АЛМАТИНСКАЯ АКАДЕМИЯ МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН
имени МАКАНА ЕСБУЛАТОВА

«ТАКТИКА И МЕТОДИКА РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КРАЖ И МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ В СЕТИ ИНТЕРНЕТ»

Методическая рекомендация

Алматы 2023

АЛМАТИНСКАЯ АКАДЕМИЯ МВД
РЕСПУБЛИКИ КАЗАХСТАН
им. М. ЕСБУЛАТОВА

«ТАКТИКА И МЕТОДИКА РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КРАЖ И МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ В СЕТИ ИНТЕРНЕТ»

Методическая рекомендация

Алматы
2023 г

Обсуждено и одобрено на заседании научно-методического совета Алматинской академии МВД Республики Казахстан им. М. Есбулатова (протокол №13 от 21. 11.2023 г.).

Рецензенты:
Коржумбаева Т.М. – начальник кафедры административно-правовых дисциплин Алматинской академии МВД Республики Казахстан имени Макана Есбулатова, к.ю.н., ассоциированный профессор, полковник полиции
Шегебаева А. – старший научный сотрудник Центра исследования проблем уголовной политики и криминологии МНИИ Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор философии (PHD)

Тактика и методика раскрытия и расследования краж и мошенничеств, совершаемых в сети Интернет. Методические рекомендации. – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан им. М. Есбулатова, 2023. – 64 с.

Настоящая методическая рекомендация посвящена проблемам раскрытия и расследования краж и мошенничеств, совершенных в сети Интернет. Изучение данных материалов поможет при подготовке сотрудников ОВД и позволит последним своевременно принять необходимые меры по противодействию Интернет-мошенничеству.

Данная методическая рекомендация предназначена для сотрудников оперативных и следственных подразделений и других служб ОВД, а также для преподавателей, слушателей и курсантов учебных заведений МВД Республики Казахстан.

Введение

С развитием информационных технологий и широким распространением сети интернет современное общество столкнулось с новыми вызовами и угрозами, связанными с киберпреступностью. Киберпреступления, совершаемые в сети, представляют собой сложное и многогранное явление, требующее специализированных знаний и методик для их раскрытия и расследования. Этот вводный материал представляет обзор современных киберпреступлений и подходы к их расследованию, а также освещает важность адекватной борьбы с этими угрозами в цифровом мире.

Сегодня киберпреступники опережают события, используя новейшие технологии и методы для достижения своих целей, будь то финансовая выгода, кибершпионаж, нарушение частной жизни или даже угрозы национальной безопасности. Феномен киберпреступности разнообразен и обладает множеством проявлений, от фишинга и мошенничества с использованием банковских карт до распространения вредоносных программ и даже кибератак на критическую инфраструктуру.

Расследование киберпреступлений требует не только технических навыков, но и понимания психологии киберпреступников, структур организаций, стоящих за киберугрозами, и мировой кибербезопасной экосистемы. Это также связано с соблюдением законов и правил в области цифровой деятельности и защиты прав человека в онлайн-среде.

В настоящем веке кибербезопасность становится неотъемлемой частью жизни организаций и граждан, и эффективное раскрытие и расследование киберпреступлений является важным компонентом обеспечения безопасности и надежности онлайн-среды. В данном руководстве мы рассмотрим тактику и методику раскрытия и расследования краж и мошенничеств, совершаемых посредством сети

интернет, и предоставим практические рекомендации для борьбы с этими киберугрозами.

В следующих разделах данной методической рекомендации мы представим основные виды онлайн-преступлений, тактику и методику их раскрытия и расследования, а также рекомендации по профилактике и защите от киберпреступлений. Надеемся, что данное руководство поможет укрепить безопасность в сети Интернет и сделает нашу онлайн-среду более защищенной и надежной для всех ее пользователей.

1. Определение и классификация онлайн-преступлений

В этом разделе можно будет изучить различные виды онлайн – преступлений, их характеристики и критерии классификации. Это позволит специалистам и правоохранительным органам лучше понимать и различать эти виды преступлений при раскрытии и расследовании.

1.1. Типы онлайн – преступлений

Фишинг: Этот вид атаки включает в себя отправку поддельных электронных сообщений или создание фальшивых веб-сайтов, которые имитируют легитимные организации или сервисы. Целью фишинга является обман пользователя и заставление его предоставить конфиденциальные данные, такие как логины, пароли, номера кредитных карт и другие личные сведения.

Пример фишинга: Пользователь получает электронное письмо, в котором говорится, что его аккаунт в банке был заблокирован из-за подозрительной активности. Письмо содержит ссылку на фальшивый веб-сайт банка, где пользователь должен ввести свой логин и пароль. Злоумышленники получают доступ к этим данным и могут использовать их для доступа к банковскому счету.

Фарминг: Этот вид атаки направлен на изменение DNS-записей или взлом роутеров, чтобы перенаправить пользователей на фальшивые веб-сайты без их согласия. На этих фальшивых сайтах злоумышленники могут собирать чувствительные данные.

Пример фарминга: Атакующие изменяют DNS-записи роутера в общественном Wi-Fi-сетапе, чтобы перенаправить пользователей на фальшивый веб-сайт при попытке доступа к банковскому сайту. Пользователи могут вводить свои логины и пароли, которые сохраняются злоумышленниками.

Киберкражи: Киберпреступники могут воровать финансовые средства, личные данные или ценную информацию, используя различные методы, включая вредоносные программы (малварь), взлом учетных записей и

сетевые атаки. Это может включать в себя кражи с банковских счетов, а также кражи интеллектуальной собственности.

Пример киберкражи: Киберпреступник использует вредоносную программу, чтобы получить доступ к базе данных онлайн-магазина и украсть информацию о кредитных картах клиентов. Затем он продает эту информацию на черном рынке.

Кибервороvство: Этот вид преступлений может включать в себя кражу цифровых активов, таких как криптовалюты, драгоценные металлы и другие ценности, которые хранятся в электронной форме.

Пример кибервороvства: Злоумышленники взламывают криптокошельки пользователей и крадут их криптовалютные сбережения.

Социальная инженерия: Суть этой атаки заключается в манипуляции психологическими факторами для обмана пользователей и получения доступа к их конфиденциальной информации. Злоумышленники могут использовать манипулятивные методы, например, представляться доверенными лицами или убеждать пользователей предоставить информацию добровольно.

Пример социальной инженерии: Злоумышленник, выдающий себя за сотрудника технической поддержки, звонит на рабочий номер сотрудника и убеждает его предоставить свой пароль для «технической проверки». Сотрудник, не подозревая мошенничество, сообщает пароль.

Мошенничество с банковскими картами: Киберпреступники могут использовать украденные данные банковских карт для совершения незаконных транзакций, включая снятие денег с банковских счетов и покупку товаров или услуг.

Пример мошенничества с банковской картой: Злоумышленник получает доступ к данным банковской карты, крадя информацию о карте с помощью вредоносного программного обеспечения на банкомате. Затем он снимает

деньги с банковского счета жертвы или делает покупки в Интернете.

Другие виды онлайн-преступлений:

Распространение вредоносных программ: Злоумышленники могут распространять вирусы, черви и троянские программы для заражения компьютеров и сбора информации.

Пример распространения вредоносных программ: Злоумышленники отправляют жертвам вредоносные вложения в электронных письмах. Если жертва открывает вложение, вирус инфицирует ее компьютер, позволяя злоумышленникам получить удаленный доступ к системе.

DDoS-атаки (атаки на отказ в обслуживании): Атаки, направленные на перегрузку целевых серверов трафиком, что приводит к временной недоступности веб-сайтов и онлайн-сервисов.

Пример DDoS-атаки: Киберпреступники координированно направляют большой объем запросов на веб-сайт или сервер, перегружая его и делая недоступным для обычных пользователей.

Социальные атаки: Эти атаки могут включать в себя клевету, хакерские группы, а также моббинг и кибербуллинг в социальных сетях.

Пример социальных атак: Злоумышленники могут использовать фальшивые профили в социальных сетях для клеветы, диффамации, распространения ложной информации и других форм манипуляции общественным мнением.

В понимании каждого из этих типов онлайн-преступлений и их характеристик заключается ключ к успешному раскрытию и расследованию. Эти примеры иллюстрируют разнообразие методов и тактик, используемых злоумышленниками в сети Интернет для совершения преступлений. Эффективное раскрытие и расследование таких атак требует глубокого понимания и подготовки специалистов, что будут рассмотрены в следующих разделах методической рекомендации.

1.2. Критерии классификации онлайн-преступлений

1.2.1. Масштабы ущерба

Масштабы ущерба оцениваются в зависимости от экономических и социальных последствий преступления.

Мелкие преступления: включают в себя относительно небольшие киберпреступления, которые могут привести к ограниченным финансовым потерям, например, мошенничество с одним банковским счетом или фишинг, нацеленный на нескольких пользователей.

Пример мелкого преступления: Злоумышленник отправляет фишинговое электронное письмо, которое обманывает одного пользователя и приводит к утере его аккаунта в онлайн-игре. Ущерб составляет несколько десятков долларов.

Крупные преступления: Включают в себя более серьезные атаки, которые могут иметь глобальные экономические последствия, такие как кибератаки на крупные банки или кражи данных из крупных корпораций.

Пример крупного преступления: Группа хакеров проводит атаку на крупный банк, крадет данные более чем 100 000 клиентов и устанавливает вымогательское программное обеспечение на серверы банка, требуя миллионы долларов в выкупе.

1.2.2. Методы атаки

Методы атаки описывают технические способы, используемые злоумышленниками при совершении преступлений.

Вредоносное программное обеспечение (малварь): включает в себя вирусы, черви и троянские программы, которые могут заразить компьютеры и мобильные устройства жертв.

Пример вредоносного программного обеспечения (малвари): Злоумышленник отправляет электронное письмо с вложением, которое содержит вредоносный файл. При

открытии файла, вирус заражает компьютер пользователя и шифрует его файлы, требуя выкуп в криптовалюте для их разблокировки.

Социальная инженерия: использует манипуляции и обман, чтобы убедить пользователей предоставить конфиденциальные данные или выполнить нежелательные действия.

Пример социальной инженерии: Атакующий звонит сотруднику компании, выдающему себя за сотрудника технической поддержки, и убеждает его предоставить пароль для доступа к корпоративной сети.

Взлом и воровство данных: Злоумышленники могут взламывать базы данных, сетевые системы или аккаунты пользователей, чтобы получить доступ к чувствительной информации.

1.2.3. Цели атаки

Цели атаки могут варьироваться от финансовой выгоды до идеологических или политических мотивов.

Финансовые выгоды: киберпреступники могут атаковать с целью получения прибыли, например, путем кражи денег, продажи украденных данных или вымогательства выкупа.

Пример финансовых выгод: киберпреступники взламывают базу данных онлайн-магазина и крадут данные кредитных карт клиентов для последующей продажи на черном рынке.

Политические или идеологические мотивы: группы хакеров могут атаковать организации или государственные учреждения, чтобы выразить свои политические или идеологические убеждения.

Пример политических мотивов: Группа хакеров атакует веб-сайт государственного агентства в знак протеста против действий правительства.

1.2.4. Типы жертв

Типы жертв варьируются от отдельных пользователей до крупных организаций и государственных структур.

Индивидуальные пользователи: Киберпреступники могут нацеливаться на отдельных пользователей, взламывая их социальные сети, электронные почты или банковские аккаунты.

Пример индивидуальных пользователей: Злоумышленник взламывает аккаунт социальной сети одного пользователя, чтобы получить доступ к его личным фотографиям и сообщениям.

Коммерческие организации: Преступники могут атаковать компании, чтобы получить доступ к конфиденциальным данным, интеллектуальной собственности или провести вымогательство.

Пример коммерческих организаций: Киберпреступники нападают на малый бизнес, крадя финансовые данные и клиентскую базу данных.

Государственные учреждения: Нападения на государственные структуры могут иметь серьезные политические и безопасностные последствия.

Пример государственных учреждений: Государственный веб-сайт становится целью массовой DDoS-атаки, что приводит к временной недоступности онлайн-государственных услуг.

Понимание этих критериев классификации помогает определить характер и масштаб угрозы, а также выбрать соответствующие методы и тактику для эффективной борьбы с онлайн-преступлениями. Это является ключевым элементом в раскрытии и расследовании киберпреступлений.

2. Тактика и методика раскрытия и расследования онлайн-преступлений

В данном разделе можно исследовать эффективные тактики и методики, которые можно использовать при раскрытии и расследовании онлайн-преступлений. Это включает в себя широкий спектр действий, начиная от сбора информации о преступлении до судебного преследования преступника. Важно помнить, что успешное расследование требует сотрудничества и координации между правоохранительными органами, специалистами по кибербезопасности и другими заинтересованными сторонами.

2.1. Сбор информации и первичная оценка

Собрать данные о преступлении: Первый шаг – собрать все доступные данные о преступлении. Это включает в себя информацию о времени и месте совершения атаки, методах, использованных злоумышленниками, и виде ущерба, который был нанесен жертве.

Оценить уровень угрозы: Оцените степень угрозы, которую представляет данное преступление. Это поможет определить, насколько срочными являются действия по расследованию и раскрытию.

2.2. Обеспечение цифровой безопасности

Защита улик: Важно предпринимать меры для защиты цифровых улик, таких как веб-серверные журналы, данные о сетевом трафике и киберследы. Это поможет сохранить доказательства для дальнейшего расследования и судебного процесса.

Обеспечение целостности данных: Следует обеспечить целостность данных, чтобы предотвратить изменение, повреждение или уничтожение доказательств. Использование хэширования и защищенных хранилищ может помочь в этом процессе.

2.3. Идентификация и анализ

Идентификация преступника: Попробуйте определить, кто стоит за преступлением. Это может включать в себя трассировку IP-адресов, анализ использованных учетных записей и методов атаки.

Анализ методов атаки: Изучите методы, использованные при совершении атаки, чтобы лучше понять технические характеристики и схемы действия злоумышленника.

2.4. Сотрудничество и координация

Сотрудничество с другими службами: Сотрудничество с киберполицией, информационными службами, международными правоохранительными органами и частными компаниями по кибербезопасности может быть критически важным для успешного расследования.

Координация действий: Обеспечьте эффективную координацию между всеми вовлеченными сторонами, чтобы избежать дублирования усилий и обеспечить эффективное использование ресурсов.

2.5. Заключительный отчет и подготовка к судебному процессу

Подготовка заключительного отчета: Составьте детальный отчет о расследовании, включая собранные доказательства, анализ методов атаки и информацию о подозреваемых.

Судебное преследование: Подготовьте материалы и свидетельства для судебного процесса. Сотрудничайте с юристами и прокурорами для обеспечения успешного судебного разбирательства.

Важно отметить, что эффективное раскрытие и расследование онлайн-преступлений требует постоянного обновления знаний и соблюдения законов и нормативных актов, связанных с кибербезопасностью и цифровым следствием. По мере развития технологий киберпреступники также совершенствуют свои методы, и правоохранительные

органы должны быть готовы к адаптации и борьбе с новыми угрозами.

2.6. Тактика и методика раскрытия и расследования краж и мошенничеств в сети интернет

2.6.1. Виды мошенничества, совершаемого с использованием информационных систем

В настоящее время мошенники оперативно реагируют на изменения в социально-экономической сфере жизни и «изобретают» новые виды и способы совершения мошенничества. Наиболее распространенными видами преступлений в сети Интернет, связанных с хищениями, являются:

Мошенничество в интернет-магазине

Для обмана мошенники пользователей часто используют онлайн-магазины:

а) просят внести предоплату и после получения денег исчезают. Связаться с ними невозможно;

б) поставляют вместо заказного подделку. Претензии предъявлять некому.

Интернет-попрошайничество. Лжеблаготворительность.

В различных сайтах и приложениях выкладываются объявления о помощи на лечение и оказании материальной помощи. Придуманные, красивые тексты, мошенниками могут тронуть любого человека. Данная схема подкупает наличием документов, подтверждающих факт болезни и отзывов знакомых. Однако, в результате тщательной проверки, оказаться, что человек на фото давно умер, или, что еще хуже, т.е. мошенники попросту подменили банковские реквизиты в самой форме просьбы о помощи.

«Фишинг» Фишинг–(англ. Phishinotfishing «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинами паролям [6].

Взлом аккаунтов в соцсетях «Кликджекинг» (англ. Clickjacking) – механизм обмана пользователей Интернета, при котором злоумышленник может получить доступ к

конфиденциальной информации или даже к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу. Возможны применения различных технологий – от подписки на ресурс в социальной сети до кражи конфиденциальной информации и совершения покупок в интернет-магазинах за чужой счёт.

Интернет-мошенничество на биржах Данный вид мошенничества распространен в среде пиринговых бирж, где участникам предоставляется возможность своим торговать цифровыми монетами между собой при использовании конкретной внешней электронной платежной системы или же банковских карт. Мошенники используют такие биржи с целью кражи средств с аккаунта платежной системы или банковской карты.

Неожиданный выигрыш в Интернете

Выигрыши и подарки без участия в чем-либо. На сотовый телефон приходит SMS-сообщение, либо на почту приходит электронное письмо с информацией о выигрыше приза, для получения которого необходимо перечислить деньги на Qiwi-кошелек.

Интернет-казино

Секреты рулетки – указанный вид мошенничества в интернете рассчитан на азартных людей, желающих выиграть в онлайн-казино. Убедительные сайты предлагают надежные методы выигрыша, однако в рулетке никакие виды математических схем не действуют.

Финансовые пирамиды в Интернете

Финансовые пирамиды–предлагают вложить деньги в успешную программу, привлечь других людей и за них получать дивиденды. Размеры дивидендов обещают совершенно нереальные.

Шесть кошельков – человек получает электронное письмо с предложением отправить на каждый из шести кошельков по одному доллару. Далее он должен создать такое же послание и распространить его в сети, где последним,

шестым номером будет вписан уже собственный номер электронного кошелька.

Интернет-мошенничество на сайтах знакомств и в социальных сетях

Брачная афера – все начинается с обычного знакомства по объявлению на каком-либо сайте или в социальной сети. Указанный вид мошенничества в Интернете отличается от других тем, что для «раскрутки» человека на деньги иногда требуется около 2-3 месяцев. Завоевав доверие, интернет-мошенник рассказывает о своих финансовых проблемах и просит помощи в их решении, но, после получения денег пропадает, связаться с ним больше не удается.

Заработок на обмене валют

Пользователям предлагается заработать деньги, используя для обмена валюты электронные обменные пункты. Мошенники просят открыть два счета в разных платежных системах и при помощи двух обменных пунктов поменять валюту, затем совершить обратный обмен. Один из обменных пунктов является поддельным и принадлежит мошенникам.

Мошенничество в сфере интернет-кредитования

При оформлении кредита от частных фирм и физических лиц, которые оказывают услуги только после предоплаты, обещают выдать кредит, а после получения денег (предоплаты) исчезают. Кроме того, некоторые интернет-сайты предлагают клиентам оставить заявку, заполнить анкеты с личными данными на оформление кредита либо кредитной карты. Однако мошенники могут воспользоваться информацией клиента.

Фальшивые криптовалюты – не зарегистрированные блокчейны, путем обмана убеждают пользователей и участников о покупке успешной и перспективной криптовалюты с предложением перевести деньги на другие Qiwi-кошельки.

Мошенничество при помощи SMS

«Нигерийские письма» – вид киберпреступности, который получил наибольшее развитие с появлением

рассылок по электронной почте. Письма появились в Нигерии и распространялись по почте в бумажной форме. Мошенники, как правило, просят у получателя письма помощи в многомиллионных денежных операциях, обещая крупную сумму от процентов.

Интернет-мошенничество на фрилансе

Мошенники создают клоны успешных фрилансовых аккаунтов на других биржах и действуют от их имени, принимая предоплату от заказчиков. Портфолио и вся личная информация, естественно, воруется.

В случаях, когда указанные деяния сопряжены с неправомерным доступом в информационную систему или сеть телекоммуникаций, содеянное подлежит квалификации по совокупности уголовных правонарушений по ст.ст. 190 и 205 УК РК, если в результате неправомерного доступа к компьютерной информации произошло уничтожение и модификация, нарушение работы ЭВМ, системы ЭВМ или их сети.

Кибersквоттинг

Кибersквоттинг (от англ. cybersquatting) – это способ заработка денег, который основан на анализе новостей рынка с целью выявления названий компаний и брендов новых товаров, для которых еще не зарегистрированы одноименные доменные имена. Обнаружив такой бренд, кибersквоттер регистрирует доменное имя на себя в надежде перепродать его впоследствии компании, владеющей соответствующим брендом.

Кибersквоттеры – это люди, которые регистрируют домен с целью их перепродажи.

Согласно законодательству кибersквоттинг не законен, так как зарегистрированный товарный знак или бренд имеет приоритет над доменным именем, и у владельца товарного знака есть законные основания для судебного иска.

2.6.2. Сбор и анализ финансовых данных

– Сбор данных о преступлении:

Информация о жертвах и потерпевших: Начните собирать информацию о жертвах и потерпевших. Это может включать в себя их контактные данные, место жительства, место работы, а также детали о том, как они стали жертвами мошенничества или кражи.

Хронология событий: Создайте хронологию событий, включая даты, времена и места, связанные с преступлением. Это поможет лучше понять ход событий и их последовательность.

Описание преступления: Получите подробное описание того, как произошло мошенничество или кража. Соберите информацию о методах, используемых злоумышленниками, и способах, которыми они получили доступ к данным или средствам жертв.

– Сбор электронных следов:

IP-адреса и логи серверов: Попытайтесь получить доступ к IP-адресам, связанным с мошенничеством или кражей. Это может включать в себя запросы логов серверов, которые могут содержать информацию о действиях злоумышленников.

Электронная переписка: Если мошенничество или кража связаны с электронной перепиской (например, фишинговые письма), соберите копии электронных сообщений и анализируйте их на наличие подозрительных элементов.

Банковские транзакции: Получите информацию о банковских транзакциях, связанных с преступлением. Это может включать в себя банковские выписки и данные о переводах средств.

Организация досудебного производства по преступлениям, совершаемым в Интернете, обусловлена установлением лица, причастного к совершению уголовного правонарушения, и доказыванием его умысла на совершение соответствующего деяния.

В большинстве случаев решение по материалам уголовного дела принимается по факту события без наличия данных о лице, к нему причастном. По данной категории уголовных правонарушений установить причастное лицо возможно путем определения:

1. Установление IP-адреса, с которого был осуществлен удаленный доступ к сайту интернет-банка и последующее неправомерное списание средств со счета потерпевшего;

2. Получение движения денежных средств по банковскому счету потерпевшего с расшифровкой данных, куда были направлены списанные денежные средства и (или) как они были использованы.

3. Получение сведений от банка, на какой номер был заменен «доверительный номер», куда приходили СМС-коды для изменения условий доступа в интернет-банкинге.

Для установления лица, совершившего неправомерный доступ в информационную систему необходимо использовать все возможные законные средства.

4. Установить IP-адрес злоумышленника можно следующим образом:

– через сайт, на который зашел злоумышленник. При входе на сайт фикируется IP-адрес, время доступа (ЧЧ.ММ.СС), также указывается операционная система и интернет-браузер абонента;

– через почтовый сервер. При обмене электронными письмами, почтовый сервер фиксирует IP-адрес, откуда они были отправлены.

Имея вышеуказанные данные, сопоставив значение MAC-адреса и значение IP-адреса при помощи интернет-провайдеров возможно установить физический адрес подключения. Расшифровка этих значений имеется в биллинговом центре на сервере провайдера, что позволяет определить конкретный физический адрес подключения и абонента.

Более сложную ситуация представляет собой то, что при совершении правонарушения злоумышленник использовал

сеть Интернет в общественных местах, где имеется бесплатный wi-fi роутер. При этом мобильному устройству выделяется динамический IP-адрес, который использует множество устройств одновременно.

При совершении правонарушения злоумышленник может получить доступ в сеть Интернет через устройство при использовании SIM-карты. В этом случае дополнительно направляется запрос сотовому оператору о имеющимся данным, а именно IP-адрес, MAC-адрес, время доступа в виде ЧЧ.ММ.СС.В биллинговом центре, на серверах сотового оператора также сохраняется важные данные, которые позволяют установить, с какого абонентского номера осуществлялся выход в сеть Интернет.

Зная реальный IP-адрес, с которого был осуществлен удаленный доступ, можно определить круг лиц, которые могут быть причастны к совершенному интернет-мошенничеству. Этот способ эффективен, когда доступ осуществлялся через статический IP-адрес (предоставление статического IP-адреса – это услуга провайдера, как правило, дополнительная, которая оказывается за дополнительную плату). Вместе с тем, субъекты могут получать доступ в иных местах, где предоставляется общий доступ к сети Интернет через wi-fi роутер. В таком случае он будет осуществлен посредством мобильного устройства через динамический IP-адрес, и в этом основной недостаток рассматриваемого способа установления преступника. Также у провайдера может сохраниться информация о телефонном номере абонента (MSISDN) [27], операционной системе и браузере соответствующего мобильного устройства. Зная MSISDN, можно получить данные от оператора сотовой связи об индивидуальном номере абонента (IMSI) [28], или об идентификаторе абонента (MSIN) [29], если в устройстве использовалась SIM-карта, а также данные о международном идентификаторе мобильного оборудования (IMEI) [30], которым в интересующий период был предоставлен динамический IP-адрес. Если же использовалось иное

мобильное устройство, позволяющее совершать доступ в сеть Интернет без SIM-карты, то от провайдера можно затребовать сведения о MAC-адресе сетевой карты устройства и о международном идентификаторе мобильного оборудования (IMEI). Если в дальнейшем будет установлено лицо, у которого будет изъято мобильное устройство с соответствующим IMEI и SIM-карта с соответствующими MSISDN и IMSI (MSIN), а также мобильное устройство с соответствующим MAC-адресом сетевой карты, то данные предметы могут являться косвенными доказательствами его виновности.

При этом могут возникнуть следующие сложности:

– SIM-карта может быть не зарегистрирована на конкретное лицо;

– SIM-карта может быть выброшена или уничтожена субъектом, использовавшим ее для доступа в сеть Интернет;

– мобильное устройство может быть продано после совершения деяний.

Установление данных о том, куда были направлены списанные средства и (или) как использованы.

Средства могут направляться на банковские счета и счета «электронных кошельков» платежных систем на территории как Республики Казахстан, так и иных государств. Если деньги будут переведены на счет (банковский, «электронного кошелька») на территории Казахстана и в дальнейшем обналичены, то необходимо проводить следственные и оперативно-розыскные мероприятия в отношении лица, обналичившего средства, так как он будет причастен к совершенному преступлению. Если же средства переведены на счет в другое иностранное государство, а также в случае наличия данных о неправомерном доступе с территории другого иностранного государства, то возникает необходимость в направлении запроса по каналам Интерпола в правоохранительные органы иностранных государств – членов Интерпола о преступлении в области высоких технологий, носящем международный характер.

Необходимо учитывать, что по рассматриваемым видам преступлений наибольшая эффективность достигается при комплексном рассмотрении специфических аспектов доказывания, обусловленных характером компьютерной информации.

– Анализ данных:

Анализ финансовых следов: Если преступление связано с финансовыми потерями, проведите анализ финансовых данных, чтобы выявить маршрут денежных средств, местоположение счетов и иные финансовые следы.

Идентификация схемы преступления: Попытайтесь определить схему, используемую злоумышленниками. Это может включать в себя идентификацию точек уязвимости или методов атаки, которые были использованы.

Анализ метаданных: Проведите анализ метаданных, чтобы выявить связи между различными данными и событиями. Метаданные могут также помочь определить источник информации и маршрут передачи данных.

– Сбор улик:

Сбор физических улик: Если возможно, соберите физические улики, такие как устройства, использованные злоумышленниками (например, фишинговые устройства или камеры наблюдения).

Сохранение цифровых следов: Обеспечьте сохранность цифровых следов, чтобы они могли быть использованы как доказательства в суде. Это включает в себя создание резервных копий и обеспечение целостности данных.

***5.* Сотрудничество и координация:**

Сотрудничество с киберполицией и другими службами: Сотрудничайте с киберполицией и другими службами правопорядка для обмена информацией и совместного расследования.

Координация действий: Обеспечьте эффективную координацию между всеми вовлеченными сторонами, чтобы избежать дублирования усилий и обеспечить эффективное использование ресурсов.

Сбор и анализ данных – это ключевой этап в расследовании интернет-мошенничества и краж. Надежная исходная информация и детальный анализ позволяют выявить следы злоумышленников, определить схему преступления и собрать улики, которые могут быть использованы в судебном процессе.

При проведении анализа действующего национального законодательства, республиканских программ, регламентирующих вопросы противодействия интернет-мошенничеству, были изучены нормативно-правовые акты, законы, указы, постановления, программы и международно-правовые акты.

Судебно-следственную практику по делам о мошенничестве определяют нормативные постановления Верховного Суда Республики Казахстан. Нормативное постановление Верховного Суда РК от 11 июля 2003 года №8 «О судебной практике по делам о хищениях» и нормативное постановление Верховного Суда РК «О судебной практике по делам о мошенничестве» от 29 июня 2017 года. В последнем мошенничество разделено по блокам, группам, способам совершения мошенничества, даны разъяснения по рассмотрению уголовных дел некоторых способов совершения мошенничества.

В противодействии любого вида преступлений решающее значение имеет их своевременная профилактика. Так, согласно п. 4 ст. 1 Закона Республики Казахстан «О профилактике правонарушений» от 29 апреля 2010 года, под профилактикой правонарушений понимается комплекс правовых, экономических, социальных и организационных мер, осуществляемых субъектами профилактики правонарушений, направленных на сохранение и укрепление правопорядка путем выявления, изучения, устранения причин и условий, способствующих совершению правонарушений.

В Республике Казахстан основные направления профилактики преступности определяются в рамках государственных программ по профилактике

правонарушений и борьбе с преступностью: – 17 ноября 2020 года приказом Министра внутренних дел от №787 утверждена Программа МВД Республики Казахстан по защите имущества на 2021-2023 годы; – 18 марта 2016 года утвержден Межведомственный план МВД, ГП, КНБ, МЗиСР, МСХ, МНЭ по профилактике краж чужого имущества на 2016-2017 годы.

Министерством информации и коммуникаций Республики Казахстан разработана Государственная программа «Информационный Казахстан-2020», утвержденная Указом Президента РК 8 января 2013 года №464.

В 2016 году при Министерстве оборонной и аэрокосмической промышленности создана межведомственная рабочая группа по разработке Концепции кибербезопасности «Киберщит Казахстана» на 2017-2020 годы.

В целях реализации Указа Президента Республики Казахстан от 15 февраля 2017 г. №422 «О мерах по реализации Послания Главы государства народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность» принята Концепция «Киберщит», утвержденная Постановлением Правительства РК от 30 июня 2017 года №30.

В План мероприятий по реализации Концепции включено предложение МВД о проработке вопроса о получении доступа к сведениям о соединениях казахстанских пользователей зарубежных социальных сетей и мессенджеров. Данная мера предполагает размещение их серверов на территории Республики Казахстан либо заключение договоров с казахстанскими операторами связи. Кроме того, предусмотрены мероприятия по обучению, повышению квалификации специалистов по кибербезопасности и исследованию цифровых доказательств. В состав рабочей группы Министерства национальной экономики по развитию электронной торговли включены сотрудники Управления «К» Департамента криминальной

полиции. Соответствующие предложения касательно деятельности интернет-магазинов, мер по предотвращению совершения мошенничества направлены в МНЭ. На постоянной основе осуществляется взаимодействие с КНБ по вопросам противодействия киберпреступлениям. В целях обеспечения оперативности получения сведений о соединениях казахстанских пользователей по согласованию с КНБ получен канал по проверке принадлежности IP-адресов отечественных интернет-провайдеров (в т.ч. операторов сотовой связи).

Осуществляется тесное взаимодействие с банками второго уровня (службы безопасности) по оперативному обмену информацией в целях своевременного реагирования на электронные хищения.

2.6.3. Идентификация и отслеживание подозреваемых

Для проведения анализа личности интернет-мошенника необходимо рассматривать вопрос личности с криминологической точки зрения, потому как именно в рамках криминологии учение о личности преступника получило наибольшее развитие.

Одной из характерных особенностей, присущих интернет-преступности, является преобладание преступников мужского пола. Несмотря на то, что среди пользователей Интернета соотношение женщин и мужчин примерно одинаково, последние проявляют более высокую криминальную активность. Преобладание лиц мужского пола среди интернет-преступников, как и в большинстве традиционных преступлений, объясняется исторически сложившимся более высоким уровнем социальной активности мужчин.

Анализируя данные по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан по половой принадлежности интернет-мошенников, следует отметить, что в последние годы, помимо

интенсивного роста интернет-мошенничеств, увеличилась и доля женщин. Так, если соотношение мужчина/женщина в 2016 году составляло 80,95% на 19,05%; в 2017 году 75,31% на 24,69%, в 2018 году 65,2% на 34,2%, то в 2019 году 57,37%, на 42,63% 2020 году 57,42%, на 42,58% соответственно. Это можно объяснить профессиональной ориентацией отдельных должностей и специальностей на автоматизированные компьютерные системы (кассир, секретарь, менеджер, экономист, контролер, бухгалтер и т.д.), которые чаще занимают женщины.

Анализируя возраст различных интернет-преступников, можно отметить, что подавляющее большинство преступленных посягательств совершается лицами в возрасте до 34 лет, причём пик приходится на период примерно с 18 до 25 лет.

Интернет-мошенники делятся на две основные категории:

1) лица, которые находились с потерпевшим в контакте (переписка, телефонные разговоры, предложения о работе, имеющие доступ к его личным данным).

2) лица, не имеющие связей с потерпевшим.

В первую группу входят сотрудники, которые имея свое служебное положение злоупотребляют им. К ним относятся операторы, программисты, инженеры, технический персонал, клерки, работники, обеспечивающие безопасность, сотрудники контролирующих структур, лица, решающие организационные вопросы. Аналогичные преступные действия могут осуществлять и бывшие сотрудники организаций, которые применяют информацию, полученную во время работы в целях совершения преступных деяний.

Во вторую группу входят лица, обладающие специальными познаниями в сфере современных компьютерных технологий, которые используют в корыстных целях.

Мошенничество в сети Интернет нередко совершают и сотрудники организаций, занимающие руководящие посты,

поскольку главным образом они являются высококвалифицированными специалистами, имеют достаточный уровень компьютерной подготовки и профессиональных знаний, навыков и умений. По роду деятельности руководители получают доступ к большому объему информации и могут давать указания своим подчиненным, однако не несут прямую ответственность за функционирование самой компьютерной системы.

В основе подозрения, как уголовно-процессуального явления, лежит информация, которой обладает следователь или дознаватель о причастности конкретного лица к расследуемому преступлению. При этом информация, из содержания которой следует вывод о совершении лицом преступления, может быть получена органом уголовного преследования как из оперативных, так и процессуальных источников.

Наличие информации, свидетельствующей о причастности лица к преступлению, во многом определяет характер деятельности органа расследования на этапе подозрения и его отношение к заподозренному лицу. В уголовно-процессуальной деятельности существует несколько ситуаций, объективно позволяющих органу уголовного преследования заподозрить лицо в совершении преступления.

Подводя итог по исследованию личности интернет-мошенника, мы пришли к следующим выводам:

1. При расследовании мошенничеств с использованием сети Интернет лицам, осуществляющим досудебное расследование необходимо использовать все допустимые и законные методы и средства для получения необходимой информации от подозреваемого лица для проведения полного и объективного расследование мошенничества.

2. По половому признаку для интернет-мошенников в Республике Казахстан преобладают лица мужского пола, они проявляют более высокую криминальную активность по сравнению с женским полом.

3.Характерной особенностью для интернет-мошенников является молодой возраст и совершение преступления впервые.

Отслеживание подозреваемых: Сотрудничество с провайдерами услуг и киберполицией может помочь в отслеживании подозреваемых до их реального местоположения.

Сотрудничество с провайдерами услуг: Обратитесь к интернет-провайдерам, хостинг-компаниям и онлайн-сервисам для получения информации о подозреваемых и запросите данные о трафике, логах и активности на их платформах.

Использование технических методов: Примените технические методы для отслеживания подозреваемых, такие как трассировка IP-адресов, анализ сетевого трафика и использование инструментов для выявления их местоположения.

Киберследы: При необходимости наймите специалистов по киберследствам, которые могут помочь в отслеживании подозреваемых и выявлении их источника и местонахождения.

Сотрудничество с правоохранительными органами и международными службами:

Сотрудничество с киберполицией: Взаимодействуйте с киберполицией и другими правоохранительными органами, специализирующимися на борьбе с интернет-преступностью. Предоставьте им доступ к информации и доказательствам, которые вы собрали.

Сотрудничество с международными службами: Если подозреваемые находятся за границей, сотрудничайте с международными правоохранительными службами и организациями для отслеживания их местоположения и передачи информации.

Осмотр физических мест:

Обыски и обследования: При наличии юридических разрешений и оснований, проводите обыски и обследования

физических мест, которые могли бы быть связаны с подозреваемыми. Это может включать в себя их дома, офисы и другие места.

Следственные действия: Проводите следственные действия для выявления физических улик, таких как компьютеры, документы, устройства хранения данных и другие материалы, связанные с преступлением.

Оперативные мероприятия:

Организация оперативных мероприятий: При необходимости, организуйте оперативные мероприятия для отслеживания и задержания подозреваемых силами правоохранительных органов.

Соблюдение законности: Всегда соблюдайте законы и правовые процедуры при проведении оперативных мероприятий и аресте подозреваемых.

Идентификация и отслеживание подозреваемых – сложный и многозвенный процесс, который требует сотрудничества с различными сторонами и специалистами. Важно при этом соблюдать законность и учитывать юридические аспекты весьма важны.

2.6.4. Процессуальные особенности расследования интернет-мошенничеств

Процесс расследования уголовных дел в отношении интернет-мошенничеств направлен на выявление и закрепление криминалистический значимой информации, подлежащей трансформации в качестве доказательств по делу.

Элементы, формирующие следственную ситуацию, тесно взаимосвязаны. Каждый из них частично содержит информацию о другом, что и позволяет выдвигать обоснованные версии и проводить целенаправленное расследование.

Между тем для разработки криминалистической методики расследования мошенничеств, совершенных в сфере информационных технологий, как и других

преступлений, существенное значение имеет установление типичных следственных ситуаций, выявление факторов, наиболее полно отражающих сущность данного преступления.

Рассматриваемые вопросы и соответствующие направления расследования преступлений в информационной сфере во многих случаях являются условными, поскольку зависят от индивидуальных особенностей ситуаций и случайных факторов, влияющих на возникновение следственной ситуации и процесс ее разрешения.

Исходя из этого, в данном разделе даны только самые общие рекомендации, которые должны адаптироваться к каждому уголовному делу о мошенничестве, совершаемому в сфере информационных технологий, согласно конкретной ситуации, сложившейся на начальном этапе расследования.

Начало досудебного расследования при совершении мошенничеств с использованием интернет-ресурсов, как правило, включает в себя семь этапов:

1) принятие (поступление) заявления (сообщения) о правонарушении;

2) первичная уголовно-правовая квалификация деяния и его регистрация в ЕРДР либо проведение первого по времени неотложного следственного действия (например, снятие информации, подтверждающей факт совершения мошенничества, с соответствующих сайтов Интернета);

3) определение подследственности преступления;

4) вынесение постановления о начале досудебного расследования и принятии его к своему производству;

5) дача поручения о проведении негласных следственных действий по установлению механизма мошеннических действий и способа реализации преступного умысла, источника перечисления денежных средств, потерпевшего и подозреваемого;

6) проверка по криминалистическим учетам наличия уголовных дел, расследуемых по аналогичным фактам, в

целях выяснения вероятности их соединения в одно производство;

7) обращение посредством СМИ к пользователям Интернета в целях выявления потерпевших от действий интернет-мошенников по выявленной преступной схеме.

После получения и закрепления информации, дающей основание подозревать конкретное лицо в совершении интернет-мошенничества и его допроса в качестве подозреваемого, задачи первоначального этапа досудебного расследования считаются выполненными.

Обстоятельства, подлежащие доказыванию на первоначальном этапе расследования по фактам интернет-мошенничеств Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Мошенничество путем обмана или злоупотребления доверием пользователя информационной системы – это те же действия, но совершенные с помощью Интернета. Данный вид мошенничества является относительно новым и в то же время распространенным и опасным видом преступления. Это связано, в первую очередь, с возможностью глобального (т.е. выходящего за границы отдельно взятого государства) использования компьютерных технологий, позволяющих скрыть действительный источник распространяемой информации и лица, получающего денежные средства потерпевших (например, путем использования интернет-кошелька).

К числу обстоятельств, подлежащих доказыванию по рассматриваемой категории уголовных дел, относятся:

–место, время, условия, способ совершения мошенничества;

–наличие преступного умысла, направленного на завладение чужим имуществом подобным способом;

–предмет мошенничества (что было присвоено: сумма денег и т.д.);

–характер и размер причиненного ущерба;

–в отношении кого совершено мошенничество (государственная или общественная организация, коммерческая структура, частное лицо);

–данные о личности преступника (сайт, анкетные данные, электронные адреса);

–данные о мошеннической преступной группе и иных лицах, участвовавших в ее действиях (состав, численность, техническая оснащенность, техническая специализация);

–данные о личности потерпевшего, обстоятельства контакта с мошенником [12]. Названные обстоятельства принято называть главным фактом, поскольку от доказанности или недоказанности этих обстоятельств напрямую зависит решение вопроса об уголовной ответственности – главного вопроса уголовного дела [13, с.136]. В первую очередь, следует установить, какое событие произошло. Видов и схем мошенничества в сети Интернет разнообразное количество [14, с.15]. Основные признаки мошенничества в Интернете – навязчивая реклама, обещающая огромный доход без вложения знаний и большого труда; требование ввода ваших персональных данных на сомнительных ресурсах; требование отправки SMS (которые в действительности являются платными), например, за скачивание необходимой литературы; заманчивые предложения, приходящие через почту от незнакомых людей (письма счастья) и т.д. Легкий заработок в Интернете, сайты с бесплатной музыкой, финансовые пирамиды, онлайн-казино, красотки с сайта знакомств, айфоны в полцены – почти всегда это мошенничество. Предложения под прикрытием официальных компаний или организаций с переводом денег на счета физических лиц. Наиболее известными способами совершения данного вида преступления являются фишинг, киберсквоттинг, тайпсквоттинг, мошенничество с помощью платежных систем (программного обеспечения), иные способы интернет-мошенничества. Способов совершения интернет-мошенничеств большое количество. Это связано в первую очередь, с существенным расширением спектра услуг,

предоставляемых в сфере информационных технологий. С помощью этих сведений можно выяснить, не совершены ли другие мошенничества аналогичным способом, и кто их мог совершить. Кроме того, установление способа интернет-мошенничества позволяет выдвинуть версии о лицах его совершивших, определить возможные места нахождения следов преступления. Предметом мошенничества в сети Интернет являются не наличные денежные средства, а виртуальные, то есть данные банковских карт, счетов, переводы денежных средств с помощью платежных систем. При получении денежных средств, ввиду отсутствия контакта между злоумышленником и жертвой, установить преступника в таком случае маловероятно. Под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман). В обоих случаях обманутая жертва сама передает свое имущество мошеннику. Характеризуя личность потерпевших, нужно иметь в виду, что нередко сами жертвы, движимые корыстными побуждениями и стремлениями обойти существующий порядок, действуют нечестным путем, в результате чего становятся жертвами мошенников. С другой стороны, жертвами мошенников оказываются люди простодушные, излишне доверчивые или неискушенные, которые поддались эмоциям и потеряли бдительность. Данные о преступнике по данной категории дел на первоначальном этапе получить очень сложно. Как правило, узнать мошенников можно по манере общения и интересу к личным данным, данным платежных карт. Все зависит от способа мошенничества. Мошенники – своего рода элита преступного мира, «талантливые артисты», находчивые и изворотливые, проворные в действиях, нешаблонно мыслящие. Они, так называемые «белые воротнички», образованы, не злоупотребляют спиртным и наркотиками, отличаются психологической устойчивостью, оптимизмом, конформизмом, самоконтролем, добротой и отзывчивостью [15]. Как правило, выделяют две категории

злоумышленников: – мошенники, не имеющие постоянного места жительства и работы, неоднократно судимые за мошенничество и другие преступления против собственности; – мошенники-рецидивисты, совершающие в основном мелкие мошенничества, чаще всего их жертвами становятся частные лица. В части 2 ст.113 УПК РК говорится о необходимости выявления обстоятельств, способствовавших совершению преступления. Хотя в данной норме говорится об установлении только этой группы обстоятельств, необходимо учесть, что доказыванию подлежат и причины преступлении [12]. В частности, необходимо выяснить причины возникновения у лица антиобщественных взглядов и привычек; причины, вызвавшие формирование умысла на совершение деяния или пренебрежительного отношения к интересам других лиц и общества в целом; обстоятельства, облегчившие реализацию антиобщественных установок лица, сделавшие возможным совершение данного преступления и т п. В случае рецидива необходимо установить его причины, а также обстоятельства, способствовавшие совершению лицом нового преступления. Типичные следственные ситуации на начальном этапе досудебного расследования по фактам интернет-мошенничеств

Расследование интернет-мошенничеств имеет ситуационный характер и представляет собой деятельность, направленную на решение конкретных задач, определяемых наличием обстоятельств, которые необходимо и возможно установить в конкретных условиях. Этот процесс находится под постоянным влиянием информации и полностью зависит от нее.

Типичные следственные ситуации играют важную роль в формировании методик расследования, позволяют разрабатывать направления по их разрешению, тем самым деятельность следователя становится целенаправленной. Типичные следственные ситуации формируются при изучении материалов следственной практики. Практика

расследования интернет-мошенничеств позволяет разделить следственные ситуации в зависимости от содержания исходной информации [16 с.271].

Первую группу составляют ситуации, когда исходная информация содержит данные о конкретном лице, которое совершило преступление:

1) выявленный факт совершения интернет-мошенничества, когда известны и установлены:

–способы совершения и сокрытия преступления;

–свидетели;

–материально фиксированные следы преступления;

–преступление совершено группой лиц, одно из которых задержано на месте преступления в момент или непосредственно после его совершения, остальные преступники скрылись с места происшествия или их местонахождение неизвестно;

–местонахождение похищенного имущества, денежных средств.

2) выявленный факт совершения интернет-мошенничества, когда известны и установлены:

–способы совершения и сокрытия преступления;

–свидетели;

–материально фиксированные следы преступления;

–личность преступника, но он скрылся с места совершения преступления;

3) выявленный факт совершения интернет-мошенничества, когда известны и установлены:

–способы совершения и сокрытия преступления;

–свидетели;

–материально фиксированные следы преступления;

–личность преступника (преступников), но его (их) действия завуалированы под видом законных финансовых и иных операций;

–местонахождение похищенного имущества, денежных средств или их части [17 с.36].

Для первой группы следственных ситуаций характерен следующий алгоритм следственных и негласных следственных действий (оперативно-розыскных мероприятий):

1) осмотр места происшествия с привлечением соответствующих специалистов (специалиста-криминалиста, специалиста по информационным технологиям и т.п.);

2) личные обыски задержанных, их рабочих мест и мест проживания;

3) контроль и запись телефонных переговоров, снятие информации с каналов связи, передающих электронную почтовую корреспонденцию, и иных сообщений;

4) допрос подозреваемых;

5) проверка подозреваемых по базам криминалистических учетов;

6) выемка:

–документов, характеризующих порядок и организацию работы на предприятии, в учреждении или в организации – месте обнаружения следов преступления;

–документов, отражающих работу субъекта с компьютерной информацией;

–документов, характеризующих операции, в процессе которых допущены нарушения и совершены преступные действия;

–мобильного устройства, с которого осуществляется доступ в сеть Интернет;

–log-файлов, содержащих сведения об IP-адресе, с которого произошел неправомерный доступ.

7) допрос лиц, причастных к соответствующим электронным операциям или подозреваемых в связях с лицами, совершившими преступные действия;

8) анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведение ревизии, документальной или иной проверки, в частности повторной (за какой период и с участием каких специалистов они проводились).

Вторую группу составляют ситуации, когда исходная информация не содержит данных о конкретном лице, которое совершило преступление, известен лишь факт совершения преступления.

В этом случае процесс расследования усложняется дефицитом информации о личности преступника и событии преступления; необходимостью одновременной проверки многих следственных версий и проведением значительного количества оперативно-розыскных мероприятий и следственных действий по установлению неизвестных обстоятельств.

Примерами таких ситуаций могут быть следующие:

1) выявленный факт совершения интернет-мошенничества когда:

–отсутствует информация о личности правонарушителя;

–не установлены свидетели;

–отсутствует информация о способе совершения преступления;

–не обнаружены материально фиксированные следы;

–не установлено местонахождение похищенного имущества.

2) выявленный факт совершения интернет-мошенничества когда:

–имеются данные о способе совершения преступления;

–установлены свидетели;

–отсутствуют сведения о личности преступника;

–отсутствуют материально фиксированные следы совершения преступления

Изучение уголовных дел данной категории показало, что с учетом анализа и оценки приведенных выше типичных ситуаций выдвигаются различные версии, строятся возможные гипотезы расследуемого события, основанные на конкретных материалах дела.

Для второй группы следственных ситуаций обычно планируют и осуществляют следующие первоначальные

следственные действия, оперативно-розыскные и организационные мероприятия:

1) допрос заявителя и лиц, на которых указано в исходной информации как на возможных свидетелей;

2) осмотр места происшествия с привлечением соответствующих специалистов (специалиста-криминалиста, специалиста по информационным технологиям);

3) выемка и дальнейший осмотр средств компьютерной техники, предметов, материалов и документов (в частности тех, которые находятся в электронной форме на электронных носителях), характеризующих электронные операции, в ходе которых по имеющимся данным совершены преступные действия;

4) назначение судебной компьютерно-технической и других экспертиз;

5) решение вопроса о возможности установления личности преступников и их задержания на месте преступления, необходимые в связи с этим меры;

6) проведение негласных следственных действий с целью выявления лиц, виновных в совершении преступлений, а также следов и других вещественных доказательств;

7) допросы свидетелей (очевидцев), установленных во время проведения расследования;

8) допросы подозреваемых (свидетелей), ответственных за проведение операций, связанных с электронными расчетами;

9) обыски на рабочих местах и по месту жительства подозреваемых.

Дальнейшие действия следователь должен планировать с учетом информации, полученной в процессе проведения вышеуказанных следственных действий.

Если полученная в ходе расследования информация считается достаточной для вынесения постановления о признании подозреваемым и квалификации его деяний конкретному лицу, то начальный этап расследования признается оконченным, и расследование переходит к

последующему этапу – проведение последующих следственных действий и негласных следственных действий (оперативно-розыскных мероприятий).

При недостаточности информации возникает одна из промежуточных ситуаций, которая, как и начальная, является исходной для выдвижения версий, планирования расследования, проведения следственных действий и негласных следственных действий (оперативно-розыскных мероприятий).

Особенности производства отдельных следственных действий (обыска, выемки) и назначение судебных экспертиз при расследовании интернет-мошенничеств

Общие положения проведения обыска и выемки содержатся в ст. ст. 252, 253 и 254 Уголовно-процессуального кодекса Республики Казахстан. Так, согласно ст.252 УПК РК основанием производства обыска является наличие достаточных данных полагать, что указанные предметы или документы могут находиться в определенном помещении или ином месте либо у конкретного лица. В соответствии со ст. 254 УПК РК определённые предметы и документы, имеющие значение для уголовного дела, при необходимости могут быть изъяты.

Производство обыска и выемки при расследовании интернет-мошенничеств, связано с получением доказательств способа совершения преступления, совершенного с использованием компьютерной техники и телекоммуникационных сетей. Таким образом, главной целью производства обыска при расследовании мошенничества с использованием сети Интернет является обнаружение и изъятие электронных носителей, на которых осталась информация, касающаяся как самого мошенничества, так и лиц, совершивших это преступление (информация об их нахождении или перемещении), предметы, являющиеся результатом (продуктом) преступления (например, контрафактные компьютерные программы) и (или) документы, содержащие важную информацию для дела

(квитанции; блокнот с личными записями; документы о переводе, обналичивании денежных средств и т.д.)) [18].

По делам об интернет-мошенничестве поисковые мероприятия при производстве обыска отличаются специфическими особенностями и делятся на две стадии обзорную и детальную.

На обзорной стадии следователю необходимо:

– осмотреть все помещение. В связи с тем, что искомый объект находится в форме электронной информации, в первую очередь нужно обратить внимание на компьютерную технику, находящуюся в помещении, на ее расположение, состояние (включена или выключена), а также на состояние телекоммуникационных сетей. При осмотре помещения следует произвести поиск портативных запоминающих устройств (флэш-карты, внешний жёсткий диск), а также замаскированных высокотехнологичных продуктов маленького размера, которые тоже могут являться носителями компьютерной информации (напр., кулон, часы, серьги) (см.рис.№1).

Рис.№1. (нож-флэш карта, часы-флэш карта, ручка-флэш карта).

– необходимо определить объединён ли компьютер в локальную сеть с другими компьютерами, а также подключён ли он к другим телекоммуникационным сетям;

– с помощью специалиста на осматриваемом компьютере (если он находится во включённом состоянии) необходимо: проверить наличие средств защиты информации, вирусных программ и удалённого доступа;

– при осмотре компьютера, ноутбука, планшета либо сотового телефона определить: какая операционная система установлена: какие были выполнены операции и какие использовались программы, начиная с включения (в случае, если он был включён). Изображение на экране необходимо снять на видео (либо с помощью «скриншота»), в случае необходимости, выполняемые программы остановить.

На детальной стадии обыска следователю необходимо:

– при осмотре работающего компьютера: с помощью специалиста, следует провести поиск компьютерной информации, имеющей значения для расследуемого преступления, в осматриваемом компьютере. Если информация, касающаяся расследуемого мошенничества с использованием сети Интернет, найдена, то необходимо определить, где именно она находится.

После проведения осмотра компьютера он по всем правилам выключается, упаковывается и изымается. При осмотре неработающего компьютера: зафиксировать его месторасположение, а также (если есть) его периферийных устройств; определить и зафиксировать соединения компьютера с телекоммуникационными сетями, периферийным оборудованием и иными устройствами;

– при обнаружении на месте обыска и выемки мобильного телефона, смартфона или планшетного компьютера для поиска в них нужной информации, относящейся к расследуемому преступлению, совместно со специалистом, можно применить мобильный комплекс по сбору и анализу цифровых данных. В случае, если нет возможности предварительно исследовать информацию в мобильном устройстве, следователь, по имеющимся у него сведениям, принимает решение о необходимости его изъятия. После производства обыска и выемки вся обнаруженная компьютерная техника, содержащая искомую информацию по расследуемому интернет-мошенничеству, перед изъятием должна быть правильно упакована и опечатана. По окончании обыска и выемки составляется протокол следственного действия и описи к нему [18].

Тактические приемы, используемые при проведении экспертиз

Производство судебной экспертизы регламентируется главой 35 УПК РК, а также Законом РК «О судебно-экспертной деятельности» 10 февраля 2017 года.

При назначении экспертизы следователь не должен допускать, с одной стороны, необоснованного промедления, а

с другой – неоправданной поспешности. Успех экспертного исследования во многом зависит от полноты и своевременности представления следователем необходимых объектов и образцов для проведения экспертизы, а также правильной постановки вопросов. Экспертиза назначается немедленно после того, как собраны все необходимые для исследования объекты [19].

Следователь, назначая экспертизу, определяет конкретные основания, предмет экспертизы, объекты и сведущее лицо (лицо, имеющее обширные познания в определенной сфере своей деятельности) или судебно-экспертное учреждение.

Подготовка материалов на экспертизу представляет собой комплекс процессуальных, тактических и технических мероприятий по собиранию и оформлению всех необходимых вещественных доказательств, документов, образцов, исходных сведений. *Подготовка включает:*

–принятие решения о необходимости назначить экспертизу;

–вынесение мотивированного постановления;

–подбор объектов, представляемых в распоряжение эксперта;

–выбор эксперта или экспертного учреждения;

–постановку вопросов, выносимых на разрешение;

–материалы уголовного дела.

В процессе расследования интернет-мошенничества, могут быть назначены следующие судебные экспертизы:

1) технико-криминалистическая экспертиза документов – для установления подлинности использованных документов, печатей, штампов;

2) почерковедческая экспертиза – для установления личности исполнителя рукописного текста и подписи на документе, выполненной путем подражания;

3) судебно-бухгалтерская экспертиза – для получения источника доказательств в ходе исследования хозяйственных операций;

4) фоноскопическая экспертиза – для исследования данных контроля и записи телефонных переговоров;

5) компьютерно-техническая экспертиза – для исследования компьютерных устройств, машинных магнитных носителей информации и программных продуктов.

Все большую актуальность в настоящее время для исследования документов по уголовным делам об интернет-мошенничестве приобретает назначение и проведение компьютерно-технических экспертиз. Это обусловлено тем, что документация готовится в основном с помощью компьютерной техники.

Экспертному исследованию подлежат предметы и документы, имеющие значение для расследования уголовного дела и изъятые в предусмотренном законом порядке в ходе осмотра, обыска, выемки, либо добровольно предоставленные лицами, заинтересованными в исходе уголовного дела.

Объектами исследования компьютерно-технических экспертиз по уголовным делам данной категории являются:

–компьютеры, их системы и сети;

–периферийные устройства: модемы, сканеры, принтеры и коммуникационные устройства, а также сопроводительные документы к ним; магнитные носители информации (жесткие и оптические диски, дискеты и т.п.);

–документы, изготовленные с использованием компьютерных систем и электронных средств передачи и копирования информации (факсы, ксерокопии и т.д.) и иные электронные технические средства.

В распоряжение экспертов также предоставляются:

– электронные документы (платежные документы и т.п.);

– изъятая техническая документация на компьютерные устройства;

– пароли доступа к компьютерной информации;

– протоколы осмотра компьютерной техники; изъятая компьютерная техника.

Задачами компьютерно-технической экспертизы является идентификация объекта, являющегося компьютерным средством, а также его диагностика, выявление и изучение следовой картины представленного устройства, получение доступа к компьютерной информации и ее всестороннее исследование.

На решение судебно-экспертного исследования средств компьютерной технологии выносятся следующие вопросы:

1) по аппаратным средствам:

– какая модель компьютера представлена на исследование, параметры периферийных устройств, каковы технические характеристики представленной компьютерной техники;

– исправна ли представленная компьютерная техника? Возможна ли ее эксплуатация? Если нет, то по каким причинам, возможно ли использование представленного технического комплекса для осуществления тех или иных функциональных задач (например, выхода в Интернет, запись компакт-дисков);

– соответствует ли представленная документация данным техническим устройствам и периферийному оборудованию;

– какие условия сборки компьютера и его комплектующих: фирменная сборка, сборка из комплектующих на другой фирме или кустарная (самодельная) сборка;

– имеют ли место неисправности отдельных устройств компьютера;

– не проводилась ли адаптация компьютера для работы специфических пользователей (левша, человек с дефектом зрения и т.д.);

– каковы ориентировочные даты создания вычислительного комплекса с заданными возможностями и даты изготовления его отдельных блоков.

2) по программным продуктам:

– какая операционная система установлена в представленном системном блоке;

– какие программные продукты эксплуатируются на данном компьютере, соответствует ли установленная в представленном системном блоке операционная система лицензионно выпущенной продукции, либо являются они лицензионными, или «пиратскими» копиями, или собственными оригинальными разработками, когда проводилась инсталляция (установка) данных программ;

–каково назначение программных продуктов;

–для решения, каких прикладных задач они предназначены;

–какие способы ввода и вывода информации используются, соответствуют ли результаты выполнения программ нужным действиям;

–какие программные методы защиты информации (пароли, идентификационные коды, программы защиты и т.д.) используются;

–имеется ли в представленном системном блоке, установленное программное обеспечение (указывается название);

–находится ли данное программное обеспечение в работоспособном состоянии;

–каковы дата и время установки программного обеспечения;

–были ли попытки подбора паролей или другие попытки незаконного вмешательства в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей;

– имеются ли в предоставленных системных блоках программы, приводящие к неправомерному доступу к охраняемой законом компьютерной информации, внесению изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ПК;

– каковы основные функции представленного программного обеспечения;

– какая информация содержится в скрытых файлах;

– каково назначение представленных программ для ПК;

– возможно ли осуществление заданного вида деятельности с использованием представленных технических средств и размещенного на нем информационного и специального программного обеспечения (запись компакт-дисков, подготовка и изготовление поддельных денежных знаков).

3) по информационным объектам:

– имеется ли на представленном магнитном диске или в составе технических средств вычислительной техники необходимое информационное обеспечение для решения какой-либо конкретной функциональной задачи;

– имеются ли на представленных магнитных носителях файлы с документами, относящимися к той или иной сфере деятельности (файлы с изображениями денежных знаков, бланками юридических лиц и оттисками печатей);

– имеются ли на представленных магнитных носителях ранее удаленные файлы (указываются названия), размеры и даты создания, давность уничтожения;

– возможно восстановление ранее удаленных файлов и каков их смысл;

– имеются ли на магнитном носителе какая-либо информация (указать вид ее представления);

– изменялось ли содержание файлов (указать, каких именно), если да, то в чем он оказался;

– какова дата и время создания файлов (указать названия);

– в каком виде хранится информация о результатах работы антивирусных программ, программ проверки контрольных сумм файлов, какой смысл данной информации.

2.6.5 Предупреждение интернет-мошенничества

Одной из задач правоохранительных органов является информационно-просветительская деятельность по максимально возможному доведению до широких слоев населения сведений об угрозе со стороны мошенников, действующих в сети Интернет. Меры профилактического характера могут заметно сузить поле для преступных посягательств и позволят выявлять многие из них на ранней стадии.

В настоящее время существует огромное количество различных видов мошенничества в сети Интернет. Однако с течением времени появляются все новые виды мошенничества. Наиболее часто пользователи сети Интернет подвергаются: а) мошенничеству:

–в сфере онлайн-покупки;

–с платежной картой;

–в сфере кредитования;

–в сфере онлайн-кредитования;

–во фрилансе;

б) хищению денежных средств с использованием телефонных звонков и SMS-уведомлений;

в) взлому персональных данных в Интернете.

Мошенничество в сфере онлайн-покупки

Поддельные интернет-магазины копируют online-площадки известных брендов. Риск лишиться денег и не получить покупку очень велик. Многие из них создаются для того, чтобы пользоваться доверием покупателей к узнаваемой торговой марке.

Схем обмана немного, каждую из них можно определить еще в процессе покупки. Самое неприятное, что ждет клиента – ситуация, когда, получив деньги, Интернет-магазин перестает отвечать на письма и звонки. Другие схемы менее очевидны и раскрываются только после того, как сделана покупка: выявляется некомплектность заказа, возникают дополнительные платежи, обнаруживается несоответствие

товара описанию на сайте, вам продают поддельный или некачественный товар и нарушены сроки доставки.

В целях избежание обмана со стороны мошенников при совершении онлайн-покупок необходимо:

– внимательно изучить реквизиты продавца и адресного стационарного офиса;

– знать, что полноценный Интернет-магазин должен быть на собственном «домене» [20];

– обратить внимание в поисковиках на рейтинг магазина;

– почитать на разных форумах отзывы о магазине;

– проверить срок деятельности организации;

– проверить качество и целостность доставленного товара перед оплатой;

– производить оплату после доставки заказного товара.

Мошенничество с платежной картой

С расширением сферы применения пластиковых карт увеличивается количество мошеннических действий в отношении их обладателей. Различные способы так называемого «взлома» пластиковых карт, в первую очередь банковских и платёжных карт, прогрессируют с каждым днём.

Этот вид мошенничества включает использование украденных или поддельных платежных карт для прямых покупок или снятия наличных, а также украденных данных карты для покупки товаров по телефону или через Интернет.

Для защиты банковской карты необходимо:

– всегда хранить карту в безопасном месте;

– номер из 16 цифр, имя и фамилию владельца, указанные на лицевой части карты, можно пересылать только проверенным людям;

– срок действия карты никому не сообщать и не пересылать;

– трехзначный код безопасности на обратной стороне карточки никому не сообщать;

– подключить SMS информирование обо всех операциях по карте (SMS-банкинг). Так можно оперативно реагировать на несанкционированный перевод денег с карты;

– периодически менять PIN-код (данная операция повышает защищенность банковской карты);

– закрывать свой PIN-код при совершении покупок в магазине или использовании банкомата;

– подписать любые новые карты;

– держать карту в поле зрения при оплате товаров или услуг;

– хранить свой PIN-код в безопасности;

– при оплате покупок в Интернете игнорировать требования ввести на

страницах сайта PIN-код карты;

– если ожидаете получение карты или PIN-кода в почтовом отправлении,

а оно не приходит, немедленно сообщить об этом «эмитенту» [21] карты;

– в случаи утери или кражи карты, немедленно сообщить в банк

Мошенничество в сфере кредитования

В последнее время возобновились случаи объявлений, SMS-рассылок или электронных писем с сообщением о возможности легкого и быстрого получения кредитов, а также приумножения сбережений. Мошенники, используя безысходность и доверчивость граждан, привлекают их доступными условиями получить финансовые средства, при этом настаивают на предоплате им за положительное разрешение вопроса о кредитовании. Кроме того, мошенничество в сфере кредитования обусловлено желанием людей за короткое время заработать путем вкладов и инвестирования в сомнительные проекты [22].

Сегодня существует огромное количество схем мошенничества с выманиванием денег у доверчивых людей. Схемы постоянно меняются, совершенствуются. Среди самых популярных можно выделить следующие:

1. Кредит одобрен, но заблокирован.

Мошенник предлагает помощь в получении кредита, при этом оговаривается сумма вознаграждения за эту помощь. По результатам «работы» клиенту приходит сообщение по мобильной связи «из банка», с формулировкой, что кредит одобрен. Однако, мошенник сообщает клиенту, что кредит заблокирован службой безопасности банка до тех пор, пока клиент не рассчитается за помощь в получении кредита.

2. Оплата страховки.

Мошенник сообщает клиенту, что кредит в банке согласован, но для его получения необходимо предварительно оплатить страховку.

3. Оценка кредитоспособности.

Мошенники предлагают оплатить клиенту оценку кредитоспособности для возможности получения кредита от частного инвестора.

4. Заключение договора о совместной деятельности.

Мошенник с клиентом заключает договор о совместной деятельности. По условиям договора клиент должен в определенные сроки вносить суммы предоплаты. После внесения предоплаты вторая сторона обязуется создать предприятие. Клиент вносит предоплаты, в результате ничего не получает [23].

В целях избежания обмана со стороны мошенников в сфере кредитования необходимо знать:

–кредиты не выдаются под меньший процент, чем банки принимают депозиты;

–если в действительности кредит одобрен, то никакой банковский сотрудник или служба безопасности не могут заблокировать его;

–предоплаты за кредит в виде страховок или других платежей не существует;

–у каждой организации, представляющей финансовые услуги, должна быть соответствующая лицензия, в которой прямо фигурируют слова «финансовые услуги»;

–договор в финансовых организациях всегда составляется в двух (иногда трех) экземплярах, один из которых предоставляется клиенту и должен храниться у него;

–у любой финансовой организации должен быть Устав, в котором четко описаны источники средств, выдаваемых в качестве кредитов клиентам;

–в договоре надо читать и анализировать все пункты и подпункты. Особенно те, которые напечатаны мелким шрифтом.

Мошенничество в сфере онлайн-кредитования

Быстрое кредитование пользуется повышенным спросом среди заемщиков, которым срочно требуется в долг небольшая сумма. Обычно заемщики в спешке могут допустить несколько грубых ошибок, повышающих кредитный риск. Оставляя свои данные на непроверенных сайтах, заемщик сталкивается с риском использования конфиденциальной информации злоумышленниками. Паспортные сведения могут применяться мошенниками для получения кредитов, а данные с платежными реквизитами позволяют опустошить счета заемщика путем самовольного списания средств.

В целях защиты от онлайн-кредитного мошенничества необходимо:

–привлекать к сотрудничеству только проверенные компании, работающие на рынке не менее одного года;

–оставлять персональные данные на защищенных сайтах, адрес которых начинается с «https://»;

–регулярно проводить мониторинг состояния счетов в целях контроля за выполнением платежных операций;

–хранить в тайне пароли от аккаунтов для систем Интернет-банкинга, а также CVC и PIN-коды карт.

Мошенничество во фрилансе

Фриланс – это механизм, суть которого заключается в том, что частное лицо или фирма нанимает для выполнения определенной задачи человека, не зачисляя его в штат фирмы. Работник может находиться в другом городе или даже в

другой стране, но может работать и в офисах заказчика. Широкое распространение «фриланс» получил с развитием Интернета: сеть и сопутствующие информационные и банковские технологии позволили некоторым категориям работников уменьшить частоту появления в офисах, а то и полностью перейти на удалённую работу [24].

Особенность работы в Интернете заключается в том, что при общении с потенциальным заказчиком мы не видим его вживую. Таким образом, все общение строится лишь на доверии, и нередко даже опытные специалисты могут остаться обманутыми недобросовестным работодателем.

Многие успешные «фрилансеры» работают только на какой-нибудь одной бирже. Мошенники же создают клоны их аккаунтов на других биржах и действуют от их имени, принимая предоплату от заказчиков.

Прежде чем переводить предоплату, необходимо собрать следующую информацию о фрилансере:

–найти его аккаунты на биржах и в социальных сетях;

–сравнить данные на бирже с данными из социальных сетей. Если на бирже указано, что фрилансер находится в Караганде, а в социальной сети нашли похожего пользователя из другого города – это повод задуматься;

–фотографии, контакты друзей и знакомых;

–отзывы пользователей;

–наличие сертификата.

Профессиональные фрилансеры оставляют в сети десятки следов – они общаются на профильных форумах, ведут блоги, пишут статьи. Если ничего не нашли об этом человеке, есть повод задуматься.

При переводе денег исполнителю необходимо указывать в назначении платежа, за что переводите деньги. При необходимости сможете использовать эти данные для доказательства, что переводили деньги за работу.

Хищение денежных средств с использованием телефонных звонков и SMS-уведомлений

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок. SMS-мошенничества – это мошенничество «вслепую». Сообщение рассылаются в большом объеме, в надежде на доверчивого получателя. Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом. Цель мошенников – заставить передать свои денежные средства «добровольно». Для этого используются различные схемы мошенничества. Изъятие денежных средств может проходить разными способами. Жертву попытаются заставить передать деньги из рук в руки или оставить в установленном месте, приобрести карты экспресс-оплаты или сообщить мошеннику код карты, перевести деньги на свой счет и ввести специальный код и перевести на указанный счет определенную сумму денег, объясняя это необходимостью «внести предоплату» или заплатить «страховой взнос» [25].

В целях защиты от хищения денежных средств с использованием телефонных звонков и SMS-уведомлений необходимо:

–не производить никаких действий по просьбам, полученным по телефону от посторонних лиц;

–не сообщать персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;

–проверять информацию, позвонив в контактный центр банка;

–не открывать вложенные файлы, не переходить по ссылкам;

–не переводить деньги на неизвестные расчетные счета и телефоны;

–не верить, если звонят с сообщением, что Ваши близкие попали в беду, и предлагают свою помощь за деньги;

–не подтверждать операции, которые не проводили;

–обращаться в правоохранительные органы.

Взлом персональных данных в Интернете

С приходом цифровой эры возможностей оставить что-либо конфиденциальным становится все меньше. Данные о наших повседневных действиях: общении с друзьями, поездках в отпуск и покупках – все это и многое другое записывается и хранится на серверах разных компаний и организаций. Данные хранятся на подключенных к Интернету серверах, их покупают, продают, используют разнообразными способами, а иногда и воруют [26].

Абсолютной защиты от сетевых угроз не существует, однако имеются надежные способы значительного снижения степени опасности. Прежде всего, следует использовать защищенное интернет-соединение, никогда и никому не сообщать свои конфиденциальные данные, не убедившись предварительно, что сайт безопасный и проверенный.

Также следует использовать специализированные программы (антивирус, антиспам, файервол).

Нельзя доверять незнакомым контактам (вложения в электронных письмах и сообщениях с незнакомых адресов (вирус вполне возможно «замаскировать» под невинный на первый взгляд документ), гиперссылки, призывающие посмотреть видеоролики или фото).

Для защиты персональных данных предлагается соблюдать следующие правила, которые помогут сохранить конфиденциальность:

–не указывать личную информацию в профиле социальных сетях;

–не хранить в электронной почте и не выкладывать в открытый доступ копию документов, удостоверяющих личность;

–не хранить на электронной почте и не выкладывать в открытый доступ онлайн - фотографии документов, билетов и платежных чеков;

–не пользоваться открытыми Wi-Fi точками;

–не оставлять незаблокированными сотовые телефоны и компьютеры;

–прежде чем вводить логин и пароль на сайте, необходимо убедиться, что в адресной строке браузера указан верный адрес;

–не открывать вложения и не переходить по ссылкам из электронной почты или мессенджеров сомнительных адресатов;

–закрыть страницу, если в браузере появится сообщение о переходе на подозрительный сайт;

–следить как мобильные приложения используют личные данные;

–никогда не повторять ввод одинаковых паролей на разных ресурсах;

–позвонить по официальному номеру банка или другой организации, от имени которой было отправлено подозрительное письмо;

–установить на свой ПК защитное программное обеспечение и следить за регулярностью обновлений антивирусных баз;

–создать два адреса электронной почты: частный (для переписки) и публичный

3. Профилактика и защита от онлайн-преступлений

Профилактика и защита от онлайн-преступлений играют ключевую роль в обеспечении безопасности в интернет-среде. В этом контексте важно не только расследовать и наказывать преступников, но и предотвращать возможные угрозы.

Кибергигиена и образование:

Обучение и информирование: Один из наиболее важных аспектов профилактики – это обучение и информирование пользователей о потенциальных угрозах. Проводите обучающие семинары, вебинары и курсы по кибербезопасности.

Сильные пароли: Обучайте людей создавать и использовать сложные и уникальные пароли для своих онлайн-аккаунтов. Советуйте им также регулярно менять пароли.

Антивирусное и антималварное программное обеспечение: Поощряйте использование антивирусных и антималварных программ и регулярно обновляйте их.

Социальная инженерия и фишинг:

Обучение узнаванию мошеннических попыток: Учите пользователей распознавать признаки социальной инженерии и фишинга, чтобы они не стали жертвами обмана.

Бдительность: Советуйте быть бдительными при получении подозрительных сообщений или запросов на предоставление личной информации.

Защита личных данных:

Контроль доступа: Убедитесь, что ваши личные данные и аккаунты доступны только вам. Используйте двухфакторную аутентификацию, чтобы усилить защиту входа.

Ограничение общедоступности: Не публикуйте слишком много личной информации в открытых источниках, таких как социальные сети.

Защита устройств:

Обновление программного обеспечения: Регулярно обновляйте операционные системы и программы на всех ваших устройствах. Обновления часто включают исправления уязвимостей.

Антивирусное программное обеспечение: Установите надежное антивирусное программное обеспечение на свои устройства и регулярно сканируйте их.

Онлайн-покупки и финансовые операции:

Проверка надежности сайтов: Перед совершением онлайн-покупок убедитесь, что сайт является надежным и защищенным. Используйте только известные и проверенные платежные системы.

Мониторинг финансовых операций: Регулярно проверяйте свои банковские и финансовые операции на предмет несанкционированных транзакций.

Программы и инструменты защиты:

Используйте VPN: Виртуальные частные сети (VPN) могут помочь обеспечить безопасность при передаче данных через открытые сети.

Установите файрволлы: Используйте программы или устройства, которые предоставляют брандмауэры (файрволлы) для защиты сетевого трафика.

Используйте браузеры с механизмами защиты: Некоторые современные браузеры обладают встроенными механизмами защиты от мошеннических веб-сайтов и вредоносных программ.

Соблюдение законов и уведомление о преступлениях:

Сообщение о преступлениях: Если вы стали жертвой онлайн-преступления, обязательно сообщите о нем в местные правоохранительные органы и органы киберполиции. Важно сохранить все доказательства.

Соблюдение законов: Всегда соблюдайте законы и нормы в интернете. Незаконные действия могут привести к негативным последствиям.

Профилактика и защита от онлайн-преступлений требуют постоянной бдительности и образования. Эффективные меры защиты помогают не только избежать потери личных данных и финансовых средств, но и содействуют общей кибербезопасности.

Заключение

Мошенничество в сети Интернет обладает рядом отличий по сравнению с традиционным мошенничеством. Эти отличия обусловливают особенности расследования данного преступления. В частности, такие особенности проявляются при производстве оперативно-розыскных мероприятий и следственных действий. Проведение оперативно-розыскных мероприятий и следственных действий при расследовании Интернет-мошенничества осложняется тем, что часть добываемой при их производстве информации добывается из источников виртуальной информации (компьютер потерпевшего или преступника, удалённый локальный сервер, сеть Интернет и т.д.). Применение специальных познаний при расследовании мошенничества требует также от следователя знания высоких информационных технологий для определения необходимой специализации, которой должно обладать эксперт и специалист, а также для наиболее продуктивного взаимодействия с указанными лицами на всех этапах предварительного расследования Интернет-мошенничества.

Изучение проблем расследования Интернет-мошенничества должно проходить с одной стороны, в тесном взаимодействии научных исследователей и практикующих специалистов, а с другой – с привлечением специалистов из других наук (помимо криминалистики), например, информатики, вирусологии и т.п. Такой подход позволит глубже изучить аспекты расследования и предупреждения Интернет-мошенничества, а также его связь с другими правовыми и социальными явлениями. В теории и практике реагирования на инциденты информационной безопасности на предприятиях отмечается высокая значимость такого этапа, как анализ проведённого расследования с целью увеличения эффективности пользу и сотрудникам правоохранительных органов, занимающихся расследованием преступлений в сфере высоких технологий.

Как и традиционное мошенничество, Интернет-мошенничество характеризуется высокой динамичностью с точки зрения способов совершения. Поэтому чрезвычайно важным представляется обсуждение наиболее сложных моментов в расследовании. Выполнение данной рекомендации позволит повысить уровень теоретической и практической подготовки следователей за счёт более оперативного освоения новых знаний.

Важное значение тактических приемов, как тактико-криминалистических средств досудебного производства, которые оказывают воздействие на материальные и идеальные объекты с целью изменения их состояния, обусловлено особой сложностью криминалистической поисково-познавательной деятельностью следователя. Многообразие свойств и связей таких объектов, ситуаций, в которых они получают свое проявление, а также организационных связей следователя с иными субъектами, прежде всего с должностными лицами, осуществляющими оперативно-розыскную деятельность и специалистами в области информационных технологий, требует от криминалистической науки совершенствования в разработке системных средств научного познания о тактико-криминалистических средствах досудебного производства.

Список использованных источников

1. Свободная энциклопедия Википедия, статья «IP-адрес» // https://ru. wikipedia.org/wiki/IP-адрес (дата обращения: 25.08.2023).
2. Свободная энциклопедия Википедия, статья «MSISDN» // https://ru. wikipedia.org/wiki/MSISDN (дата обращения: 25.08.2023).
3. Свободная энциклопедия Википедия, статья «IMSI» // https://ru. wikipedia.org/wiki/IMSI (дата обращения: 25.08.2023).
4. Свободная энциклопедия Википедия, статья «MSIN» // https://ru. wikipedia.org/wiki/ MSIN (дата обращения: 25.08.2023).
5. Свободная энциклопедия Википедия, статья «IMEI» // https://ru. wikipedia.org/wiki/ IMEI (дата обращения: 25.08.2023).
6. Свободная энциклопедия Википедия, статья «Кликджекинг» // https:// ru.wikipedia.org/wiki/Кликджекинг (дата обращения: 25.08.2023).
7. Блокчейн // Википедия. [2021] // «https://ru.wikipedia.org/?curid= 5677831&oldid=112514965 (дата обращения: 25.08.2023).
8. Криптовалюта // Википедия. [2021] // https://ru.wikipedia.org/?curid= 4573896&oldid=112977807 (дата обращения: 25.08.2023).
9. Нигерийские письма // Википедия [2021] // https://ru.wikipedia.org/? curid=107632&oldid=112978585 (дата обращения: 25.08.2023).
10. Кто такие киберсквоттеры? // https://wwhois.ru/whois_squat.html (дата обращения: 25.08.2023).
11. Киберсквоттинг // Википедия https://ru.wikipedia.org/?curid=107180& oldid=112620443 (дата обращения: 25.08.2023).

12. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V ЗРК // http://adilet.zan.kz/rus/docs/K1400000231 (25.08.2023).

13. Чурилов С.Н. Предмет доказывания в уголовном судопроизводстве и криминалистике. Научно-практическое пособие. // – М.: ЗАО Юстицинформ, 2010. – С. 136.

14. Коновалова В.Е., Колесниченко А.Н. Теоретические проблемы криминалистической характеристики // Криминалистическая характеристика преступления // – М., 1984. – С.15-19.

15. Курс лекций Краснодар КРУ МВД России // https://shikardos.ru/text/ kurs-lekcij-krasnodar-kru-mvd-rossii-2013-bbk-88-4-odobreno-o/page-7 (25.08.2023).

16. Обирин А.И., Каплун Д.Д. Следственная ситуация как система // Вестник Тихоокеанского государственного университета. 2014. №1 (32). – С. 271-274.

17. Князьков А.С. Классификации следственных ситуаций // Вестник Томского государственного университета. 2013. №1 (7). – С. 36-47.

18. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: диссертация кандидата Юридических наук: 12.00.12. – Москва, 2016 // http://www.dslib.net/finans-pravo/taktika-proizvodstva-sledstvennyh-dejstvij-pri-rassledovanii-kiberprestuplenij.html#7466023.

19. Мартынова И.Г. К вопросу о назначении судебных экспертиз при расследовании мошенничества, совершаемого в отношении юридических лиц в сфере экономики // Известия ТулГУ. Экономические и юридические науки. 2013. №4-2. // https://cyberleninka.ru/article/n/k-voprosu-o-naznachenii-sudebnyh-ekspertiz-pri-rassledovanii-moshennichestva-sovershaemogo-v-otnoshenii-yuridicheskih-lits-v-sfere (дата обращения: 02.04.2021).

20. Домен // Википедия // https://ru.wikipedia.org/wiki/Домен#:~:text= Доме́н%20(фр.%20domaine)%20%20область%3B,от%20смеж

ных%20областей%3A%20Домен%20(магнетизм) (дата обращения: 25.08.2023).

21. Эмитент карты -кредитная организация, выпускающая карты //http:// dic.academic.ru/dic.nsf/fin (дата обращения: 02.04.2021).

22. Мошенничество при оформлении кредитов // http://finpravsentr.ru/ moshennichestvo-pri-oformlenii-kreditov-40459/ (дата обращения: 25.08.20213.

23. Как не стать жертвой кредитных мошенничеств // https:// pomochcredit.pro/kak-ne-stat-zhertvoj-kreditnyx-moshennikov (дата обращения: 25.08.2023).

24. Фрилансер // Википедия // https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B8%D0%BB%D0%B0%D0%BD%D1%81%D0%B5%D1%80 (дата обращения: 25.08.2023)

25. Шадрин Ю.А. «Предупреждён-значит, вооружён» // https:// monchegorsk.gov-murman.ru/zhitelyam/obshchestvennaya-bezopasnost/v-pomoshch -grazhdaninu/moshennichestva_broshyura.pdf (дата обращения: 25.08.2023).

26. Способы защиты Ваших персональных данных. http:// nordconsulting.ru/sposoby-zashhity-vashih-personalnyh-dannyh (дата обращения: 25.08.2023).

27. Концепция «Киберщит», утвержденная Постановлением Правительства РК от 30 июня 2017 №30// http://adilet.zan.kz/rus/docs.

28. Корыстная цель как признак хищения в уголовном праве // https:// businessman.ru/koryistnaya-tsel-kak-priznak-hischeniya-v-ugolovnom-prave.html.

29. Борчашвили И.Ш., Мукашев А.К. Преступление против собственности: Монография. – Астана, 2009.

30. Борчашвили И.Ш. Комментарий к УК РК. Особенная часть (том 2). – Алматы: Жеті жарғы, 2015.

Содержание

Введение 3

1. Определение и классификация онлайн-преступлений
1.2. Критерии классификации онлайн-преступлений..... 8

2. Тактика и методика раскрытия и расследования онлайн-преступлений 11

3. Профилактика и защита от онлайн-преступлений.....55

Заключение 58

Список использованных источников 60

Редактор:
Саратекова К.Н.

Отдел организации научно-исследовательской и
редакционно-издательской работы Алматинской академии
МВД Республики Казахстан им. М. Есбулатова
050060 Алматы, ул. Утепова, 29

Подписано в печать «03» ноября 2023 года.
Формат 60х84 1/16. Бум.тип. №1. Офсетная печать.
Уч.изд. 2,3 п.л. Тираж 50 экз.