporate Commonwealth Entities [Electronic resource] – Access mode: https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities (date of access: 25.03.2025).

81. Cyber agencies unveil new guidelines to secure edge devices from increasing threat [Electronic resource] – Access mode: https://www.ncsc.gov.uk/news/cyber-agencies-unveil-new-guidelines-to-secure-edge-devices-from-increasing-threat (date of access: 25.03.2025).

82. ACSC annual cyber threat report released [Electronic resource] – Access mode: https://www.minister.defence.gov.au/media-releases/2021-09-15/acsc-annual-cyber-threat-report-released (date of access: 27.03.2025).

83. Cybercrime Law [Electronic resource] – Access mode: https://www.cybercrimelaw.net/EU.html (date of access: 29.03.2025).

84. Commission reached an agreement on the new international cybercrime convention [Electronic resource] – Access mode: https://home-affairs.ec.europa.eu/news/commission-reached-agreement-new-international-cybercrime-convention-2024-08-13_en (date of access: 01.04.2025).

85. European Cybercrime Centre [Electronic resource] – Access mode: https://en.wikipedia.org/wiki/European_Cybercrime_Centre (date of access: 05.04.2025).

86. New EU Agency to deal with the European cybercrime problems [Electronic resource] – Access mode: https://www.baltic-course.com/eng/baltic_states/?doc=68448 (date of access: 08.04.2025).

87. A Collective EU Response to Cybercrime: EUROPOL's European Cybercrime Centre [Electronic resource] – Access mode: https://ccdcoe.org/incyder-articles/a-collective-eu-response-to-cybercrime-europols-european-cybercrime-centre/ (date of access: 11.04.2025).

88. Virtual Currencies and Ransomware: Combating Criminal Use – The Law Enforcement Response [Electronic resource] – Access mode: https://idsf.io/wp-content/uploads/2022/06/Virtual-Currencies-and-Ransomware_Philipp-Amann.pdf (date of access: 15.04.2025).

89. Cybercrime. The biggest threat to individuals, companies and states alike - is there a way out or is everything lost? [Electronic resource] – Access mode: https://securitymadein.lu/cyber/topic-of-the-month/cybercrime/ (date of access: 17.04.2025).

90. Convention on Cybercrime [Electronic resource] – Access mode: https://en.wikipedia.org/wiki/Convention_on_Cybercrime (date of access: 19.04.2025).

Джилкишиев Р.Б.

91. Russian ITC Security Policy and Cybercrime [Electronic resource] – Access mode: https://www.ponarseurasia.org/russian-itc-security-policy-and-cybercrime/ (date of access: 22.04.2025).

92. Всестороннее исследование проблемы киберпреступности [Электронный ресурс] – Режим доступа: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 26.04.2025).

93. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях [Электронный ресурс] – Режим доступа: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_R.pdf (дата обращения: 27.04.2024).

94. Comparative analysis: the Budapest Convention vs the UN Convention Against Cybercrime [Electronic resource] – Access mode: https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime (date of access: 27.04.2025).

95. UN Cybercrime Convention: a troubling new treaty [Electronic resource] – Access mode: https://lens.civicus.org/un-cybercrime-convention-a-troubling-new-treaty/ (date of access: 31.04.2025).

96. China proposes UN treaty criminalizes ‘dissemination of false information’ [Electronic resource] – Access mode: https://therecord.media/china-proposes-un-treaty-criminalizing-dissemination-of-false-information (date of access: 02.05.2025).

97. From Budapest to Hanoi: Comparing the COE and UN Cybercrime Conventions [Electronic resource] – Access mode: https://www.lawfaremedia.org/article/from-budapest-to-hanoi--comparing-the-coe-and-un-cybercrime-conventions (date of access: 04.05.2025).

98. INTERPOLI-24/7 Global Police Communications System Training [Electronic resource] – Access mode: https://datastore.iatistandard.org/activity/US-GOV-15-P7013 (date of access: 07.05.2025).

99. INTERPOL Global Complex for Innovation LEED Energy Modelling [Electronic resource] – Access mode: https://www.iesve.com/services/projects/2386/interpol-singapor (date of access: 09.05.2025).

100. INTERPOL agreement with Cellebrite strengthens efforts in combating cybercrime [Electronic resource] – Access mode: https://cellebrite.com/en/interpol-agreement-with-cellebrite-strengthens-efforts-in-combating-cybercrime/ (date of access: 13.05.2025).

101. INTERPOL Global Complex for Innovation – Welcome to the future of cybercrime fighting [Electronic resource] – Access mode: https://www.kaspersky.com/blog/interpol-global-complex-for-innovation-welcome-to-the-future-of-cybercrime-fighting/4157/ (date of access: 15.05.2025).

102. Inside Interpol's digital crime centre [Electronic resource] – Access mode: https://www.itnews.com.au/news/inside-interpols-digital-crime-centre-410768 (date of access: 17.05.2025).

Джилкишиев Р.Б.

103. Inside INTERPOL's New Cybercrime Innovation Center [Electronic resource] – Access mode: https://www.fastcompany.com/1814963/inside-interpols-new-cybercrime-innovation-center (date of access: 21.05.2025).

104. Guidelines For Digital Forensics First Responders [Electronic resource] – Access mode: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf#:~:text=,developed%20the%20INTERPOL (date of access: 23.05.2025).

105. Арсеньев В.Д. Вопросы общей теории судебных доказательств. - М.: Юрил.лит., 1964. – 179 с.

106. Хван В.А. Планирование расследования преступлений. - Алма-Ата: Казгосиздат, 1956. – 44 с.

107. Проект об утверждении Концепции развития цифровой экосистемы на 2022-2027 года («Киберщит-2»): Постановление Правительства Республики Казахстан от 28 июня 2022 года. [Электронный ресурс] – Режим доступа: https://www.gov.kz/memleket/entities/mdai/documents/details/320322?lang=ru (дата обращения: 30.05.2025).

108. Jilkishiyev R., Begaliyev Y. Problems of Investigation of Crimes in the Field of Information Technology. Pakistan Journal of Criminology Vol. 16, No. 03, July—September 2024. pp. 97-114.

109. Саруханян А.Р. Преступления против порядка управления: общая характеристика, вопросы квалификации: дисс…канд. юрид. наук. – Ставрополь, 2002. – 177 с.

110. Джакишев Е.Г. Проблемы совершенствования криминалистических приемов и средств борьбы с хищениями и иными корыстными преступлениями в сфере экономики: дисс. …докт. юрид. наук. - Алматы, 1994. – 39 с.

111. Гавло В.К. Воронин С.Э. Актуальные проблемы поисково-познавательной деятельности в суде: учебное пособие. – Барнаул: БЮИ МВД России, 2000. – 124 с.

112. Возгрин И.А. Введение в криминалистику: история, основы теории, библиография. – СПб.: Изд-во «Юридический центр Пресс», 2003. – 475 с.

113. Повезнюк Г.И. Концептуальные основы криминалистического установления личности. Автореф. дисс …докт, юрид. наук: 12.00.09. – Алматы, 2003 – 23 с.

114. Саматова Г.Б. Схемы по уголовному праву Республики Казахстан. Преступления против личности. Учебное пособие. – Алматы: Аркаим, 2003. – 88 с.

115. Исхаков К.Е. Проблемы преодоления противодействия расследованию путем использования тактических приемов: автореф. … канд. юрид. наук: 12.00.09. – Алматы, 2004. – 30 с.

116. Возгрин И.А. Криминалистическая методика расследования преступлений. – Минск: Выш. школа, 1983. – 215 с.

Джилкишиев Р.Б.

117. Нургалиев Б.Б. Тактические основы изобличения лиц, противодействующих расследованию преступлений путем дачи ложных показаний. Автореф. дисс. … канд.юрид.наук. 12.00.09. - Алматы, 2006. – 28 с.

118. Булатов С.Я., Мамутов А.М. Ответственность за преступления против личности по уголовному кодексу Казахской ССР. - Алма-Ата: КГУ, 1961. – 102 с.

119. Гинзбург А.Я. Криминалистические основы следственных действий (по Уголовно-процессуальному кодексу Республики Казахстан): учеб. пособие по криминалистике / под ред. А.Ф. Аубакирова. – Алматы: Данекер, 2002. – 306 с.

120. Барсуков В.С., Водолазский В.В. Современные технологии безопасности. - М.: «Нолидж», 2000. – 496 с.

121. Попов В.И., Бегалиев К.А. Теоретические вопросы осмотра места происшествия // Вопросы борьбы с преступностью. Вып.39 – Алма-Ата – С. 60 – 67.

122. Гинзбург А.Я., Когамов М.Ч. Основы тактики опроса граждан в оперативно-розыскной и уголовно-процессуальной деятельности по законодательству Республики Казахстан: Учебно-практическое пособие. – Астана: 2005. – 40 с.

123. Ахпанов А.Н., Хан А.Л. Преобразование первоначальной стадии уголовного процесса в Республике Казахстан: анализ новелл законодательства. Сборник матер. межд. круглого стола «Современные проблемы криминалистики», посвященного 60-летию Ким К.В. - Астана: ТОО «КазГЮУ Консалтинг», 2015. – 266 с.

124. Уголовное право Республики Казахстан. Особенная часть. Курс лекций. В двух книгах. Книга 2. Темы 9-17. Под общей редакцией д.ю.н., профессора академика АЕН РК Борчашвили И.Ш. – Алматы: Жеті жарғы, 2006. – 704 с.

125. Шмарион В.И. Ответственность за преступления против чести, достоинства личности по российскому уголовному законодательству. Автореф. дисс.канд. юрид. наук. 12.00.08. - Ростов-на-Дону. – 2001. – 29 с.

126. Россинская Е.Р. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем / Е.Р. Россинская, Г.П. Шамаев // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). – 2015. - Т.6, № 1. [Электронный ресурс] – Режим доступа: http://brj-bguep.ru/reader/article.aspx?id=19969 (дата обращения: 05.06.2025).

127. Низамов В.Ю. Производство следственных действий в условиях взаимодействия следователя и органа, осуществляющего оперативно-розыскную деятельность: учеб.-практ. пособие / В.Ю. Низамов, Д.А. Степаненко. - Иркутск: Изд-во БГУЭП, 2004. – 169 с.

128. Белкин Р.С. Курс советской криминалистики. – М.: Изд-во Акад. МВД СССР, 1979. Т. 3. – 409 с.

Джилкишиев Р.Б.

129. Булатов С.Я., Мамутов А.М. Ответственность за преступления против личности по уголовному кодексу Казахской ССР. Алма-Ата, 1961. – С. 100-101.

130. Рахметов С.М. Теоретические основы совершенствования системы мер борьбы с преступлениями против правосудия по уголовному законодательству Республики Казахстан. Автореф. дисс... докт. юрид. наук.: 12.00.08. - Астана, 2006. – 57 с.

131. Алексеев С.С. Социальная ценность права в советском обществе. – М.: Юрид.лит., 1971. – 223 с.

132. Ахпанов А.Н., Кусаинов Ш.К. Привлечение в качестве обвиняемого в уголовном судопроизводстве Республики Казахстан. – Караганда: КЮИ МВД Республики Казахстан, 2005. – 168 с.

133. Жуманиязов М.А. Сущность уголовной политики Республики Казахстан. Дисс... канд. юрид. наук.: 12.00.08. – М., 2006. – 218 с.

134. Бегалиев Е.Н. Актуальные вопросы уголовного судопроизводства и уголовно-процессуального законодательства // Вестник Уральского юридического института МВД России. – 2019. - №2. - С. 5-8.

135. Рудый Н.К. Уголовно-правовая охрана чести, достоинства и репутации: дисс... канд. юрид. наук.: 12.00.08. – М., 2002. – 177 с.

136. Иванов О.И. Общественное мнение и власть // Социально-политический журнал. - 1993. - №7. – С. 35-40.

137. Борчашвили И. Судебная экспертиза: обеспечивая установление истины». [Электронный ресурс] – Режим доступа: Zakon.kz (дата обращения: 25.06.2025).

138. Анисимов А.Л. Честь, достоинство, деловая репутация: гражданско-правовая защита. – М: Юристь, 1994. – 88 с.

139. Костюк М.Ф. Уголовно-правовые и криминологические проблемы борьбы с преступностью в исправительных учреждениях. Автореф. дисс... докт. юрид. наук: 21.00.08. - М., 2000. – 13 с.

140. Ной И.С. Охрана чести и достоинства личности в советском уголовном праве. - Саратов, 1959. – 125 с.

141. Нуркаева Т.Н. Личные (гражданские) права и свободы человека и их обеспечение уголовно-правовыми средствами (вопросы теории и практики): дисс... докт. юрид. наук: 12.00.08. – Уфа, 2003. – 323 с.

142. Рахметов С.М., Турецкий Н.Н. Преступление против личности: Учеб. пособие – Алматы: Жеті жарғы, 2004. – 176 с.

143. Трайнин А., Менынагин В., Вышинская З. Уголовный кодекс РСФСР: Комментарий / Под ред. и с предисл. пред. Верх. Суда И.Т. Голякова. 2-е изд. - М.: Юр. изд. НКЮ СССР, 1946. – 280 с.

Джилкишиев Р.Б.

ПРИЛОЖЕНИЯ

Приложение А

Акт внедрения

«УТВЕРЖДАЮ»
Декан факультета
«Компьютерные технологии и кибербезопасность» МУИТ, к.т.н.
_____Сейлова Н.А
«___»_____ 2025 г.

АКТ
о внедрении результатов диссертационного исследования Джилкишиева Руслана Булатовича по теме: "Расследование преступлений в сфере информационных технологий»

Комиссия в составе: декана факультета «Компьютерные технологии и кибербезопасность» МУИТ, к.т.н., ассоциированного профессора Сейловой Н.А. (председатель); заведующей кафедрой «Кибербезопасность», к.т.н., ассоциированного профессора Ескендировой Д.М.(член комиссии); профессора кафедры «Кибербезпасность», д.т.н. Бабенко Т.В. (член комиссии); сениор-лектора кафедры «Кибербезпасность», м.т.н. Онгенбаевой Ж.Ж. (член комиссии) составили настоящий акт о том, что научные результаты диссертационной работы Джилкишиева Руслана Булатовича «Организация технической настройки и интеграция системы распознования лиц в существующую инфраструктуру видеонаблюдения» и «Тестирование и оптимизация работы системы ИИ-распознования лиц» использованы и внедрены в практические и лабораторные занятия дисциплин образовательных программ «Аппаратные средства защиты информации» и «Компьютерная безопасность».

Председатель комиссии _____ **Сейлова Н.А.**

Члены комиси _____ **Ескендирова Д.М.**

_____ **Бабенко Т.В.**

_____ **Онгенбаева Ж.Ж.**

Джилкишиев Р.Б.

Джилкишиев Р.Б.

Приложение Б

Акт внедрения

«Утверждаю»
Главный коммерческий директор
ТОО «KT Cloud Lab»,
_____ Т.К. Исабеков
«__» _____ 2025 г.

АКТ
о внедрении результатов диссертационного исследования Джилкишиева Р.Б. по теме: «Расследования преступлений в сфере информационных технологий» в практическую деятельность.

Комиссия в составе: директора по обеспечению организации и поддержке услуг Акбауова Т.Т. (председатель); заместителя директора обеспечению организации и поддержке услуг Талипова М.Ж. (член комиссии) и начальника технической поддержки блока по инфокоммуникационным технологиям Данебаева Е.М. (член комиссии), составили настоящий Акт о том, что научные результаты диссертации Джилкишиева Руслана Булатовича использованы и внедрены в практическую деятельность нашей организации в следующих сферах:

- посредством взаимодействия операторов связи с органами путем обмена цифровой информации;
- в сфере исследования цифровой информации, находящейся на облачных ресурсах центра обработки данных.

Председатель комиссии _____ **Акбауов Т.Т.**

Члены комиссии _____ **Талипов М.Ж.**

_____ **Данебаев Е.М.**

Приложение В

Акт внедрения

Ғылыми-зерттеу жұмысының нәтижелерін енгізу
АКТІСІ

1. Ғылыми-зерттеу жұмысының атауы: «Расследование преступления в сфере информационных технологий».

2. Шығатын нәтиженің түрі: «Теоретические основы расследования информационных технологий в сфере киберпреступности» тақырыбындағы дәріс.

3. Жұмысты орындаушы(-лар): Джилкишиев Руслан Булатович.

4. Ғылыми зерттеуді орындау негізі: Қазақстан Республикасы ІІМ Алматы академиясының ғылыми зерттеулер мен тәжірибелік-құрастырушылық жұмыстар жоспары.

5. Ғылыми зерттеу нәтижелерін қабылдау туралы күні мен мәлімет: «Теоретические основы расследования информационных технологий в сфере киберпреступности» атты дәріс Қазақстан Республикасы ІІМ Алматы академиясына енгізу үшін 2025 жылдың «9» 04 қабылданғанын растайды.

6. ҒЗТКЖ-ні енгізу туралы мәлімет: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы докторантураның түлегі Р.Б. Джилкишиевтың «Теоретические основы расследования информационных технологий в сфере киберпреступности» атты дәріс Қазақстан Республикасы ІІМ Алматы академиясының қызметкерлеріне қосымша материал ретінде пайдалануға енгізілді.

7. Енгізудің тиімділігі туралы мәліметтер: жүргізілген ғылыми зерттеулердің нәтижелері тәжірибелік және оқу процесінде пайдаланылуы мүмкін.

Қазақстан Республикасы ІІМ
Мақан Есболатов атындағы
Алматы академиясы
бастығының орынбасары
полиция полковнигі **Е. Бимолданов**
«9» 04 2025 ж.

Джилкишиев Р.Б.