АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

СЕКЕНОВА БОТАГОЗ БАЗАРХАНОВНА

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ОТДЕЛЬНЫХ ВИДОВ ИНТЕРНЕТ - МОШЕННИЧЕСТВА: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Специальность 7М12301 – Правоохранительная деятельность
Диссертация на соискание академической степени
магистра юридических наук

Научный руководитель,
Доктор (PhD),
ассоциированный профессор
(доцент) _____ Медиев Р.А.
подпись

Магистрант _____ Секенова Б.Б.
подпись

г. Косшы, 2022

Б.Б. Секенованың «Интернет - алаяқтықтың жекелеген түрлерін тергеудің ерекшеліктері: мәселелер мен перспективалар» магистрлік диссертациясына

ТҮЙІНДЕМЕ

Диссертациялық зерттеу интернеттегі алаяқтықтың жекелеген түрлерін тергеудің ерекшеліктерін зерттейді.

Жұмыста интернет - алаяқтықты сот-сараптамалық талдауға, интернет-алаяқтықты тергеудің бастапқы кезеңінің ерекшеліктеріне және интернет - алаяқтықты оңтайландыру және сапалы тергеу шарты ретінде арнайы білімді қолдануға баса назар аударылды.

РЕЗЮМЕ

магистерской диссертации Б.Б. Секеновой «Особенности расследования отдельных видов интернет - мошенничества: проблемы и перспективы»

В диссертационном исследовании изучаются особенности расследования отдельных видов интернет - мошенничества.

В работе были сделаны акценты на криминалистический анализ интернет - мошенничества, особенности первоначального этапа расследования интернет - мошенничества и использование специальных знаний как условие оптимизации и качественного расследования интернет - мошенничества.

SUMMARY

master's thesis B.B. Sekenova «Features of the investigation of certain types of Internet fraud: problems and prospects»

The dissertation study examines the features of the investigation of certain types of Internet fraud.

The work focuses on the forensic analysis of Internet fraud, the features of the initial stage of the investigation of Internet fraud and the use of special knowledge as a condition for optimizing and qualitatively investigating Internet fraud.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

г. — год, город

УК — Уголовный кодекс

УПК — Уголовно-процессуальный кодекс

ЕРДР — Единый Реестр Досудебного Расследования

КРКоАП — Кодекс Республики Казахстан об административных правонарушениях

МВД РК — Министерство внутренних дел Республики Казахстан

РК — Республика Казахстан

РФ — Российская Федерация

СНГ — Содружество Независимых Государств

СССР — Содружество Советских Социалистических Республик

ст. — статья

США — Соединенные Штаты Америки

ч. — часть

ЭВМ — электронно-вычислительная техника

ПК — персональный компьютер

СКТ — средства компьютерных технологий

КТ — компьютерная техника

ПО — программное обеспечение

МВД — Министерство внутренних дел

ИТ — информационные технологии

ОРМ — оперативно розыскные мероприятия

НСД — негласные следственные действия

ВВЕДЕНИЕ

Актуальность проводимого исследования. Уголовные правонарушения в области информатизации и связи является одним из активно прогрессирующих видов виртуальной преступности в условиях нашего социума и массового распространения цифровых устройств (гаджетов) облегчающая жизнь человека.

Процесс развития в области телекоммуникационной связи, цифровизации всей сферы жизнедеятельности человека, его безграничный доступ через сети Интернета к любым веб-страницам и сайтам, с возможностью мгновенного обмена информацией, ускорил развитие не только социальную сферу жизнедеятельности человечества, но и совершенно новых видов уголовных правонарушений.

Тем самым на сегодняшний день с помощью любых персональных устройств (компьютеров, гаджетов) и различного рода программ для обработки информационных данных совершаются преступные посягательства на личные данные граждан Республики Казахстан охраняемых Законом Республики Казахстан «О персональных данных и их защите» [1], основанные на Конституции Республики Казахстан [2].

Несмотря на кажущуюся малозначительность деяния, указанные правонарушения несут в себе реально высокую степень социальную опасность, поскольку их несвоевременное пресечение приводит к появлению у правонарушителя чувства безнаказанности в интернет среде и дает возможность оттачивать свои навыки «хакерства», далее в будущем способствующее совершению более тяжких преступлений.

Актуальный характер приобретает вид мошенничества, совершаемые с помощью Интернета, IT-технологии, сетей телекоммуникации и с использованием платежных банковских карт (интернет - мошенничество). В деятельности органов уголовного преследования отмечены проблемы эффективности расследования уголовных дел связанных с интернет -

мошенничеством, совершаемые через сети телекоммуникации [3]. Так как интернет - мошенники с каждым днем создают новые схемы для совершения данного правонарушения.

Борьба с интернет - мошенничеством представляет собой сложный, многогранный процесс, включающий применение экономических, финансовых, организационно - управленческих и законодательных мер.

Тем самым, диссертантом выбран вопрос исследования особенности расследования отдельных видов интернет-мошенничества, совершенное: путем обмана или злоупотребления доверием пользователя информационной системы (ст.190 ч.2 п.4 Уголовного кодекса Республики Казахстан) [4] (далее - интернет мошенничество).

Оценка современного состояния решаемой научной проблемы или практической задачи. Существенно увеличилось количество мошенничества совершаемых в сети Интернет, возрос причиняемый ущерб, изменились способы совершения и «инструментарий» мошенников (пишутся новые программы), придумываются новые мошеннические схемы. Феномен Интернет-мошенничество в наше время обрел широкое распространение. Результаты авторской работы могут стать фундаментом для внесения изменений в законодательство Республики Казахстан, а так же для разработки методических рекомендации по досудебному расследованию интернет - мошенничества в правоохранительной деятельности.

Цель, задачи, объект и предмет исследования.

Целью исследования является рассмотрение теоретических и практических особенностей расследования отдельных видов интернет - мошенничеств, и разработка рациональных способов организации раскрытия и расследования данного вида правонарушения.

Задачи исследования:

- изучить общие положения криминалистической характеристики интернет - мошенничества;

- проанализировать процессуальную модель механизма совершения интернет - мошенничества, его соотношение с криминалистической характеристикой;

- проанализировать особенности выявления признаков интернет - мошенничества и регистрации уголовного дела;

- изучить тактические особенности производства отдельных следственных действий на первоначальном этапе расследования интернет - мошенничества;

- рассмотреть формы использования специальных знаний при расследовании интернет - мошенничества;

- рассмотреть судебные экспертизы при расследовании интернет - мошенничества: проблемы и перспективы;

Предметом исследования является комплекс условий и явлений, обуславливающий выявление мошенничества в глобальной сети Интернет.

Объектом исследования, выступает мошенничество в глобальной сети Интернет, как специфическое противоправное явление, и особые формы социальной реакции на него.

Методы и методологические основы проведения исследования, составляет совокупность общенаучных (анализ, синтез, аналогия), частно-научных (статистический, социологический) и специальных (сравнительно-правовой и формально юридический) методов познания.

Обоснование научной новизны впервые комплексно проанализированы особенности и тактика расследования, раскрытия уголовных правонарушений, а именно интернет - мошенничества.

Также разработано и предлагается для использования в практической деятельности «Методические рекомендации по вопросам расследования и производства следственных действий по уголовным правонарушениям в сети Интернет».

Основные положения, выносимые на защиту.

1. Реализация на территории Республики Казахстан интегрированного банка данных «Интернет-мошенничество», даст возможность правоохранительным органам, анализировать и выявлять многоэпизодные правонарушения и правонарушения прошлых лет, путем идентификации способа совершении интернет-мошенничества (даты, период и место зарегистрированных заявлений и сообщений).

2. В целях повышения эффективности расследования уголовных дел в сети Интернета в оперативно-следственных подразделениях правоохранительных органов следует создать специализированные группы (отделы) для раскрытия и расследования правонарушений, совершаемые с использованием информационных технологий и сетей телекоммуникаций, с обязательным учетом специалиста-эксперта. (Использование современных экспертно-аппаратных программных комплексов позволяющих восстанавливать историю работы ПК, скопированные, удаленные файлы и др.).

3. Необходимо рассмотреть вопрос разработки Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам в сфере информатизации и связи». Так как на сегодняшний день при изучении материалов уголовных дел по преступлениям совершенные в сфере информатизации и связи, нет единой практики вопросов квалификации и методики и тактики расследования, (например, интернет – мошенничество, киберпреступления, интернет – хищение).

Апробация и внедрение результатов. Основные положения и выводы, содержащиеся в диссертации, нашли отражение в опубликованных 3 статьях, в том числе **1** — в международном научно-практическом журнале «Мир закона», **2** — в материалах международной научно-практической конференций.

1. ИНТЕРНЕТ - МОШЕННИЧЕСТВО КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА

1.1. Общие положения криминалистической характеристики интернет - мошенничества

Под общими положениями криминалистической характеристикой интернет - мошенничества понимается научно-практическое понятие о модели криминалистически значимых признаков рода и вида (групп) правонарушений (интернет – мошенничества), являющиеся в организационной и упорядоченной сочетаемый архиважных обстоятельств их проведения, а также закономерных соединительное звено между ними, и работающих для решения вопросов расследования правонарушений.

Таким образом, при исследовании криминалистической характеристики интернет - мошенничества, совершаемых с использованием сети интернет, необходимо установить и изложить как важнейшие определенное положение (составные части) совершения указанных правонарушений, так и взаимная связь среди данных сопутствующих явлений, с целью способствования полученной теоретической модели досудебному расследованию. Указанную теоретическую модель, по мнению исследователей, создает дальнейшее обстоятельства (составные части):

- объект, определяемый предметом правонарушений;
- средства правонарушений;
- субъект правонарушения (личность интернет - мошенника).

Видовым объектом интернет - мошенничества, совершаемых с использованием сети интернета, являются общественные отношения, складывающиеся в отношении собственности на имущества, находящиеся во владений, т.е. предмет правонарушения. Важнейшее обозначение для расследования правонарушений имеет вид указанного предмета правонарушения – цифровые деньги, которая, с одной стороны, детерминирует

субъекта и средства правонарушения, а с другой - тактику и методику расследования.

Рассмотрение и анализ субъекта интернет - мошенничества, совершаемых с использованием сети интернет (личности интернет - мошенника), владеют отдельное место в подходящий данному случаю криминалистической характеристике, т.к. являются только положительными по отношению выявления, досудебного расследования правонарушения.

Анализ практики расследования интернет - мошенничества, совершаемых с использованием сети интернет, показал, что субъектами таких правонарушений могут быть:

1) системные администраторы, бухгалтера, работники организаций, в том числе руководители;

2) уволенные работники организации;

3) иные лица.

Существуют несколько подходов к классификации личности интернет - мошенника по мотивам совершения правонарушений. Приведем классификацию, предложенную В.Б. Веховыми [5], дифференцирующую личность «интернет - мошенника» на 3 варианта:

1. Субъекты, отличающиеся качеством, являющиеся солидное соединение компетенции в области IT технологий и программирования (C++, Javascript, Payton), направленный на своеобразный преданность и изобретению новые схем. Резко выраженной уникальностью правонарушителей данного варианта имеется недостаток конкретное проявление антиобщественных умыслов. Относительно все правонарушения проводятся интернет – мошенниками в рамках выставления своих интеллектуально-технических и высоко-профессиональных умений.

2. Интернет - мошенничества могут совершаться правонарушителями, имеющими «интернет зависимость».

3. Целенаправленно занимающиеся интернет - мошенничеством имеющий выраженные корыстные намерения, именуемые «hacker». В сравнении от первого варианта переходной группы «начинающих» и второй особой группы «склонных», правонарушители третьей группы определяются рецидивностью совершения интернет – мошенничества, с имеющим возможность сокрытие правонарушения, и владеющий солидными навыками переубеждения.

В профессиональном плане интернет - мошенник, особенно те, которые создают (разрабатывают) вирусные программы и другие способы мошенничества, являются специалистами в области программирования, автоматизированных систем, системного администрирования, функционирующих в онлайн платформах (банковские сайты, онлайн биржи т.п.), а также владеют специальными навыками и умениями в сфере создания и управления сайтов [6].

Характеризуя таких правонарушителей, ученые-криминалисты исследуют нижеуказанные их качество привычек:

1) основная масса правонарушители, а именно интернет - мошенники склонны физика - математическим наукам и предпочитают работу технического или математического характера. Особые симпатии у указанных лиц к жанру фантастика. Также данные лица, владеют английским языком или, как правило, хорошо читают на нем;

2) интернет - мошеннику темперамент свободолюбий и самолюбие;

3) интернет - мошенники склонны «бессонным времяпровождением», когда никто не мешает;

4) длительный период времени интернет - мошенника сопровождает безбрачная семейная жизнь, вследствие времяпровождения в социальных сетях интернета;

5) внимание обустройству жилья и поддержанию в нем порядка интернет - мошенники не уделяют.

Логическим центром жилища является персональный компьютер, куда непрерывно подключаются локальные соединение, вводится, и в дальнейшем утилизируются программы (вредоносные и лицензионные);

6) длительное времяпровождение в социальных сетях интернета, подводит к тому, что данные правонарушители, являясь знатоками своего дела, постоянно поддерживают общения с собеседниками в такой же консервативной манере.

Специалисты отмечают следующую последовательность: чем законспирировано и информационно сложная схема интернет - мошенничества, количество правонарушителей, совершающее данное деяние сокращается. Обычно конструируется ситуационные моменты, когда только один метод совершения подобного правонарушения или используемый метод интернет - мошенничества практически единогласно может указать на данные правонарушителя.

Помимо профессиональных правонарушителей обосабливаются также субъектов:

- не имеющие глубокими умениями в сфере IT технологий, владеющих лишь некоторыми потребительскими навыками работы в социальных сетях интернета. Обычно, их действия нацелены на блокирование, модификацию, уничтожение и копирование не имеющий, защиты информации, после специального обучения конкретным навыкам;

- имеющих психологические отклонения, к числу которых относят субъекты, страдающих разнообразными компьютерными фобиями.

Долгое времяпровождение в онлайн среде, в социальной среде, приводит к существенному изменению психологии людей, их образа жизни. В частности, логика, психология мышления и поступков, даже повседневное поведение опытных программистов во многих случаях отличаются от психологии, мышления и поведения «обыкновенных» пользователей интернета.

Согласно статистическим данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан о зарегистрированных преступлениях, предусмотренных п. 4 ч. 2 ст. 190 УК Республики Казахстан в период времени с 2016 по 2020 года наибольшим количеством интернет - мошенников, являются лица мужского пола. Согласно статистике, среди пользователей Интернета соотношение женщин и мужчин примерно одинаково. Мужчины проявляют более высокую криминальную активность. Преобладание лиц мужского пола среди интернет-мошенников объясняется более высоким уровнем социальной активности мужчин [7].

За последний пять лет мужчин совершающие интернет – мошенничество неуклонно растет: в 2016 г. – 17; 2017 г. – 61; 2018 г. – 208; 2019 г. – 393; 2020 г. – 499 правонарушении. Женщины: в 2016 г. – 4; 2017 г. – 20; 2018 г. – 111; 2019 г. – 292; 2020 г. – 370 правонарушении.

Возраст интернет – мошенников						
годы	**10-20 лет**	**21-30 лет**	**31-40 лет**	**41-50 лет**	**51-60 лет**	**61-70 лет**
2016	4	8	7	2	0	0
2017	5	37	21	16	2	0
2018	57	195	47	20	3	0
2019	103	399	120	49	13	1
2020	144	459	220	35	17	2

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. Это можно расшифровать профессиональными навыками отдельных должностей и специализацией на цифровые компьютерные системы (кассир, секретарь, менеджер, экономист, контролер, бухгалтер и т. д.), кем являются чаще всего женщины [8].

Также интернет – мошенники (одиночки) постепенно переходят на новый уровень, связанные с хорошо законспирированными и ячейками групп, объединяющими хакеров из разных областей территорий нашей страны или зарубежных государств. Данное направление представляется тем, что большое количество интернет - мошенничества, совершаемых в социальных сетях, является достаточно, латентное явление, куда привлекаются большое количество субъектов с различными способностями. Вместе с тем каждый из этих субъектов может находиться в различных ролях в совершении интернет - мошенничества, тем самым, в разной мере может состоять в иерархии преступной группы.

Основные способы интернет - мошенничества, совершаемые с применением IT технологий (гаджетов), требуют навыки высококвалифицированного специалиста, подразумевающий организации преступных групп, где отдельные субъекты исполняют нацеленные правонарушения, для реализации одного результата. Так, например, преступная группа, совершающее интернет - мошенничество, имеют данные подгруппы:

- отдельные субъекты, взаимосвязанные с организатором и непосредственно привлечённые в совершении интернет - мошенничества: технический исполнитель;

- отдельные субъекты, взаимосвязанные с обнальщиком: субъект имеющие юридические лица, поддельные банковские карты и СИМ-карты;

- отдельные субъекты, взаимосвязанные с организатором, но не привлеченный именно в процесс интернет - мошенничества: IT - специалист, разработчики, исполнители [9].

Вместе с тем, вокруг отдельных субъектов, имеющих отношение интернет - мошенничеству, необходимо выделить «финансовых агентов», которые передают обнальщикам копии документов и иные реквизиты, субъектов, и (или) оформляют на подставного человека (например, для покупки

или регистрации фейковых юр. лиц), также банковские карты, с использованием которых проводятся операции по обналу украденных денег.

Также отметим, что отдельные лица, участвующие в интернет - мошенничестве, зачастую могут находиться не только в различных областях Казахстана, но и зарубежом. Правонарушители получают необходимые данные и контактируют с целью совершения интернет - мошенничества и иных компьютерных правонарушений в сети интернет.

Существует значительное количество темных сайтов, форумов, блогов и т.п., где концентрируются отдельные лица, склонные к совершению рассматриваемых и иных интернет правонарушений, происходит обмен мнениями и опытом, в том числе в данных сайтах находят единомышленников и объединяются в отдельные группы для создания новейших изощренных способов и методов интернет - мошенничеств с использованием сети интернет. Находясь в дали, друг от друга, обращаясь по никнейму (по кличке, прозвище), интернет - мошенники могут на протяжении длительного времени совершать данные правонарушения.

Также необходимо отметить, третье лицо (специально не принимающее участие в интернет - мошенничестве) могут пользоваться имуществом без осведомления их криминального происхождения.

В качестве средств интернет - мошенничества, совершаемых с использованием информационных технологий (гаджетов), необходимо рассматривать следующие структурные элементы:

- обстановку правонарушения;
- орудия совершения правонарушения;
- способы интернет - мошенничества.

Под положением правонарушения необходимо понимать систему разного рода взаимосвязанных объектов, процессов и явлений, характеризующих время и место правонарушения, особое поведение непрямых к данному деянию отдельных субъектов, психологические взаимосвязи между ними и другие

факторы объективной реальности, выявляющие условия планированию интернет – мошенничества [10].

Обстановку интернет - мошенничества, совершаемых с использованием сети интернета, имеют программные, цифровые, пространственные, организационные, временные, социально-психологические факторы их планирования, проведения и конспирация. Исключительностью указанного правонарушения является то, что на их проведение практически не оказывают воздействие природно-климатические условия.

Раскрытие особенностей обстановки интернет – мошенничества позволяет в короткое время установить, в каком направлений необходимо идти при осмотре места правонарушения, исследований персонального компьютера (гаджетов) и файлов, вызове и допросе свидетелей имеющие право на защиту и решении вопросов о необходимости выемки определенных документов и файлов.

Планирование, проведение и конспирация интернет - мошенничества, совершаемые в сети интернета, разнесены в пространстве режима он-лайн. Этим определяется особенность интернет - мошенничества, совершаемые в сети интернет, в том числе направленных на создание, применения и распространения вирусов: место совершения правонарушения (место, где проводились действия объективной стороны состава правонарушения) и место наступления преступных последствий (место, наступления результата противоправного деяния) не совпадают. Указанная закономерность независима от видов интернет - мошенничества.

Необходимо отметить, что местом подготовки интернет - мошенничества, совершаемых в сети интернет, могут являться жилые и служебные помещения, которые оборудуются персональными компьютерами и гаджетами, оборудованиями для разработки, модификации и распространения вирусных программ, сбора информации, а также других подготовительных действий. При этом указанные подготовительные действия даже по одному факту интернет -

мошенничества, как правило, расположены в разных местах (помещениях), также и в местах удаленные друг от друга в разных регионах страны, так и за рубежом.

Вместе с тем местами планируемых действий могут являться точки размещения на сайтах объявлений, о предоставлении тех или иных услуг, за определенные денежные средства.

Также, к местам подготовки интернет - мошенничества, совершаемых в сети интернет, можно отнести здания, в которых находятся сервера, в том числе за рубежом. Данное обстоятельство подтверждается выявлением фактов совершения интернет - мошенничество с использованием proxy-серверов с IP-адресами других стран.

Согласно ст. 5 УК Республики Казахстан временем совершения уголовного правонарушения признается время осуществления общественно опасного действия (бездействия) независимо от времени наступления последствий [4].

Список условий деяния интернет - мошенничества довольно разные и включающие отдельные группы и в целом цифровую IT - систему предприятий и ее возможности, со способами удовлетворения онлайн платежа, антивирусной программы, правовые основы реализации цифровых технологий.

Условия совершения интернет - мошенничества в сети интернет, неразрывно связаны с потерпевшими таких правонарушений.

Характеристика потерпевших до совершения, во время и после совершения интернет - мошенничества помогает точнее определиться во многих обстоятельствах правонарушения.

Поведение потерпевшего во многом зависит от сложной схемы правонарушения внешних и внутренних факторов. Поведение предпринимающий потерпевший, может существенно облегчить интернет - мошеннику совершение правонарушение. Между, интернет - мошенником и потерпевшим в большинстве случаев можно выявить связь и определить

причины, по которым имущество именно данного лица стали целью посягательства.

Отметим, что привести исчерпывающий перечень способов интернет - мошенничества, совершаемых в сети интернет невозможно, так как указанные схемы имеют разнообразные направления, в зависимости от профессионализма, избирательности и нового подхода интернет - мошенников. Вместе с тем, несмотря на различные схемы правонарушения интернет - мошенничества, можно указать следующие:

- рассылка СМС-сообщений о крупном выигрыше или блокировке банковских счетов;

- создание Интернет-магазинов по продаже товаров, предлагающих продукции по низким ценам и требующих предоплаты на карту;

- размещение объявлений о продаже продукцией в платформе онлайн-объявлений с требованием переводов денежных средств авансом;

- создание, использование и распространение вирусов, позволяющих онлайн менять платежные переводы с персональных устройств потерпевшего или манипулировать операциями выдачи денег из банка.

Орудиями интернет - мошенничества, совершаемых в сети интернет, являются программы IT - технологий, связанные с сетью интернет, флешки, флеш-носители, специальные технические средства, вирусные программы, бот-сети и т.п.

Вместе с тем, технология перевода и снятия включает в себя каналы отправки цифровых денег через специальные платежные системы расчетов, электронные кошельки, типа QIWI кошелек, WebMoney, Яндекс деньги.

Схемы вывода цифровых денег из платежной системы WebMoney:

- виртуальная карта;

- Интернет - банкинг;

- банковская карта;

- карта, заказанная через сервис WebMoney;

- банковский перевод;

- обменные пункты и дилеры WebMoney;

- почтовый перевод;

- денежный перевод;

- цифровые деньги;

- биржа exchanger.kz.

- офис банка или партнера;

В рамках снятия похищенных денежных средств, интернет - мошенники применяют методы «распыления», включающий операции перечисления данных средств, с первого банковского счета на другие банковские счета, счетов иных финансовых систем, счетов компаний телекоммуникационной и сотовой связи.

В заключений, рассматриваемого раздела, необходимо отметить, что знание общих положений криминалистической характеристики интернет - мошенничества, совершаемые в сети интернет, дает предметно разрабатывать следственно-оперативные версии и исполнять отдельные следственные действия и их производстве, так как положение, образующие данную характеристику, находятся в закономерных связях между собой (системно-структурных, функциональных и т.д.). Основными (базовыми) элементами интернет - мошенничества, совершаемые в сети интернет:

- объект, предопределяемый предметом правонарушений;

- средства правонарушений;

- субъект правонарушения (личность интернет - мошенника).

Присутствие закономерных связей между положениями (составной части) криминалистической характеристики интернет - мошенничества, совершаемых в сети интернет, не исключает особенностей каждого конкретного факта правонарушения. Данные особенности, вместе с выявленными закономерностями, образуют систему, влияющие на производства досудебного расследования.

1.2. Процессуальная модель механизма совершения интернет-мошенничества, его соотношение с криминалистической характеристикой

Современный уровень развития цифровых технологий позволяет в короткие сроки обеспечить охват практически всего населения. Актуальный характер приобретает виртуальные виды мошенничеств, совершенные с помощью сети Интернет, IT-технологии, сетей телекоммуникации и с использованием платежных карт.

Данная работа направлена на анализ процессуальной модели механизма совершения интернет - мошенничества, и ее соотношение с криминалистической характеристикой.

Процессуальная модель механизма совершения интернет-мошенничества исключительно велико. Модель механизма совершения хищений чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием детерминирован предметом преступного посягательства, а точнее его формой (электронные (цифровые) денежные средства), доступ к которой обеспечивается цифровой онлайн платформой банковских и кредитных организации.

Давая общую характеристику процессуальной модели механизма совершения интернет - мошенничества, совершаемых в сетях интернета, необходимо отметить, что они представляют собой систему целенаправленных связанных действий (процесс), нацеленных на динамику подготовки, совершения и сокрытия правонарушений.

Процессуальную модель механизма совершения интернет-мошенничества, нами будет рассматриваться через призму следственных ситуации, направленных на первоначальные процессуальные действия для закрепления доказательств, при расследовании правонарушений данного вида.

Ситуация первая. Интернет - мошенничество через сайты объявлений. Интернет мошенник - продавец

Интернет-мошенник размещает на сайтах объявлений («OLX», «krisha.kz», «kolesa.kz» и др.) данные о каких-либо товаров и продаж, передаче в аренду помещений либо оказании каких, либо услуг, за которые в дальнейшем берут предоплату, на основании этого забирая деньги.

В данной следственной ситуации, следователю первоначально необходимо допросить потерпевшего и свидетелей, для установления криминалистически значимой информации, которые в дальнейшем даст возможность, планировать расследование интернет - мошенничества.

Во-первых, необходимо установить абонентский номер интернет - мошенника, по которому связывался с потерпевшим и свидетелем. Во-вторых, установить, какую услугу предлагал интернет - мошенник, и на каких сайтах размещал объявления. В-третьих, установить сведения по банковской карте или электронному кошельку интернет - мошенника, по которому были переведены денежные средства.

Для установления указанного, следователю необходимо составить отдельное поручение на проведение оперативно-розыскных мероприятий (далее - ОРМ), где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по информациям о сайтах разместившие объявления: 1) установить электронную почту, указанные при регистрации на сайтах объявлений; 2) установить IP-адрес устройства (гаджета), с которого было подано объявление; 3) провести анализ дополнительных объявлений, установленных при помощи Cookie.

- по банковской карте или электронному кошельку интернет -мошенника, по которому были переведены денежные средства: 1) провести анализ

передвижения денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить данный по оплате банковской карте или услугой «мобильного банкинга».

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести первым для качественного закрепления и фиксации доказательств.

Ситуация вторая. Интернет - мошенничество через сайты объявлений. Интернет мошенник-покупатель

Интернет - мошенник связывается по телефону, по объявлению потерпевшего, ссылаясь на сайты («OLX», «krisha.kz», «kolesa.kz» и т.д.) и сообщает, что ему необходимо купить его товар и может внести предоплату, для этого просит сообщить необходимые данные по банковской карте и поступивший по СМС код. Получив необходимые сведения, переводит через онлайн сервисы или проводя покупку. Также интернет - мошенник просит прибыть к банкомату и провести ряд необходимых комбинаций, включая мобильный банкинг, с последующим совершением кражи денег.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет – мошенника, во-вторых информацию по объявлению интернет - мошенника, размещенные на сайтах, в-третьих банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по информациям о сайтах разместившие объявления: 1) установить электронную почту, указанные при регистрации на сайт объявлений; 2) установить IP-адрес устройства (гаджета), с которого было подано объявление; 3) провести анализ дополнительных объявлений, установленных при помощи Cookie.

- по банковской карте или электронному кошельку интернет - мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация третья. Интернет - мошенничество со взломом страниц социальных сетей

Интернет - мошенник пользуется услугами по взлому страницы социальных сетей (Vk.com, ok.ru, drugvokrug.ru и др.) либо проводит это сам. Далее связывается со всеми друзьями из списка контактов, пишет сообщения о просьбе одолжить деньги под разными предлогами (не хватает на покупку, заболели родители и т.д.).

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых период взлома и переписки в социальной странице потерпевшего, во-вторых, банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по социальной странице потерпевшего: 1) установить информацию о пользователе страницы социальной сети; 2) установить IP-адрес устройства

(гаджета), с которого осуществлялось переписка интернет - мошенника с родственниками.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация четвертая. Интернет - мошенничество, совершенное с использованием интернет сайтов (Интернет магазинов)

Интернет - мошенник покупает (или создает) сайт по предоставлению товара и услуг различного характера. Регистрирует пару виртуальных номеров (8-800-000-000…) у SIP-провайдера и вносит их на сайте в качестве контактов. Далее принимает потенциальных покупателей, принимая от них деньги за товары с сайта.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых услуги SIP-провайдера по виртуальному номеру интернет - мошенника, во-вторых, доменное имя, и хостинг арендованного сайта, в-третьих организацию арендодателей хостинга.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по SIP-провайдеру виртуального номера интернет - мошенника: 1) установить IP-адрес устройства (гаджета), с которого осуществлялись виртуальные звонки; 2) чаты по которым проводились звонки «Telegram», «Viber» или «WhatsApp» и т.д.

- по доменному имени и хостингу арендованного сайта: 1) данные о субъекте, осуществившем аренду; 2) пользовательские банковские карты и счета для оплаты арендатору; 3) IP-адреса, онлайн почты, телефоны арендатора.

- по сайтам хостинг - арендодателей: 1) установить аренду части пространства на данном сервере; 2) запросить соответствующие договора и оплату предоставляемых услуг; 3) допросить хостинг - арендодателя.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация пятая. Интернет - мошенничество, совершенное под предлогом заказа банкета (или связь с курьером)

Интернет - мошенник связывается с организацией и сообщает, что ему необходимо воспользоваться ее услугами по пред-заказу банкета, пред-заказу большой партии продукции или других услуг. После интернет - мошенник передает адрес, где он может встретиться с администратором компании и берет его контакты. Далее интернет - мошенник переговаривает с администратором и просит по пути перевести на счет абонентского номера (или банковской карты) необходимую сумму, которую он переведет позже.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет - мошенника, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация шестая. Интернет - мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств

Интернет - мошенник рассылает СМС-сообщений с текстом о списании денег или блокировке банковской карты. В этом сообщении указывается другой сотовый номер (иногда виртуальный 8-800-000-000…), который может дать информацию о произошедшем. Потерпевший связывается по данному телефону, после чего интернет - мошенник пытается узнать данные банковской карты.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет - мошенника, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства, в-третьих - услуги SIP-провайдера по виртуальному номеру интернет - мошенника.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

- по SIP-провайдеру виртуального номера интернет - мошенника: 1) установить IP-адрес устройства (гаджета), с которого осуществлялись

виртуальные звонки; 2) чаты по которым проводились звонки «Telegram», «Viber» или «WhatsApp» и т.д.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация седьмая. Интернет - мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду

Через домашний или сотовый номер потерпевшего связывается интернет - мошенник, обращаясь под видом близких родственников (привет дедушка, привет папа и т.д.). Сообщает, что попал в больницу или сбил человека, либо с кем-то подрался и т.д., а после передает трубку работнику правоохранительных органов, который за денежное вознаграждение предлагает помочь в вопросе об отказе в составлении протокола или регистрации уголовного дела.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет - мошенника, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по банковской карте или электронному кошельку интернет - мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация восьмая. Интернет - мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы

Через домашний или сотовый номер потерпевшего связывается интернет - мошенник, который, представляется сотрудником правоохранительных органов. И сообщает, что данный момент задержана группа интернет - мошенников, сбывавших несертифицированные БАДы, и что потерпевшему прилагается компенсация. Но для ее получения необходимо перевести деньги на счет (например, налоговый сбор или государственную пошлину).

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет - мошенника, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация девятая. Интернет - мошенничество, совершенное с использованием вредоносных программ на ОС «Android»

Потерпевшему на абонентский номер с операционной системой «Android» со скрытого номера поступает СМС-сообщения: «Добрый день, я по

Вашему объявлению. Интересует ли обмен с доплатой с моей стороны? Ссылка: https://www.olx.kz/FriZksk)», или СМС-сообщение: «Гляди, как мы хорошо вышли на этой фотографии. Ссылка www. URL/ZreizE1eaAa)». Потерпевший нажимает на данную ссылку, тем самым активируя вирус в своем телефоне (во многих случаях применяются вирусы, так называемые «Triada», «Marcher», «Loki», «Faketoken»), предоставляющий интернет - мошеннику доступ к СМС-командам. Далее интернет - мошенник крадет деньги, с помощью сообщений на номер «800».

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых абонентский номер интернет - мошенника, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить ранее судимых проживающих в данном секторе.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств.

Ситуация десятая. Интернет - мошенничество, совершенное с использованием социальных сетей (интернет магазин «Instagram»)

Интернет - мошенник создает онлайн страницу или сообщества в интернете, ассоциирующий себя как онлайн - магазин. Далее принимает покупки, получая от них деньги за покупку того или иного товара.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить, во-первых название сайта или интернет магазина, во-вторых банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Далее следователь выносит отдельное поручение на проведение ОРМ, где оперативным подразделениям необходимо провести следующее ОРМ:

- по абонентскому номеру: 1) информацию о субъекте, разместившем объявление о продаже (наименование товара) с сотового телефона (номер интернет - мошенника), 2) IP-адреса, электронные почты, абонентские номера арендатора.

- по банковской карте или электронному кошельку интернет – мошенника, по которому были переведены денежные средства: 1) передвижение денежных средств; 2) в случае снятия денежных средств, запросить видео с банкомата; 3) в случае покупки в интернет магазинах, запросить по покупке.

Далее по обстоятельству следователь решает, какие следственные действия оптимально провести, для качественного закрепления доказательств [11].

Криминалистическая характеристика интернет - мошенничества отличается от общеизвестных уголовных правонарушений против собственности. Основные структурные элементы правонарушений указанного вида имеют рядом особенностей. Общеправовая практика в первую очередь выделяет следующие криминалистически значимые сведения:

- о личности интернет - мошенника;

- о мотивах и целях преступного поведения интернет - мошенника;

- о типичных способах подготовки, совершения и сокрытия интернет - мошенничества;

- о времени, месте и обстановке преступных посягательств.

Обстановка совершения интернет - мошенничества принимает в себе собственные, прикладные, технические и социальные и психологические факторы среды, в которой совершается правонарушение. Она имеет влияние на формирование всех остальных структур криминалистической характеристики интернет - мошенничества, определять характерные поведения правонарушителя и потерпевшей стороны.

Основным компонентом обстановки планирования, совершения и сокрытия интернет - мошенничества, являются определенные условия рода деятельности потерпевшего (физических и юридических лиц), среди которых объективным и субъективным условиям относятся (таблица 1):

Таблица 1.

Объективные	**Субъективные**
- род деятельности или вид занятия (область работы - частная, финансовая, организационная, предприятие, цифровая, оказание услуг, частная организация, ТОО, транспортная и т.д.);	- игнорирование рекомендуемых инструкции режимов обработки цифровых информации;
- собственность физического лица или юридического лица, вид права отдельных видов имущества, в т.ч. цифровых информации и информационных ресурсов;	- неимение или недостаток средств защиты цифровой информации;
- задача и структура предприятий производственного процесса, вид	- отступление правил работы, в рамках правил безопасности

потребляемых запасов и выпускаемых товаров (в т.ч. и авторский);	компьютерной информацией;
- вид применяемых технологий, телекоммуникационные связи, их тактико-технические данные и технические недостатки;	- плохая организация производственных работ, присутствие параллельно ручных и автоматизированных этапов обработки данных (файлов);
- процесс реализации выпускаемой продукции, имущество;	- взаимоотношения должностных лиц, работников, психологическая атмосфера.
- присутствие и рабочее состояние средств учета, защиты цифровых информации, и их охрана.	

Субъективные факторы влияют на обстоятельство совершения интернет - мошенничества и некоторым образом составлять ее. Важной составной частью криминалистической характеристики правонарушений, соединенный с применением информационных технологий, может быть информация о натуре интернет - мошенника.

Правонарушителей совершающие в сети Интернет мошенничество и иные преступления называют (таблица 2):

Таблица 2.

Хакеры (от английского слова hacker)	**Крэкеры (от английского слова cracker)**	**Фрэкеры (от английского слова phracker)**
- пользователь персонального	- пользователь персонального	- субъект, специализирующийся

устройства, IT системы или их сети, занимающийся несанкционированным поиском способов получения неправомерного доступа к персональным устройствам (гаджетам) и охраняемой законом телекоммуникационных данных;	устройства, IT системы или их сети, занимающийся «взломом» (моделей, блокированием, удалением) программных средств защиты телекоммуникационных данных, охраняемых законом РК;	на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации.

Лица, указанные в таблице 2, всегда имеют довольно большими техническими навыками и прикладным характером в сфере IT технологий. Ими могут являться, лица имеющий, хобби в компьютерных играх и программированием C ++, javascript ученики, обучающиеся студенты и молодые IT специалисты, оттачивающий навыки в этой области деятельности.

Необходимо отметить, что лица совершающие правонарушения в сети Интернет, а именно интернет – мошенничество, состоят в региональных форумах, где публикуют свои кибернавыки социальных сетях (статьи, комментарии и т.д.), также проходят онлайн конференции, который ежеминутно обновляется и рассылается при помощи информационных бюллетеней. В этих онлайн сообществах есть все нужные информации для повышения уровня профессионализма молодого правонарушителя - рекомендации и схемы совершения и сокрытия интернет – мошенничества, от примитивных, до специально завуалированных и сложных. Безграничные просторы сети Интернета, также дает возможность начинающему

правонарушителю обмениваться опытом с зарубежными интернет – мошенниками в режиме онлайн.

Согласно статистическим данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан (далее - КПСиСУ) о зарегистрированных преступлениях, предусмотренных п. 4 ч. 2 ст. 190 УК РК наибольшим количеством интернет - мошенников, являются лица мужского пола. Согласно статистике, среди пользователей Интернета соотношение женщин и мужчин примерно одинаково. Лица мужского пола проявляют более высокую криминальную активность. Преобладание правонарушителей мужчин среди интернет - мошенников объясняется более высоким уровнем социальной активности последних [12].

Характерные мотивы и цели интернет - мошенничества следующие (таблица 3):

Таблица 3.

Мотивы	**Цели**
- сокрытие доходов и отказ от уплаты налогов, платежей, сборов и т.п.;	- преступные доходы, акции, кредита, драгоценные металлы, товаров, услуг, исключительные права, квоты, недвижимые имущество;
- конфликт и месть на работе коллегам или руководству по работе;	- фальсификация и подделка документов, штампов, печатей, бланков, денег в корыстных целях;
- из хулиганских побуждений;	- копирование тайной информации в корыстных целях;
- демонстрация своих высоких технических навыков и преимущество.	

Время совершения интернет-мошенничества установление вплоть до дня, часах и минутах, практическим работникам удается редко. Такие точности необходимы в рамках выявлении отдельных эпизодов правонарушений деятельности. В основном, время совершения данных правонарушений устанавливают разными по продолжительности периодами, связанными с деятельностью интернет - мошенников или предприятий. При этом, согласно ст. 5 УК Республики Казахстан, временем совершения уголовного правонарушения признается время осуществления общественно опасного действия (бездействия) независимо от времени наступления последствий [4].

Местом совершения интернет-мошенничества могут быть как места и объекты территории, так и те учреждения, организации, предприятия и системы, где применяются те или другие персональные компьютера (гаджеты) с выходом в сети Интернет. Следовательно, мест совершения интернет-мошенничество, т.е. обмана или злоупотребления доверием пользователя информационной системы, могут быть некоторое количество, также гораздо отдаленных друг от друга и находящих в разных областях, так и в других странах. Все это может быть по причине неограниченного радиуса работы и радиуса сотовой сети Интернет.

2. ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

2.1. Особенности выявления признаков интернет-мошенничества и регистрации уголовного дела

Досудебное расследование по зарегистрированным правонарушениям интернет-мошенничества нацелено на обнаружении и фиксации криминалистический значимой цифровой информацией, и в дальнейшим переводимое в качестве доказательств материалов по уголовным делам. Цифровые данные как элемент построения дальнейших следственных ситуаций исходят друг от друга. Можно отметить, что каждое следственное действие, начиная от осмотра места происшествия, передает информацию о механизме и процессе совершения правонарушения, которые позволяют следователю в дальнейшем выдвигать версии и проводить по ним расследование.

Особенности организации и проведения проверки заявлений и сообщений об интернет-мошенничествах.

Для установления основания для регистрации в Единый реестр досудебного расследования (далее - ЕРДР) [13] и проведение по ним проверочных следственных действий необходимо производства неотложных мероприятия:

- отобрать письменное заявление от физического лица;

- произвести неотложные следственные действия, как осмотра места происшествия;

- получение данных и необходимых материалов;

- давать отдельные поручения оперативникам на проведение негласных следственных действий.

При производстве осмотра места правонарушения необходимо пригласить для участия в следственных действиях:

- программистов C++, javascript, разрабатывающие программные обеспечения;

- операторов или IT специалистов по программному обеспечению, эксплуатирующие и ремонтирующие компьютеры;

- системных администраторов, программистов;

- специалистов инженеров по телекоммуникационным связям и оборудованиям;

- IT специалистов по обеспечению кибербезопасности.

Практика показывает, что указанными IT специалистами в основном бывают работники той предприятии – провайдера, через, чьи приложения и был совершен интернет - мошенничество.

При опросе потерпевшего по интернет – мошенничеству, следователю необходимо выяснить:

1. Были ли случай, временная передача или утере удостоверения личности?

Примером можно привести уголовное дело № 211510031000920 по обвинению У., в ходе расследования было установлено, что в ноябре месяце 2017 года У., находясь по адресу город Актобе, улица Э, дом № 01, квартира 1, умышленно из корыстных побуждений, с целью хищения чужого имущества, путем обмана или злоупотребления доверием, под предлогом оплаты коммунальных услуг, получила оригинал удостоверения личности и банковской карты АО «Народный Банк Казахстана» Ж., в ноябре.2017 года в неустановленном следствием время У., находясь по адресу город Актобе, жиллой массив А-2, участок №107 используя вышеуказанные документы Ж., как пользователя информационной системы, посредством интернет ресурсов, умышленно, из корыстных побуждений и извлечения материальной выгоды, путем подачи заявки от имени Ж., оформила на имя последней онлайн микрокредит в ТОО «МФО «Онлайн финанс» на возможную сумму 500 000 тенге, которые в ноябре 2017 года после одобрения займа примерно после 17:00

часов времени сняла с банкомата расположенного в ТД «А» по адресу город Актобе, улице А., дом №4 [14].

2. Были ли случай, доступа в персональному компьютеру или ноутбуку не знакомыми лицами? (ремонтниками компьютеров и ноутбуков).

Примером можно привести уголовное дело по обвинению К., в ходе расследования было установлено, что в 2016 году, в неустановленное следствием времени, К., через платформу онлайн-объявлений OLX предоставлял услуги ремонта компьютеров и ноутбуков. В ноябре месяце 2016 года, в рамках оказания услуг с выездом на дом по ремонту компьютеров и ноутбуков, во время ремонта скопировал личные данные, логин и пароль Б.

Далее находясь у себя дома по адресу п.К ул.С дом №4 Н района, со своего стационарного компьютера зашел в Интернет ресурс на сайт www.zaimer.kz для оформления кредита на имя Б.

Заполнив анкетные данные Б. для оформления кредита на имя последней в сумме 40 000 тенге и указал свой лицевой счет «K2000600009AA0060000», где на указанный лицевой счет поступили денежные средства в сумме 40 000 тенге [15].

В стадии регистрации уголовного дела ЕРДР, следователем могут быть истребованы следующие материалы и устройства:

1) история работы персональных устройств (гаджетов и смартфонов).

При расследовании уголовного дела по ст. 190 ч.2 п.4 УК Республики Казахстан, по обвинению С. В период с сентября по ноябрь 2018 года С., задавшись прямым преступным умыслом, направленным на незаконное обогащение за счет хищения чужого имущества, путем обмана и злоупотребления доверием пользователей информационной системы интернет ресурса, зарегистрировавшись в социальной сети «Инстаграмм», аккаунт «gold_be@an_g», указал ложную информацию о предоставлении ставок на спортивные матчи, а также увеличении прибыли с помощью ставок, сформировав ложное представление о подлинности своих намерений:

2018 году, примерно 18.08 часов С. из корыстных побуждений, преследуя цель незаконного извлечения наживы, достоверно зная о незаконной регистрации в социальной сети «Инстаграмм», аккаунт «gold_be@an_g», пользователю информационной системы А. через мобильное приложение «Whats app», сообщил о том, что для получения прибыли от ставок на спортивные матчи, необходимо перевести денежные средства в сумме 10 000 тенге на «Qiwi» кошелек. В свою очередь, С., заведомо зная, что не имеет фактической возможности увеличивать прибыль вложенных денежных средств потерпевшего, с целью достижения своей преступной цели перевел его денежные средства на карточный счет в АО «Каспий банк», воспользовавшись доверием потерпевшего, обналичил их и распорядился ими по своему усмотрению. Тем самым, причинил потерявшему А. материальный ущерб на сумму 10 000 тенге [16];

3) файлы и счета о проделанных операциях, например финансовых, проверок контролируемых денег, файлов и т.п.;

4) системный блок и флеш накопители данных;

5) данные (в виде файлов) о попытках противоправного примененииия персонального компьютера, незаконного подключения к сети Интернета.

На стадии регистрации уголовного дела ЕРДР, следователю в первую очередь необходимо установить факт правонарушения, для чего необходимо изъять и изучить персональный компьютер, ноутбук, смартфон, планшет и т.д.

При допросе, следователю целесообразно привлечь специалиста в области IT технологий.

В процессе подлежат выяснению следующие вопросы:

1. Когда и где именно потеряли или обманным путем завладели документами или гаджетом?;

2. Предоставляли ли свои анкетные данные, данные удостоверения личности и банковские сведения кому либо?;

3. Оформляли ли ранее в микрофинансовых организациях онлайн займы?;

4. Предоставляли ли кому, либо доступ к банковской карте?;

5. На какую сумму оформлены онлайн займы в микрофинансовых организациях?;

По всем операциям в микрофинансовых организациях онлайн займа следователем должны быть истребованы все обнаруженные сведения, для процессуального оформления.

Поводы и основания для регистрации в ЕРДР правонарушения в сфере интернет - мошенничества

Правонарушения в сфере интернет – мошенничества имеют высокую латентность и правоохранительные органы раскрывают лишь очевидные правонарушения, которая связана со сложностью восприятия без специальных навыков и знания в области цифровых технологий. Также незначительность ущерба потерпевшей стороны, которая отбивает желание, обращается в следственные органы. В некоторых случаях у работников оперативных подразделений на региональном уровне, отсутствует прикладной опыт в раскрытии схожих правонарушений. При исследовании данных по интернет – мошенничествам, в допросах потерпевших необходимо указать, что в первую очередь последние связываются и пытаются решить вопросы с организацией, представлявший услуги в онлайн платформах.

В Жамбылской области преступник позвонил по телефону жертве и сообщил о своем желании купить квартиру, объявление о продаже которой было размещено в интернете самим потерпевшим. В ходе переговоров мошенник обманом заполучил фото платежной карты и удостоверения личности жертвы. Затем, злоумышленник через личный кабинет в онлайн системе банка, получил доступ на депозитный счет потерпевшего, откуда похитил более 20.000.000 тенге путем их перевода на платежные карты подставных лиц. В то же время такие преступления сложно раскрыть из-за законодательных препятствии в области банковской тайны в соответствии ч.1 ст.50 Закона «О банках и банковской деятельности» от 31.08.1995г. [17]

Разграничение гражданско-правовых споров от интернет - мошенничества, в том числе совершенных с формальным заключением сделок

Одним из наиболее распространённых составов правонарушений, граничащих с гражданскими правоотношениями, является интернет - мошенничество.

Вопрос о разграничении интернет - мошенничества и гражданско-правовых отношений начинается в том случае, когда имеется некий договор. Маловажно какой – письменный или устный, но необходимость его обязателен. Основной сутью является взаимные отношения двух сторон: одна сторона передает денежные средства или имущество, другая – обязуется оказать услугу или передать (продать) имущество. Таким образом, обязательства должны быть встречные.

При, интернет - мошенничестве правонарушитель хочет заиметь имуществом или денежными средствами, договор является лишь ширмой преступных намерений лица.

В нормальных условиях гражданско-правовых отношений лицо метится исполнить свои обязательства по договору.

Проблема квалификации действий как мошеннических, является в следующем: необходимо выяснить и доказать умысел виновного на хищение денежных средств до момента заключения договора. Для этого необходимо установить, что виновный еще до момента вступления в гражданские правоотношения исполнять свои обязательства не собирался.

Основная сложность заключается в том, что виновное лицо тщательно скрывает свои истинные преступные намерения.

Необходимо отметить, что гражданско-правовые отношения, связанные с просто работы хозяйствующих субъектов, и правонарушения мошеннического характера разделяется тонкой гранью.

Поэтому прокурорам в ходе надзорной деятельности следует уметь четко разграничивать гражданско-правовые отношения от реального мошенничества.

Основные отличия гражданско-правовых споров от интернет - мошенничества

1. Наличие письменных сделок (договоров, расписок), не признанных судом недействительными, мнимыми или притворными.

Наличие письменных сделок (договоров), не признанных судом недействительными, мнимыми или притворными.

В соответствии со ст.179 УПК Республики Казахстан **(начало досудебного расследования)**, не подлежат регистрации заявления, сообщения или рапорт об уголовном правонарушении: о нарушениях, основанных на неисполнении или ненадлежащем исполнении гражданско-правовых сделок, совершенных в письменной форме и не признанных судом недействительными, мнимыми или притворными.

Указанные требования не распространяются на случаи подачи коллективных, многочисленных заявлений о недобросовестном исполнении договорных обязательств.

При этом, гражданско-правовая сделка должна отвечать следующим условиям:

- выражение согласованной воли всех сторон сделки;

- аналогичные сделки законодательству и нормативным актам;

- договор не должен противоречить устоям правопорядка и нравственности;

- участниками договора с обеих сторон могут быть лишь дееспособные и правоспособные лица;

- гражданин РК, договариваясь, должен быть в состоянии, позволяющем ему понимать последствия своих действий и руководить ими;

- договор не должен заключаться под воздействием заблуждения, обмана, насилия или угрозы.

2. Наличие претензии между юридическими лицами по договору оказания услуг.

Письмо-претензия или иначе письмо-рекламация – вид деловой корреспонденции, применяемый в тех условиях, когда одна сторона сделки в письменном виде высказывает, другой стороне неудовлетворение качеством исполнения обязательств или же информирует об их отсутствии.

В основном, письменной претензии предшествуют устные переговоры тет-а-тет или по телефонной линий, безрезультативного эффекта. Несмотря на от, были предварительные переговоры или нет, письменная претензия является верным способом решения подобных ситуации. Это связано с тем, что она сразу, в момент создания, переходит в доказательную юридическую силу, и в основном, позволяет справиться с вопросом в короткие сроки.

3. Наличие объективных обстоятельств, препятствующих исполнению взятых обязательств.

В соответствии с пунктом 11 Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам о мошенничестве» №6 от 29 июня 2017 года [18], в тех случаях, когда договор между сторонами заключается с обоюдными намерениями сторон исполнить соответствующие обязательства, но после его заключения и получения материальной выгоды у одной из сторон возникают объективные обстоятельства, препятствующие исполнению взятых обязательств, содеянное не может квалифицироваться как мошенничество.

Таким образом, состав уголовного правонарушения исключается, если субъект с самого начало стремилось исполнить обязательства по договору, но из-за определенных обстоятельств, возникших после передачи имущества, намерения виновного изменились.

В данном случае нет необходимости, чтобы лицо было уверено в том, что обязательства будут исполнены. Совершение сделки представляет собой

определенную степень риска, которая является частью коммерческой деятельности.

Еще одним объективным обстоятельством является письменно оформленное свидетельство о полном или частичном погашении ссуды, заверенное собственноручными подписями участников сделки (денежная расписка о возврате займа).

4. Наличие судебных решений по гражданским делам о взыскании займа, денежных средств, имущества и т.д.

Получение решения суда дает взыскателю гарантию возможности принудительно с помощью государства взыскать долг. Вступившие в законную силу судебные решения являются обязательными для всех без исключения органов государственной власти, органов местного самоуправления, общественных объединений, должностных лиц, граждан, организаций и подлежат неукоснительному исполнению на всей территории государства.

В случае, если лицо, на которое решением суда возложена обязанность выплатить долг, уклоняется от его выполнения, судебное решение подлежит принудительному исполнению в соответствии с законодательством об исполнительном производстве, т.е. этим займутся судебные исполнители.

5. Наличие исполнительного производства о взыскании займа, денежных средств, имущества и т.д.

Принимаются меры, направленные на принудительное исполнение исполнительных документов выдаваемых на основании судебных решений, определений, предписаний и постановлений по гражданским и административным делам, приговоров и постановлений в части имущественных взысканий.

За неисполнение приговора суда, решения суда или иного судебного акта либо исполнительного документа более шести месяцев, а равно воспрепятствование их исполнению предусмотрена уголовная ответственность по ст.430 Уголовного кодекса Республики Казахстан [19].

Необходимо помнить, что способы совершения интернет - мошенничества отличаются друг от друга и требуют индивидуального подхода.

Немаловажным фактором является анализ личности подозреваемого лица (не привлекался ли ранее за аналогичные правонарушения и т.д.).

Поэтому, надзирающим прокурорам следует в течение 24 часов с момента регистрации в ЕРДР проверять законность начала досудебного расследования и принятие мер по устранению нарушений (пункт 7 Инструкции по организации надзора за законностью уголовного преследования, утвержденной приказом Генерального Прокурора Республики Казахстан от 12 февраля 2018 года) [20].

В рамках регистрации в ЕРДР уголовные правонарушения по вопросам интернет – мошенничества, предлагаем рассмотреть опыт работников правоохранительных органов Российской Федерации, так например, О порядке формирования, ведения и использования подсистемы «Дистанционное мошенничество» программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня (далее - ПТК «ИБД-Ф») в ГУ МВД России [21].

В целях реализации подсистемы «Дистанционное мошенничество» утвержден приказ № 925 «Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» МВД РФ от 29 декабря 2020 года.

Порядок формирования, ведения и использования подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф».

1. Данный Порядок устанавливает положения формирования, ведения и использования системы «Дистанционное мошенничество» программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня (далее - Подсистема), направленный для сбора, систематизации, обработки и анализа сведений, собираемых в ходе проверки сообщений (заявлений) о правонарушениях, совершенных онлайн

способом с использованием IT технологий, и о досудебном расследовании уголовных дел по указанным правонарушениям в ГУ МВД РФ.

2. Объектами учета Подсистемы являются:

- зарегистрированные сообщения (заявления) о правонарушениях, совершенных онлайн способом с использованием IT технологий;

- зарегистрированные правонарушения, совершенные онлайн способом с использованием IT технологий;

- лица, подозреваемые, обвиняемые в совершении правонарушений онлайн способом с использованием IT технологий.

3. Внесение сведений в Подсистему осуществляется в следующем порядке:

3.1. Первичная информация о зарегистрированных сообщениях (заявлениях) о правонарушениях, совершенных онлайн способом с использованием IT технологий, ежедневно загружается в Подсистему из сервиса обеспечения деятельности дежурных частей ИСОД МВД РФ в автоматизированном режиме.

До разработки механизма автоматизированного пополнения Подсистемы первичная информация о зарегистрированных заявлениях (сообщениях) о правонарушениях вносится должностными лицами, которым поручено рассмотрение материалов в порядке статей 144, 145 УПК РФ, незамедлительно с момента его получения [22].

В случае регистрации уголовного дела в течение дежурных суток информация вносится должностными лицами подразделений следствия, дознания.

При работе с модулем ввода Подсистемы необходимо пользоваться правилами по внесению информации - рекомендаций по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф», разработанными ФКУ «ГИАЦ МВД РФ».

В модуле ввода поля:

- «ОВД 1 уровня»;
- «ОВД 2 уровня»;
- «Правонарушение раскрыто»;
- «Уполномоченный работник»;
- «Сотовый номер сотрудника»;
- «Фабула»;
- «Статус»;
- «Использовал»;
- «Фамилия»;
- «Имя»;
- «Число, месяц, дата рождения»;
- «Отношение к правонарушению»;
- «Наименование организации»;
- «Номер электронного кошелька»;
- «Обязательно к заполнению».

В процессе рассмотрения дела проверки по заявлениям (сообщениям) о правонарушении либо расследовании уголовного дела обязательному заполнению также подлежат поля:

- «Сотовый номер заявителя»;
- «Сотовый номер правонарушителя»;
- «Номер пластиковой карты заявителя»;
- «Номер расчетного счета заявителя»;
- «Номер пластиковой карты правонарушителя»;
- «Номер расчетного счета правонарушителя»;
- «Способ совершения правонарушения»;
- «Решение по уголовному делу»;
- «Дата последнего решения по уголовному делу»;
- «Статья УК РФ».

Считаем, что реализация на территории Республики Казахстан подобные ИБД «Интернет-мошенничество», даст возможность правоохранительным органам, анализировать и выявлять многоэпизодные правонарушения и правонарушения прошлых лет, путем идентификации способа совершении интернет-мошенничества (даты, период и место зарегистрированных заявлений и сообщений).

Отметим, что вышеуказанный перечень должна быть адаптирована, на постоянное расширение данных, к новым методам совершения интернет-мошенничество.

Также необходимо, отметить, что пришло время рассмотреть вопрос разработки Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам в сфере информатизации и связи». Так как на сегодняшний день при изучении материалов уголовных дел по преступлениям совершенные в сфере информатизации и связи, нет единой практики вопросов квалификации и методики и тактики расследования, например, интернет – мошенничество, киберпреступления, интернет – хищение и т.д.

2.2. Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования интернет-мошенничества

Основными следственными действиями, необходимыми при расследовании интернет - мошенничества, совершенные в сети Интернет являются:

- осмотр (места происшествия, предметов и документов);
- обыск (в жилище, в ином помещении, личный);
- выемка (предметов - электронных носителей информации, электронной почтовой корреспонденции);
- допрос (обвиняемого, подозреваемого, потерпевшего, свидетеля, эксперта, специалиста);
- негласные следственные действия;
- далее по обстоятельствам.

Организация осмотра (места происшествия, предметов и документов).

Особое значение осмотра места происшествия как первоначального следственного действия, заключается в том, что это самое близкое во времени и в пространстве соприкосновение следователя с событием преступления [23].

Сущность рассматриваемого следственного действия заключается в непосредственном анализе следователем (дознавателем) и другими участниками осмотра обстоятельства места преступления, в условиях которого выявляются, изучаются, фиксируются и изымаются в установленном законом порядке файлы, объекты и следы, с целью получения сведений, имеющие значение для раскрытия и расследования уголовного дела, а также событий, содержащих признаки правонарушения.

Специфика осмотра предметов (документов) при расследовании интернет - мошенничеств заключается в том, что осмотру подлежат, как правило, не

только файлы, содержащие текстовые или графические документы, подготовленные пользователем, но и рабочие журналы системных и прикладных программ, предназначенных для осуществления транзакций.

Таким образом, предполагается использование в ходе осмотра современных экспертных аппаратно-программных комплексов (например, BELKASOFT) [24], оснащенных необходимым экспертным программным обеспечением, позволяющих быстро находить требуемые файлы и интерпретировать их содержимое.

При осмотре месте происшествия могут, обнаружены такие флеш носители информации как накопитель на жёстких магнитных дисках (винчестер), флэш-карты памяти разной модификации. Необходимо указывать факт их наличия в протоколе осмотра с указанием следующих данных:

- место нахождения флеш носителя цифровой информации;
- его идентифицирующие типы;
- индивидуализирующее название;
- маркировочные обозначения, серийные номера.

Также на месте правонарушения, кроме персонального компьютера могут находиться сотовые телефоны, в памяти которых могут остаться цифровые следы события правонарушения. Данная информация описывается в протоколе осмотра с указанием сведений, аналогичных сведениям, приводимым при обнаружении флеш носителей цифровой информации.

В случае осмотра следователю удалось включить сотовый телефон, и получен доступ к данным, которые в нем находятся, в протоколе осмотра в хронологическом порядке фиксируются все производимые в дальнейшем с устройством мероприятии.

В основном возникают ситуации, в которых в ходе проведении первичных следственных действий изымается сразу несколько сотовых устройств во включенном состоянии. Выключать их в таких случаях до осмотра нецелесообразно (отключение можно произвести в рамках изъятия SIM-карты),

т.к. при последующем включении потребуются коды блокировки (PIN-код), которые могут быть известны только его последнему пользователю (подозреваемому, свидетелю или потерпевшему).

Следует обратить внимание на то, что отказ в предоставлении данных по разблокировке мобильного телефона может задержать возможность оперативного полноценного исследования его файлового содержимого (записной книжки, входящих, исходящих и непринятых звонков, СМС-сообщений GSM, WhatsApp и Viber связи, E-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера). Тем самым необходимо отметить, что если к моменту осмотра сотовый телефон было отключено, то конструктивный осмотр следует проводить только после анализе его информационной среды.

Осмотр информационной среды начинается с указания в протоколе осмотра процедуры разблокировки клавиатуры сотового телефона, перечисления графических и текстовых элементов, отображаемые на его экране после разблокировки. Затем осуществляется проверка IMEI-номера сотового устройства нажатием комбинации клавиш *#06# (пятнадцатизначный номер должен отобразиться на экране сотового телефона).

Если сотовый телефон не защищен pin кодом, то в протоколе осмотра последовательно указывается информационное содержимое (записная книга, сообщений мессенджеров, изображений, фотогалерей, видеороликов и т.д.).

Отметим, что в настоящее время правоохранительные органы обеспечиваются специальной высокотехнологичной криминалистической техникой, позволяющей извлечь необходимую информацию (включая онлайн) из сотового телефона, а также электронных накопителей (карт памяти, SIM-карт и др.) в ходе досудебного расследования. Например: универсальное устройство извлечения судебной информации (UFED - Universal Forensic Extraction Device, мобильный криминалист МК Enterprise, XRY, MOBILedit и др.).

Однако указанная криминалистическая техника дает возможность работать с любой моделью сотового телефона, гаджетов, навигаторами и персональными компьютерами, в том числе со сломанными устройствами, на основе любой операционной системы, а также позволяет войти в операционную систему в обход распознавая кодов и логинов, работать с гаджетами без аккумулятора, либо отдельно с SIM-картой.

Поэтому в случае если доступ к информационной среде мобильного телефона затруднен, то для участия к осмотру необходимо привлечь специалиста (ч. 6 ст. 220 УПК Республики Казахстан) [25], имеющего навыки пользования данными устройствами.

Таким образом, выявления, изучения, фиксация и изъятия в установленном законом порядке цифровые объекты, следы и информации из сотового телефона (гаджета) позволяют:

- напрямую выявлять лицо в совершении правонарушения (интернет - мошенничества);

- косвенно указывать на линию поведения лица, причастного его к совершенному правонарушению (интернет - мошенничества);

- способствовать установлению иных обстоятельств, имеющих значение для уголовного дела.

В заключительном этапе осмотра информационной среды сотового телефона проводится поэтапная детальная фото, видеосъемка экрана сотового телефона с информацией, представляющей значение для дела. Для визуальной фиксации большого объема сведений, содержащихся в информационной среде, следует применять видеозапись.

Также следователь в обязательном порядке комментирует с параллельной фиксацией в протокол осмотра все следственные действия, направлены на получение необходимой информации с помощью соответствующих мероприятий.

Тактика и технология обыска (в жилище, в ином помещении)

В качестве отыскиваемых в ходе обыска орудий правонарушения, предметов, относящихся интернет - мошенничеству, является средства сотовой связи, цифровые носители информации и иные носители информации, содержащие следы события, подлежащего расследованию.

При производстве обыска следует иметь в виду, что современные носители информации могут интегрированы в различные предметы (флэшки, наручные часы, кулон, телевизоры OLED и т.п.). Тем самым обыск необходимо проводить с применением специальных технических средств (приборов нелинейной локации), позволяющих обнаружить сотовые устройства и электронные накопители в помещениях, автомобилях, в том числе при досмотре людей или личном обыске.

Индивидуальная тактика обыска выбирается следователем в зависимости от характера и способа совершенного интернет - мошенничества, условий расследуемой ситуации. При этом следователю необходимо обращать внимание на место нахождения и возможного сокрытия цифровых устройств и в особенности извлекаемых из них накопителей (например, флэш и SIM-карты), а также на поведение участников обысков, пытающихся противодействовать расследованию или уничтожить улики с помощью магнита и т.д. Если в ходе обыска были предприняты попытки уничтожить или утаить мобильные устройства (уничтожить информацию, хранящуюся в их карте памяти), то об этом в протоколе делается соответствующая запись, и указываются принятые меры.

Выемка (предметов - электронных носителей информации, электронной почтовой корреспонденции*)*

Проведение выемка необходимы в целях изъятия цифровых носителей, содержащих файлы с искомым текстовым и графическим содержимым, а также программы, применяемых для подготовки и совершения правонарушений указанной категории. Такие носители информации в основном находятся в

персональных компьютерах, гаджетах лиц, подозреваемых в совершении правонарушения.

Необходимо отметить, что целенаправленное и полное изъятие «традиционных» файлов на бумажном носителе осуществить достаточно затруднено, поэтому лицо ведущее дело может лишь определить состав и объем изымаемых файлов. Практика показывает, что достаточно часто встречаются случаи, когда в ходе выемки изымается большой объем файлов. Тем не менее, далее следователь понимает, что многие файлы не содержат необходимую информацию, относящуюся к событию правонарушения.

Тем самым в начале, выемкой важно проконсультироваться со IT специалистом, компетентным сотрудником в финансовых операциях, проводимых с помощью электронных платежных систем, а также в инновационных компьютерных технологиях, для определения, какие файлы положенные изъятию. Такого рода консультация позволит следователю повысить эффективность данного следственного действия, исключить выемку ненужных файлов, одновременно изъять файлы, действительно содержащие доказательственную информацию по уголовному делу.

Отметим, что на практике встречаются случаи, когда выемка подменяется истребованием необходимых документов, что может привести к тому, что заинтересованные лица получат возможность удалить или частично удалить искомые файлы, либо заменить их другими. Тем самым подмена выемки истребованием документов крайне, отрицательна.

В случае при производстве выемки в известном следователю месте необходимых файлов не оказалось, то действия по их выявлению в других местах на основании того же постановления будут незаконными, а собранные таким образом доказательства недопустимыми. В данном случае необходимо незамедлительно вынести постановление о производстве обыска и произвести его для выявления скрываемых файлов, причем выемка не будет являться частью обыска, а будет представлять собой самостоятельное следственное

действие, в результате которого составляется отдельный протокол, в котором подробно отображаются ее ход и результаты.

В условиях производства выемки и обысков по делам интернет - мошенничества главные трудности возникают при изъятии персональных компьютеров в кредитной ином предприятии. Тем самым в процессе подготовки к производству выемки, в ходе которых следователь намерен изъять персональные компьютеры, необходимо изначально установить место, в котором находится необходимый персональный компьютер, а также обнаружения данных о его подключении к сети Интернет. При подключении к сети Интернет персонального компьютера в режиме онлайн, то необходимо учитывать возможность срабатывания программных средств уничтожения данных на его носителях при отключении от сети Интернет.

В данных условиях все мероприятия по корректному отсоединению от сети Интернет и выключению средств компьютерного устройства должны осуществляется IT специалистами, участниками следственного действия.

С учетом современных возможностей онлайн доступа к памяти цифровых устройств (сотовых телефонов) и расположенная в них электронных накопителей с целью уничтожения собственниками устройств через операторов связи информации, рекомендуется сразу же при обнаружении такого устройства помещать его в специальный чехол (например, «Мешок Фарадея», поставляемый в комплекте с универсальным устройством извлечения судебной информации UFED - Universal Forensic Extraction Device) [26].

В протоколе выемки следователю необходимо указывать, в каком месте и при каких обстоятельствах были обнаружены цифровые устройства, выданы они добровольно или изъяты принудительно. Все изымаемые цифровые устройства должны быть перечислены с точным указанием их количества, индивидуальных признаков, в том числе модели, серийных номеров, а в необходимых случаях стоимости. Также соответствующая запись делается в случаях, если по ходатайству законного владельца изымаемых электронных

носителей информации с разрешения следователя осуществляется копирование цифровой информации.

Тактика допроса (обвиняемого, подозреваемого, потерпевшего, свидетеля, специалиста, эксперта)

Прежде чем допрашивать подозреваемого, при расследовании интернет мошенничества следователю необходимо консультация специалиста в области IT-технологии (перед началом следственного действия), либо предусмотреть его непосредственное участие.

Допрос IT специалиста объясняет лицу осуществляющий досудебное расследование поставленным вопросам, и проводит транскрипцию сказанного иными участниками следственного действия (обвиняемым, подозреваемым, потерпевшим, свидетелем) с технического, насыщенного термином указанных лиц на язык, понятный другим участникам следственного действия (следователю, адвокату, прокурору, судье и т.д.).

Допрос судебного эксперта производится, в основном, для разъяснения данного им заключения. В данном случае также функция допроса заключается не только в раскрытии существенных деталей, не отраженных в выводах эксперта или аналитической части судебно-экспертного заключения, но и транскрипция написанного техническим языком на язык, понятный всем участникам следственного действия.

Одним из тактических приемов допроса, применяемых при расследовании много-эпизодных интернет - мошенничеств, совершенных организованным преступным сообществом, является процессуальное соглашение.

Как следует из закрепленного законодателем в п. 37 ст. 3 УПК Республики Казахстан определения, «процессуальное соглашение – соглашение, заключаемое между прокурором и подозреваемым, обвиняемым или подсудимым на любой стадии уголовного процесса или осужденным в порядке и по основаниям предусмотренным настоящим Кодексом».

Указанное процессуальное действие как тактический прием применяется прокурором, для получения развернутых показания от одного из соучастников организованной преступной группировки, содействующие в досудебном расследовании интернет - мошенничества, в раскрытии и уголовном преследовании других участников правонарушения, розыске похищенных денежных средств.

Организация негласных следственных действий

Негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации – это негласные следственные действия (далее - НСД), без предварительного информирования лиц, интересов которых оно касается, с последующим документированием уполномоченными подразделениями правоохранительных или специальных государственных органов.

Указанные следственные действия проводятся путём перехвата и снятия знаков, сигналов, голосовой информации, письменного текста, изображений, видеоизображений, звуков и другой информации, передающейся по проводной, радио, оптической и другим электромагнитным системам [27].

Порядок проведения данного следственного действия на сетях электросвязи, используемых для услуг передачи данных электрической (телекоммуникационной) связи, включая сети Интернет, регламентировано совместным приказом Министра внутренних дел Республики Казахстан «Об утверждении Правил проведения негласных следственных действий» от 12 декабря 2014 года № 892 (далее - Правила НСД) [28].

Негласные следственные действия осуществляется только на основании санкции следственного судьи с использованием оперативно-технических сил и средств уполномоченных подразделении правоохранительного или специального государственного органа [29].

Согласно Правилам НСД в соответствии со ст. 232 УПК Республики Казахстан, за исключением негласного контроля почтовых и иных

отправлений, следователь направляет поручение на проведение НСД оперативным подразделениям для документирования с использованием форм и методов оперативно-розыскной деятельности [30].

Таким образом, продуманное и полное документирование поручения на проведение НСД, увеличивает оперативность и шансы на установление и задержания интернет мошенников. В данном случае нами рекомендуется установление анкетных данных подозреваемого интернет - мошенника, который, как правило, используют легкодоступные средства анонимизации в сети Интернет (например, VPN - виртуальная частная сеть). В данном случае нам необходимо понять, что такое IP-адреса и средства анонимизации в сети (VPN).

Изучение работы IP-адрес, является важным для следователя при составлении поручения на проведение НСД в расследование интернет мошенничества, так как во многих мошеннических схемах используются сети Интернет.

IP-адрес – это уникальный идентификационный номер, который присваивается каждому компьютеру при подключении в сеть Интернета. Он представляет собой последовательность из 4 цифр в диапазоне от 0 до 255, чередующихся через точку. Например, 192.168.242.225 [31].

Интернет провайдер выдает каждому персональному устройству IP-адрес в момент начала интернет сессии – открытия первой интернетстраницы, и заканчивается закрытием интернет-сессии – закрытием последней интернет-страницы [32].

Таким образом, на каждом сайте («OLX», «krisha.kz», «kolesa.kz» и т.д.) хранятся истории соединений с его пользователями, следовательно и их IP-адреса. При каждом выходе в интернет - мошенник оставляет свой «цифровой след», по которому его можно вычислить.

Каждому интернет провайдеру выделено определенное количество IP-адресов в конкретном диапазоне, со своими ресурсами нумерации. При помощи

интернет ресурса https://2ip.ru/whois/#result-anchor, зная IP-адрес, можно легко определить провайдера.

При установлении IP-адреса и время его нахождения в сети Интернет, следователь может узнать, где находится персональный компьютер или гаджет, с которого работал интернет - мошенник (номер квартиры, дома и т.д.)

Тем, не менее, интернет - мошенники при совершении правонарушении используют средства анонимизации в сети Интернет - VPN (виртуальная частная сеть). VPN виртуальная частная сеть - это сервер третьих лиц, локализующегося на территории зарубежного государства, где при использовании VPN, установить IP-адреса интернет мошенников практический невозможно.

Однако, способы установления лиц, совершающие интернет мошенничество с помощью виртуальной частной сети VPN, есть, например, Cookie-файлы. Cookie-файлы – это фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя [33].

Например, при поиске в веб-браузерах «Google» или «Яндекс» определенного типа товара (купить запчасти на автомобиль), веб-браузер начинает выдавать рекламу именно о нем. Причина в том, что многие Интернет сайты сохраняют информации о своих пользователях (логин, ключи, пороли для быстрого доступа к веб-сайтам).

Сбор и анализ этой информации происходит посредством Cookie-файлов. Cookie-файлы веб-браузеров передают информацию своего нового пользователя, чтобы «сохранить» его, где при повторном посещении данного сайта, сайт будет знать о подключившемся пользователе ряд информации.

Особенностью Cookie-файлов является его неизменность, где интернет - мошенник может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но сайт все равно поймет, что все это время к нему подключается один и тот же пользователь, то есть используется веб-браузер одного и того же персонального компьютера.

Имея изначально информацию лишь по одному объявлению интернет-мошенника, с помощью анализа Cookie-файлов возможно, получить сведения по всем объявлениям, размещенным интернет - мошенником.

Следователю целесообразно проанализировать все объявления интернет - мошенника для установления реальных объявлений, выложенных с данного персонального компьютера (гаджета), с указанием личных IP-адресов и личного абонентского номера.

Установив анкетные данные владельца персонального компьютера или гаджета подозреваемого в совершении интернет - мошенничества, следователь выносит поручение на проведение одного или нескольких видов НСД.

Все вышеуказанное дает возможность оперативному сотруднику в короткие сроки вынести постановление на проведение НСД и обосновать следственному судье о необходимости проведения НСД, для санкционирования.

Таким образом, следует отметить следующее:

1. Вопросы расследования и производства следственных действий по уголовным правонарушениям в сети Интернет требуют тщательного анализа поступающей первоначальной информации, индивидуального и творческого подхода к каждому факту совершенного правонарушения, первоначальных познаний в сфере IT-технологии;

2. В целях повышения эффективности расследования уголовных в сети Интернета в оперативно-следственных подразделениях правоохранительных органов следует создать специализированные группы (отделы) для раскрытия и расследования дел данной категории, с обязательным учетом специалиста-эксперта. (Использование современных экспертно-аппаратных программных комплексов позволяющих восстанавливать историю работы ПК, скопированные, удаленные файлы и др.);

3. В связи с появлением новых технологий и методов совершения уголовных правонарушений в сети Интернет, повышение квалификации

сотрудников правоохранительных органов (курсы, тренинги), осуществляющих деятельность по их выявлению и расследованию, проводить на непрерывной основе.

3. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ КАК УСЛОВИЕ ОПТИМИЗАЦИИ И КАЧЕСТВЕННОГО РАССЛЕДОВАНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

3.1. Формы использования специальных знаний при расследовании интернет-мошенничества

При досудебном расследовании правонарушений в сфере интернет – мошенничества привлекаются различные специалисты и эксперты, в том числе криминалисты. Привлечение специалистов особых затруднений у следователей не вызывает, вместе с тем необходимо отметить, что исследование новых персональных гаджетов (ноутбуки, смартфоны), могут представлять некоторые затруднения, так как их операционная система ежегодно обновляются. Это объясняется отсутствием соответствующих отработанных методик исследования ее видов.

Тем самым необходимо отметить, что при досудебном расследовании интернет – мошенничества привлечение специалистов и методика исследования и назначений по ним экспертизы ежегодно будет меняться, в зависимости от схемы совершения и механизма правонарушения.

Возможности использования специальных познаний в ходе расследования правонарушений в сфере интернет - мошенничества

В ст. 7 Разъяснение некоторых понятий, содержащихся в уголовно-процессуальном кодексе определение понятию «специальные знания» дается как – не общеизвестные в уголовном процессе знания, приобретенные лицом в ходе профессионального обучения либо практической деятельности, используемые для решения задач уголовного судопроизводства [25].

Ученые юристы-процессуалисты под данным термином определяют как систему прикладных навыков и теоретических знаний в области технической науки, например, искусства, высоко-числительной техники и т.д., приобретаемых путем профессионального опыта, специальной подготовки,

привлекаемых для решения вопросов в досудебном и гражданском процессе [34]. Специальные знания в области цифровых технологий, имеют следующие направления: электротехника; телекоммуникационные системы; информационные системы; вычислительная техника (разработка программ).

Судебная экспертиза в досудебном производстве применяет основные формы научно-технических достижений. Основная работа судебной экспертизы является исследование по указанию следователя (применительно к стадии досудебного расследования) экспертом, направляемых к нему материалы (улик), также различные файлы (документы) и протокола следственных действий, для выявления фактических данных, имеющих значение для дела.

Процессуальной формой использования специальных знаний при расследовании интернет – мошенничества, является привлечение IT специалиста к досудебному расследованию, где IT специалист использует свои опыт для содействия следователю в обнаружении, закреплении и изъятии вещественных доказательств. Также, IT специалист обращает внимание следователя на обстоятельства, связанные с обнаружением и закреплением цифровых доказательств, дает пояснения в рамках специальных вопросов, возникающих при следственных действиях. Информация о фактах, установленных IT специалистом путем непосредственного наблюдения, фиксируются в протоколе осмотра правонарушения, обыска и выемки, которые являются источниками неопровержимых доказательств.

В условиях если лицо ведущий расследование обладает специальными знаниями и соответствующими научно-техническими средствами, он может проводить такие следственные действия как (осмотр, обыск и выемка) без помощи IT специалиста. Однако, закон обязывает его участие в следственных действиях.

Лицо, имеющее специальными знаниями в области цифровых технологий, может участвовать в следственных действиях для уточнения

вопросов применения специальных компьютерных оборудований в конкретной ситуации, а также для решения частных задач и путей их преодоления.

Важность привлечения IT специалиста, можно проследить в оказании помощи следственно-оперативной группе в подборе понятых, в качестве которых рекомендуется привлекать лиц имеющих познания в области цифровых технологий, так как такие понятые смогут правильно воспринять производимые следователем и специалистом действия с персональными компьютерами и гаджетами.

В подготовительном этапе следственного действия, следователю необходимо удостовериться в компетентности специалиста в области цифровых технологий. В случае выезда на осмотр место происшествия специалиста с государственного экспертного учреждения, руководство данной организации самостоятельно решают в их компетентности.

В рабочем этапе следственного действия (осмотр места происшествия), следователю необходимо озадачить специалиста в выявлении в персональных устройствах (программные обеспечения), файлы, переписки в мессенжерах (WhatsApp, Viber, Telegram, WeChat, Skype, Line и т.д.), имеющие криминалистически значимую информацию. Участникам следственно-оперативной группе необходимо особое внимание уделять по корректному обесточиванию персональных компьютеров и гаджетов, также специалист под протокол следователя визуально описывает все цифровые технологий, их отдельные детали и соответствующей файлы.

При производстве обыска либо выемки IT специалист участвует в определении вопроса комплектации выявленных цифровых средств, уточнении отдельных деталей, подлежащих изъятию. В данном случае IT специалист также непосредственно проводит корректное отключение работающего программного обеспечения и отключение гаджетов от питания электричеством, помогая следователю описать изымаемые программные средства. Также, IT

специалист принимает участие в упаковке, опечатывании выявленных улик и подготовке их к перевозке и хранению согласно образцу.

ОБРАЗЕЦ

ПОСТАНОВЛЕНИЕ

о производстве выемки

город Нур-Султан 01.01.2022 года

Следователь СО УП района «Есиль» ДП города Нур-Султана старший лейтенант полиции Мамешов Ж., рассмотрев материалы уголовного дела, зарегистрированного в ЕРДР за №211111011000116,

УСТАНОВИЛ:

Обстоятельства дела: в период с 10.01.2021 года по 01.11.2021 года, неизвестное лицо, находясь в неустановленном следствию месте, обманным путем злоупотребляя доверием, пользуясь интернет ресурсами оформило микро займы в различных компаниях от имени Махановой А. 01.01.1986 г.р., на общую сумму 300 000 тенге, тем самым причинив последней материальный ущерб.

По данному факту в УП района «Есиль» ДП г.Нур-Султана начато досудебное расследование, зарегистрированное в ЕРДР за №211111011000116 по ст.190 ч.2 п.4 УК РК *(интернет - мошенничество)*.

В ходе досудебного расследования установлено, что у Жасмоновой А, 01.01.2001 года рождения имеется выписка по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, имеющая доказательственное значение по уголовному делу.

На основании изложенного, руководствуясь ст. 198, 253, 254 УПК Республики Казахстан,

ПОСТАНОВИЛ:

1. Произвести у Жасминовой А., 01.01.2001 года рождения в присутствии представителя выемку выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года.
2. О принятом решении уведомить заинтересованных лиц;
3. Копию настоящего постановления направить прокурору района «Есиль» города Нур-Султана.

Следователь следственного отдела
УП района «Есиль» ДП г. Нур-Султана
старший лейтенант полиции **Мамешов Ж.**

ОБРАЗЕЦ

Протокол

выемки

город Нур-Султан 01.01.2022 года

Начата: в «_13_» часов «_10_» минут
Окончена: в «_13_» часов «_25_» минут

Следователь СО УП района «Есиль» город Нур-Султана старший лейтенант полиции Мамешов Ж., находясь в кабинете № 107 здания УП района «Есиль» ДП города Нур-Султан, по адресу город Нур-Султан, улица Орынбор, д.9, с соблюдением требований ст.ст. 199, 253, 254, 256 УПК РК, с применением фотофиксации на фотоаппарат марки «Samsung», произвел

выемку выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года у Жасминовой А. в присутствии представителя.

Перед началом следственного действия всем лицам, участвовавшим в производстве следственного действия, разъяснено их право делать замечания, подлежащие внесению в протокол; знакомиться с протоколом следственного действия, в котором они участвовал.

Также они были уведомлены о том, что при производстве выемки будут применяться технические средства для фиксации хода и результатов следственного действия.

До начала производства выемки лицом, осуществляющее досудебное расследование предъявлено постановление о производстве выемки от 01.01.2021 года.

В ходе досудебного расследования установлено, что у Жасминовой А., 01.01.2001 года рождения имеется выписка по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, имеющая доказательственное значение по уголовному делу.

При производстве выемки Жасминовой А. предложено добровольно выдать выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, на что Жасминова А. добровольно выдала выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года на 5 листах формата А 4.

Изъятые предметы и документы в ходе выемки предъявлены присутствующим лицам, упакованы в бумажный конверт коричневого цвета, который(е) опечатан(ы) печатью «Пакеттер үшін» и заверен подписью следователя.

К протоколу прилагается фототаблица на 5 листах.

Поступившие в ходе выемки замечания: _____.

Лицо, у которого производилась выемка _____

Представитель _____

Следователь следственного отдела
УП района «Есиль» ДП г. Нур-Султана
старший лейтенант полиции **Мамешов Ж.**

Копию протокола получил _____

В ходе досудебного расследования IT специалист может проявить инициативу в поиске цифровых устройств, правонарушения применяя цифровые технические средства. Вместе с тем важно, чтобы общие задачи проводились и под контролем следователя. В ходе следственного действия IT специалист в рамках своей компетенции имеет право предоставлять следователю и другим участникам следственно-оперативной группы справочные сведения и разъяснять вопросы, связанные с гаджетами и современными цифровыми технологиями.

Специальные знания могут использоваться не только в процессуальной форме, когда результаты их применения имеют доказательственное значение, но и в непроцессуальной форме.

Непроцессуальной формой использования специальных познаний является справочно-консультационная деятельность сведущего лица - IT специалиста не в процессуальном, а в более широком смысле этого слова. В этой форме IT специалист может оказывать помощь следователю в подготовке следственных действий и материалов для экспертизы, формировании вопросов эксперту и т.д.

Справочно-консультационная работа может осуществляться как до, так, и в, процессе досудебного расследования. В основном она необходима следователю до регистрации дела в ЕРДР или подготовительном этапе касающихся получения общих сведений о персональных компьютерах.

Процесс исследования персональных компьютеров и гаджетов в практике борьбы с интернет – мошенничеством может осуществляться как до, так и после регистрации в ЕРДР уголовного дела.

При проведении такого неотложного следственного действия как осмотр места происшествия с привлечением специалиста в досудебном расследовании интернет – мошенничества, специалист может установить:

- о механизме совершения правонарушения;

- о способе его совершения и сокрытия правонарушения;

- об специальных цифровых средствах;

- о непосредственном контакте интернет - мошенника с предметами обстановки места происшествия.

Предварительное исследование и привлечение специалиста при проведении неотложных следственных действий, как осмотр места происшествия способствует выдвижению следственно-оперативных версий, определению на поручение негласных следственных действий.

Также необходимо отметить, что при производстве предварительного исследования персональных технических средств и гаджетов, специалисту и следственно-оперативной группе необходимо быть осторожными, т.к. интернет – мошенники, могут воспользоваться вирусными программными средствами имеющие свойства самоуничтожения.

Особенности осмотра и изъятия персональных устройств и гаджетов

Для необходимости быть уверенным следователю в сохранности цифровых следов и необходимых данных по интернет – мошенничеству, во избежание утери или повреждения необходимых файлов, надо запланировать неотложное следственное действие, на подготовительном этапе.

Эффективный осмотр места происшествия персональных устройств и гаджетов следователем, начинается с подготовительного этапа. Первоначально

следователю надо изучить план расположения сети и связь между ними, также надо выяснить систему безопасности.

Профессор Н.П. Яблокова, в своих трудах отмечал, что в случаях возникновения нештатных ситуации при расследовании правонарушений совершенные с использованием информационной системы, следователю необходимо привлекать специалиста [35].

При осмотре места происшествия вероятность потери улик в персональных устройствах и гаджетах увеличивается при отсутствии специальных знаний. Этим и связано привлечение специалиста в области программирования, который способен профессионально обнаружить и извлечь необходимые данные, имеющий доказательное значение.

Ф.Г. Аминев в своих трудах отмечает, что «в документировании правонарушении, в описании персональных устройств и гаджетов специалисты оказывают неоценимую помощь, но для проведения дальнейших действий (изъятия, фиксация и упаковка объектов) их специальных знаний недостаточно» [36]. Правильная упаковка улик является необходимым и важным действием для сохранности вещественных доказательств. Ученые процессуалисты отмечают, что отсутствие навыков правильной упаковки может привести к необратимым последствиям, так например, при несоответствующей упаковке, ненадлежащим хранении цифровых микросхемы (накопителей), поступивших на судебно-экспертное исследование, могут быть уничтожены статическим электричеством (возможно, от шерстеной одежды) [37], что может повлечь к их уничтожению.

Рассмотрим несколько способов выемки цифровой информации при расследовании интернет – мошенничестве:

1. Выемка цифровой информации с носителем информации вместе.

Их можно разделить на два варианта:

А) Выемка носителя цифровой информации отдельно (магнитный диск, оптический диск, жесткий диск, флеш-карта и др.)

Б) Выемка системы цифрового устройства (устройство чтения и записи оптических дисков с оптическим диском внутри, системный блок с подключенным винчестером, принтер с установленной картой памяти принтера).

Указанный способ время затратное, где специалист обязан владеть знаниями аппаратной части компьютерных устройств.

Данный процесс наиболее применимый на территории, которая связано с надёжностью указанного способа (цифровая информация не изымается из общей информационной среды), работа его реализации (требует минимальное познание при снятии информации), итоги (возможностью обнаружения новых цифровых следов, которые лицо ведущий расследование не планировал изъять).

В данной ситуации изначальным вопросом, является решение следователем, по обесточиванию персонального компьютера (гаджета). Основной рекомендацией в данных условиях нет, следователю необходимо исходить из конкретной ситуации.

2. Интернет – мошенничество, было совершено в прошлом, с отсутствием оснований, что данное правонарушение совершается на данный момент, когда проводится досудебное расследование (обыск, выемка). В данных условиях вопросом, который необходимо решить следователю, по обесточиванию персонального компьютера (гаджета), второстепенным.

3. Интернет – мошенничество, с помощью вирусных программ, совершается на момент планируемого досудебного расследования (обыск, выемка), где следователю необходимо составить план следственного действия, по фиксации и изъятию цифровой информации

Порядок активизации подключенных специальных вирусных программ следователю необходимо согласовывать со IT специалистом. В протоколе следственного действия необходимо отражать следующее:

– установлено подключенное состояние персонального компьютера и зафиксирован порядок его отключения;

– описано место, где изымается персональный компьютер (гаджеты) и их связь между собой и окружающих предметов (с приложением необходимых фото и видео съемкой);

– описан порядок соединения между собой всех компьютеров (гаджетов) с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация, маркировочные обозначения);

–определено наличие либо отсутствие компьютерной локации, используемый канал (каналы) связи и телекоммуникаций;

– определен вид упаковки и транспортировки изъятых предметов.

ОБРАЗЕЦ

ПОСТАНОВЛЕНИЕ

о производстве выемки

город Нур-Султан 01.01.2022 года

Следователь СО УП района «Есиль» ДП города Нур-Султана старший лейтенант полиции Мамешов Ж., рассмотрев материалы уголовного дела, зарегистрированного в ЕРДР за №211111111000111,

УСТАНОВИЛ:

Обстоятельства дела: в период с 10.01.2021 года по 01.11.2021 года, неизвестное лицо, находясь в неустановленном следствию месте, обманным путем злоупотребляя доверием, пользуясь интернет ресурсами оформило микро займы в различных компаниях от имени Сериковой Н. 01.01.1981 г.р., на общую сумму 303 000 тенге, тем самым причинив последней материальный ущерб.

По данному факту в УП района «Есиль» ДП г.Нур-Султана начато досудебное расследование, зарегистрированное в ЕРДР за №211111111000111 по ст.190 ч.2 п.4 УК РК *(интернет - мошенничество)*.

В ходе досудебного расследования установлено, что у Жасминовой А., 01.01.2001 года рождения имеется выписка по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, имеющая доказательственное значение по уголовному делу.

На основании изложенного, руководствуясь ст. 198, 253, 254 УПК Республики Казахстан,

ПОСТАНОВИЛ:

1. Произвести у Жасминовой Асель, 01.01.2001 года рождения в присутствии представителя выемку выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года.

2. О принятом решении уведомить заинтересованных лиц;

3. Копию настоящего постановления направить прокурору района «Есиль» города Нур-Султана.

Следователь следственного отдела
УП района «Есиль» ДП г. Нур-Султана
старший лейтенант полиции **Мамешов Ж.**

ОБРАЗЕЦ

Протокол

выемки

город Нур-Султан 01.01.2021 года

Начата: в «_13_» часов «_10_» минут

Окончена: в «_13_» часов «_25_» минут

Следователь СО УП района «Есиль» город Нур-Султана старший лейтенант полиции Мамешов Ж., находясь в кабинете №101 здания УП района «Есиль» ДП города Нур-Султан, по адресу город Нур-Султан, улица Орынбор, д.9, с соблюдением требований ст.ст. 199, 253, 254, 256 УПК РК, с применением фотофиксации на фотоаппарат марки «Samsung», произвел выемку выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года у Жасминовой А. в присутствии представителя.

Перед началом следственного действия всем лицам, участвовавшим в производстве следственного действия, разъяснено их право делать замечания, подлежащие внесению в протокол; знакомиться с протоколом следственного действия, в котором они участвовал.

Также они были уведомлены о том, что при производстве выемки будут применяться технические средства для фиксации хода и результатов следственного действия.

До начала производства выемки лицом, осуществляющее досудебное расследование предъявлено постановление о производстве выемки от 01.01.2022 года.

В ходе досудебного расследования установлено, что у Жасминовой Асель, 01.01.2001 года рождения имеется выписка по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, имеющая доказательственное значение по уголовному делу.

При производстве выемки Жасминовой А. предложено добровольно выдать выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года, на что Жасминова А. добровольно выдала выписки по Каспий Голд за период с 10.01.2021 года по 01.11.2021 года на 5 листах формата А4.

Изъятые предметы и документы в ходе выемки предъявлены присутствующим лицам, упакованы в бумажный конверт коричневого цвета, который(е) опечатан(ы) печатью «Пакеттер үшін» и заверен подписью следователя.

К протоколу прилагается фототаблица на ____ листах.

Поступившие в ходе выемки замечания: **_____.**

Лицо, у которого производилась выемка _____

Представитель _____

Следователь следственного отдела
УП района «Есиль» ДП г. Нур-Султана
старший лейтенант полиции **Мамешов Ж.**

Копию протокола получил _____

Также необходимо отметить, что данные выводимые на экран персонального компьютера (гаджета), необходимо описывать, если для расследования это будет нужно, по согласованию IT специалистом.

При условии если на компьютере (гаджете) запущена не относящаяся интернет - мошенничеству программа, лицо ведущий расследование, с участием IT специалиста устанавливает, какая операционная система установлена на компьютере (гаджете), какие используются протоколы связи, службы доступа к файлам и сети Интернет. Лицом ведущий расследование исследуется вся информация на компьютере (гаджете), которое было задействовано в совершении интернет – мошенничества. Далее обнаруженные виртуальные программы, цифровые файлы и иные значимые информации для дела, IT специалист протоколирует и изымает. При необходимости, если это

рекомендует IT специалист, может изыматься весь персональный компьютер (гаджет) или компьютерный блок.

3.2. Судебные экспертизы при расследовании интернет - мошенничества: проблемы и перспективы

Назначение судебной экспертизы при расследовании интернет – мошенничестве следователь может согласно, главы 35 УПК Республики Казахстан, в рамках Закона Республики Казахстан «О судебно-экспертной деятельности» 10 февраля 2017 года [38].

При назначении судебной экспертизы лицо ведущие досудебное расследование не должны допускать, с одной стороны, необоснованного промедления, а с другой – неоправданной поспешности. Успех судебной экспертизы зависит во многом от полноты и своевременности представления следователем все необходимые объекты и образцы для проведения исследования, с правильно поставленными вопросами. Назначение на судебную экспертизу выносится немедленно после того, как собраны все необходимые для исследования объекты [39].

Лицу ведущий расследование, при назначении экспертизы, в условиях расследовании интернет – мошенничества, необходимо определять конкретные основания, предмет исследования, объекты и сведущее лицо (лицо, имеющее обширные познания в определенной сфере своей деятельности) или судебно-экспертное учреждение.

Вместе с тем, при расследовании интернет - мошенничества следователем назначаются следующие судебные экспертизы:

1) **Судебно-техническое исследование документов** – для исследования документов (их реквизиты и материалы), приспособления для составления документов (полных или отдельных фрагментов), либо для внесения изменений в ранее подготовленные документы, вещества для подготовки документов, либо для внесения изменений в ранее подготовленные документы.

2) **Судебно-экспертное исследование почерка и подписей** – для анализа почерковедческих текстов или их блоки, записи (цифровые или буквенные) и подписи, проведенные в стандартных или нестандартных для пишущего условиях, имеющий связь или не имеющий с намеренным изменением почерка в подлинниках документов.

3) **Судебно-экспертное бухгалтерское исследование** – для исследования и получения первоначального доказательства в ходе анализа хозяйственных операций.

4) **Судебная видеофонографическая экспертиза** – для анализа речевой и звуковой информации, зафиксированная на магнитном или цифровом носителе, средства звукозаписи, образцы для экспертного исследования, материалы дела, относящиеся к предмету анализа.

5) **Судебно-экспертное исследование средств компьютерной технологии** – для анализа разных видов компьютеров, ноутбуков (настольные, портативные, карманные и т.д.) с основными блоками (системные блоки, мониторы), внутренними узлами, деталями, комплектующими и т.д. [40].

Следователем при расследовании интернет – мошенничестве основной упор делается на судебно-экспертное исследование средств компьютерной технологии. Это обусловлено тем, что интернет – мошенник при совершении правонарушений применяет персональный компьютер (гаджет).

Объектами экспертизы являются:

1) Аппаратные объекты:

- разные виды компьютеров ноутбуков (настольные, портативные, карманные и т.д.) с основными блоками (системные блоки, мониторы), внутренними узлами, деталями, комплектующими и т.д. (далее – гаджеты);

- различного вида периферийных устройств и назначение;

- сетевые аппаратные средства (северы, рабочие станции, активное оборудование, сетевые кабели и т.д.);

- дисковые накопители данных (жесткие диски HDD, флоппи-диски FDD, оптические компакт-диски CD-ROM, CD-RW, DWD-ROM, флэш-карты USB).

2) Программные объекты:

- системное программное обеспечение (различные операционные системы для персональных компьютеров и локальных сетей MS-DOS, UNIX, Windows различных версий и т.д., вспомогательные программы – утилиты, средства разработки и отладки программ, служебная системная информация и т.д.);

- разные прикладные программные продукты (приложения общего назначения: текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций; приложения специального назначения для решения задач в определенной области науки, техники, экономики и т.д.).

3) Информационные объекты:

- файлы, подготовленные с использованием указанных выше и других программных средств (с расширениями текстовых форматов .txt, .doc, графических форматов .bmp, .jpg, .cdr, форматов баз данных .dbf, .mdb, электронных таблиц .xls, .cal и др.).

- данные в форматах мультимедиа.

4) Объекты, содержащие информацию, необходимую для производства экспертных исследований:

- различные файлы (договоры на покупку, создание (передачу) научно-технической продукции; акты сдачи-приема научно-технической продукции; калькуляции стоимости предпродажной подготовки компьютерной техники и периферийных устройств и пр.);

- сопроводительная документация к поставляемой на анализ компьютерной, вычислительной технике (периферийным устройствам, магнитным носителям), различные справочные данные, инструкции пользователя, а также материалы дел.

Задачи, решаемые в ходе данной работы, относятся к задачам диагностического, идентификационного, классификационного и ситуационного характера.

При провидении указанной экспертизы решаются следующие **вопросы:**

1) По аппаратным средствам:

- каковы технические характеристики представленные технические средства;

- имеет ли возможность использования представленного технического комплекса для осуществления тех или иных функциональных задач (например, выхода в сети Интернет, запись компакт-дисков);

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

2) По программным продуктам:

- какая операционная система установлена в системном блоке;

- имеется ли в указанном системном блоке установленное программное обеспечение (указать название);

- имеет ли указанное программное обеспечение в рабочем состоянии;

- каковы дата и время установки программного обеспечения (указать название);

- имеются ли в указанных системных блоках программы, приводящие к неправомерному доступу к охраняемой законом цифровой информации, внесению изменений в существующие программы, заведомо приводящих к незаконному уничтожению, блокированию, модификации либо сканированию данных, нарушению работы гаджетов;

- каковы основные функции представленного программного обеспечения;

- каково назначение представленных программ для ЭВМ;

- 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 средств, бланками юридических лиц и оттисками печатей);

- имеются ли на представленных магнитных носителях ранее удаленные файлы (указать названия);

- имеются ли на магнитном носителе какая-либо информация, если да, то каков вид ее представления;

- каково дата и время создания файлов (указать названия).

Исследование программно-технических технологий

Проводится специалистами-программистами, имеющими высшее образование и опыт работы с большим количеством пакетов программ.

Вопросы:

1. Какие текстовые документы (файлы) либо файлы бухгалтерской, банковской программы или базы данных по интересующей теме находятся на представленном компьютере (магнитном носителе)?

2. Какие текстовые документы (файлы) либо файлы бухгалтерской, банковской программы или базы данных по интересующей теме на представленном на компьютере (магнитном носителе) были стерты (уничтожены), каковы их имена, размеры и даты создания?

3. Как изменялось содержание документов, содержащихся в текстовых документах (файлах) либо файлах бухгалтерской, банковской

программы или базы данных по интересующей теме на представленном на компьютере (магнитном носителе)?

Особенности судебно-экспертное исследование средств компьютерной технологии

Характеристика систем обнаружения вторжений (далее - СОВ).

СОВ отличаются по ряду критериев. Установив данные критерии, специалист может установить, какие виды СОВ, вероятно, встретятся специалисту и как они функционируют. Прежде всего, СОВ можно различить, исходя из вида действий, трафика, операций или систем, которые они отслеживают. В этом условиях можно выделить три варианта СОВ: сетевые, хостовые системы и системы на основе приложения.

СОВ, которые проводят мониторинг сетевых магистралей и проводят поиск сигнатуры атак, именуются сетевыми системами; СОВ, работающие на гаджете, чтобы прикрывать и проверять операционную и файловую систему, называются хостовые системы.

СОВ, отслеживающие только работу отдельных приложений, называются системами на основе приложения. (Этот тип обработки в основном предназначен для важных приложений, таких как системы управления базами данных, системы управления содержимым, системы бухгалтерского учета и т. д.). Далее указана дополнительная информация о разных типах мониторинга в СОВ:

Характеристики сетевых СОВ

Положительно: Сетевые СОВ могут контролировать всю сеть с помощью нескольких устройств, не создавая нагрузку на сеть. Сетевые СОВ – это в основном пассивные приложения, отражающие текущую сетевую активность, не прибавляя значительное количество служебной информации или не создавая помех в работе сети. Их легко сохранить от атак, и иногда их даже не могут обнаружить атакующие. Вместе с тем, данные системы не

требуют огромных усилий для установки и использования в имеющихся сетях.

Отрицательно: Есть вероятность, что у сетевых СОВ нет возможности отслеживать и исследовать весь трафик в больших, интенсивно используемых сетях тем самым, могут не заметить атаки, предпринятые в периоды максимальной нагрузки. Также, сетевые СОВ могут не суметь проводить мониторинг в (высокоскоростных) сетях на основе коммутатора. В естественных условиях сетевые СОВ не могут анализировать зашифрованные данные, а также сообщать об положительных или отрицательных попытках атак. Таким образом, СОВ требуют обязательного участия системных администраторов, чтобы оценить результаты зафиксированной атаки.

В настоящее время большинство антивирусных программ имеют характеристики обнаружения, основанные как на анализе сигнатур, так и на анализе аномалий, но не все СОВ включают в себя оба подхода.

Некоторые СОВ имеют свойства реагировать на предпринятые атаки. Указанная реакция является по двум причинам.

Во-первых, гаджеты могут устанавливать поведение и активность в масштабе времени, близком к реальному, и реагировать активнее и решительнее на ранних стадиях атаки. Так как автоматизация дает возможность хакерам проводить атаки, само собой разумеется, что она должна помочь IT специалистам в области кибер безопасности защищать их.

Во-вторых, СОВ работают 24 часа в сутки, 7 дней в неделю, а сетевые администраторы не способны реагировать так же мгновенно в нерабочее время, как в часы пик (даже если система обнаружение отправит им сообщение о начавшейся атаке). Автоматизировав блокирование входящего трафика для одного или нескольких адресов, с которых предпринята атака, СОВ может остановить текущую атаку и блокировать будущие атаки с того же адреса.

Реализовав следующие приемы, СОВ может отразить атаки как любителей, так и знающих хакеров. Хотя знающих хакеров тяжелее блокировать полностью, эти приемы могут значительно замедлить их работу:

Разрыв TCP-подключений путем добавления пакетов с флагом сброса в соединение с хакером приводит к срывам атак.

Применение автоматизированных фильтров пакетов для того, чтобы блокировать перенаправление маршрутизаторами или брандмауэрами пакетов атаки на атакуемые серверы или хосты, останавливает большинство атак, даже атаки DoS или DDoS (распределенная атака типа «отказ в обслуживании»). Этот прием работает для адресов злоумышленников и для атакуемых протоколов и служб (блокированием трафика на разных уровнях сетевой модели ARPA).

Использование автоматического разъединения для маршрутизаторов, брандмауэров или серверов может завершить все действия, если другими средствами злоумышленников остановить не удалось. (Например, в крайних ситуациях при атаке DDoS, когда фильтрация эффективно работает только на стороне поставщика услуг Интернета, а то и выше по цепи провайдеров, как можно ближе к магистралям Интернета).

Активное выполнение обратного поиска DNS или других попыток установить личность хакера – это метод, используемый некоторыми СОВ, которые отправляют отчеты о вредоносных действиях всем поставщиками услуг Интернета на маршрутах между атакующим и атакуемым. Так как такие ответные меры могут сами установить спорные вопросы, подлежащие правовому разрешению, рекомендуется получить консультацию юриста, прежде чем отплатить хакерам той же монетой [41].

В заключении отметим, что методика и тактика судебно-экспертного исследования средств компьютерной технологии ежегодно обновляется, вместе с появлением совершенно новых программных обеспечений. Тем самым следственно-оперативным органам значительно, сложно с вынесением

постановления на судебно-экспертное исследование средств компьютерной технологии, так как новые программные обеспечения имеют свои возможности и системы безопасности, тем самым затрудняя вопросы необходимые на постановку судебному - эксперту. Для наиболее эффективного расследования уголовных дел в сфере интернет - мошенничества особенное внимание должно быть уделено вопросам использования помощи IT специалистов и экспертов в вопросах назначения и производства судебно-экспертного исследования средств компьютерной технологии.

ЗАКЛЮЧЕНИЕ

В заключении следовало бы выделить некоторые концептуально важные моменты диссертации.

Знание общих положений криминалистической характеристики интернет - мошенничества, совершаемые в сети интернет, позволяет предметно разрабатывать следственно-оперативные версии и осуществлять целенаправленные отдельные следственные действия по их проверке, так как обстоятельства, образующие данную характеристику, находятся в закономерных связях между собой (системно-структурных, функциональных и т.д.). Основными (базовыми) элементами интернет - мошенничества, совершаемые в сети интернет:

- объект, предопределяемый предметом правонарушений;
- средства правонарушений;
- субъект правонарушения (личность интернет - мошенника).

Наличие закономерных связей между обстоятельствами (элементами) криминалистической характеристики интернет - мошенничества, совершаемых в сети интернет, не исключает особенностей каждого конкретного факта правонарушения. Данные особенности, вместе с выявленными закономерностями, образуют систему, влияющие на производства досудебного расследования.

Реализация на территории Республики Казахстан подобные ИБД по «Интернет-мошенничество», даст возможность правоохранительным органам, анализировать и выявлять многоэпизодные правонарушения и правонарушения прошлых лет, путем идентификации способа совершении интернет-мошенничество (даты, период и место зарегистрированных заявлений и сообщений).

Отметим, что вышеуказанный перечень должна быть адаптирована, на постоянное расширение данных, к новым методам совершения интернет-мошенничество.

Пришло время рассмотреть вопрос разработки Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам в сфере информатизации и связи». Так как на сегодняшний день при изучении материалов уголовных дел по преступлениям совершенные в сфере информатизации и связи, нет единой практики вопросов квалификации и методики и тактики расследования, например, интернет – мошенничество, киберпреступления, интернет – хищение и т.д.

Вопросы расследования и производства следственных действий по уголовным правонарушениям в сети Интернет требуют тщательного анализа поступающей первоначальной информации, индивидуального и творческого подхода к каждому факту совершенного правонарушения, первоначальных познаний в сфере IT-технологии;

В целях повышения эффективности расследования уголовных в сети Интернета в оперативно-следственных подразделениях правоохранительных органов следует создать специализированные группы (отделы) для раскрытия и расследования дел данной категории, с обязательным учетом специалиста-эксперта. (Использование современных экспертно-аппаратных программных комплексов позволяющих восстанавливать историю работы ПК, скопированные, удаленные файлы и др.);

В связи с появлением новых технологий и методов совершения уголовных правонарушений в сети Интернет, повышение квалификации сотрудников правоохранительных органов (курсы, тренинги), осуществляющих деятельность по их выявлению и расследованию, проводить на непрерывной основе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года N 94-V. https://adilet.zan.kz/rus/docs/Z1300000094

2. Конституция Республики Казахстан принята на республиканском референдуме 30 августа 1995 года. https://adilet.zan.kz/rus/docs/K950001000_

3. Справка по состоянию судебно-следственной практики по делам о мошенничестве г. Нур-Султан 20 ноября 2019 г.

4. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. https://adilet.zan.kz/rus/docs/K1400000226

5. Вехов, В.Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: моногр. / В.Б. Вехов.– Волгоград: ВА МВД России, 2005.

6. Вехов, В.Б. там же...

7. Данные Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан о зарегистрированных преступлениях, предусмотренных п.4 ч.2 ст. 190 УК РК. https://qamqor.gov.kz/portal/page/portal/POPageGroup/MainMenu

8. Мусин А.Б. Особенности расследования преступлений, совершаемых путем обмана и злоупотребления доверием пользователя информационных систем торговых объявлений и социальных сетей. Дисс…на соискание степени магистр. –Костанай, 2021. – 106 с.

9. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий. https://incashwetrust.biz/organizacija_rassledovanija_hishhenij_denezhnyh_sredstv.html

10. Яблоков Н.П. Криминалистика: Учебник. 2-е изд., перераб. и доп. М., 2008. С. 17.

11. Медиев Р.А., Секенова Б.Б. Методические рекомендации по вопросам расследования и производства следственных действий по уголовным правонарушениям в сети Интернет. —Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2021. —21 с.

12. Данные Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан о зарегистрированных преступлениях, предусмотренных п.4 ч.2 ст. 190 УК РК. https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat

13. Книга учета информации (КУИ) – автоматизированная база данных, в которую вносятся любая информация об уголовном правонарушении, включая поводы к началу досудебного расследования, перечисленных в ч.1 ст. 180 УПК РК от 04.07.2014г. // Приказ Генерального Прокурора РК № 89 от 19.09.2014 г. «Об утверждении Правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также введения ЕРДР» // Просмотр сайта на 09.04.2015г. www.prokuror.gov.kz

14. Архив уголовного дела № 21151003100092

15. Постановление Республики Казахстан № 4718-19-00-1/64

16. Приговор именем Республики Казахстан от 23 июля 2019 года №7116-19-00-1/397 город Нур-Султан

17. «Президентскую премию» предлагал мошенник в Акмолинской области. https://timeskz.kz/58872-prezidentskuyu-premiyu-predlagal-moshennik-v-akmolinskoy-oblasti.html

18. Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам о мошенничестве» № 6 от 29 июня 2017 года

19. Методические рекомендации «разграничение гражданско-правовых споров от мошенничеств, в том числе совершенных с формальным заключением сделок». – Нур-Султан, 2020. – 10 с.

20. Инструкция по организации надзора за законностью уголовного преследования, утвержденной приказом Генерального Прокурора Республики Казахстан от 12 февраля 2018 года.

21. МВД России Главное Управление Министерства внутренних дел Российской Федерации по городу Москве (ГУ МВД России по г. Москве) Приказ от 05 Апреля 2021 г. № 121

22. Уголовно-процессуальный кодекс Российской Федерации https://www.zakonrf.info/upk/

23. Тактика осмотра места происшествия по делам о незаконном обороте наркотиков https://dspace.susu.ru/xmlui/bitstream/handle/0001.74/13523/2016_662_smarchkov.pdf?sequence=1&isAllowed=y

24. Belkasoft X - Надёжное решение для комплексной цифровой криминалистической экспертизы и расследования корпоративных инцидентов. https://belkasoft.com/ru

25. УПК Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. http://adilet.zan.kz/rus/docs/K1400000231

26. Выемка электронных носителей информации https://si-center.ru/info/vyemka-jelektronnyh-nositelej-informacii/

27. Совместный приказ Министра внутренних дел Республики Казахстан «Об утверждении Правил проведения негласных следственных действий» от 12 декабря 2014 года № 892 https://adilet.zan.kz/rus/docs/V14C0010027

28. Медиев Р.А., Сулейманова Г.Ж. Негласные следственные действия в теории и практике органов уголовного преследования Республики Казахстан Монография. —Актобе: Актюбинский юридический институт МВД РК им. М. Букенбаева, 2017. — 200 с.

29. Медиев Р.А., Сулейманова Г.Ж. там же...

30. Закон Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года № 154-XIII https://adilet.zan.kz/rus/docs/Z940004000_

31. Словарь терминов интернет-рекламы и SEO https://www.russianpromo.ru/wiki/ip-adres/

32. Материал из Википедии — свободной энциклопедии https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5% D1%81

33. Материал из Википедии — свободной энциклопедии. https://ru.wikipedia.org/wiki/Cookie

34. Вехов, В.Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов [Текст]: моногр. / В.Б. Вехов.– Волгоград: ВА МВД России, 2005.

35. Криминалистика: Практикум / Под ред. Н. П. Яблокова. М.: Юристъ, 2004. – С. 518.

36. Смирнова, С. А. Судебная экспертиза на рубеже XXI века. Состояние, развитие, проблемы. Изд. 2-е, перераб. и дополн. СПб.: Питер, 2004. – С. 355.

37. Смирнова, С. А. там же…

38. Закон Республики Казахстан от 10 февраля 2017 года № 44-VI «О судебно-экспертной деятельности» (с изменениями по состоянию на 29.06.2020 г.).

39. 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

40. Справочник для правоохранительных, специальных органов и судов по вопросам назначения судебных экспертиз в Центр судебной экспертизы Министерства юстиции Республики Казахстан, Астана, 2016

41. Крис Поуг, Кори Алтеид, Тодд Хаверкос Криминалистическое исследование Unix и Linux. file:///D:/1.%20%D0%A1%D0%95%D0%9A%D0%95%D0%9D%D0%9E%D0%92

%D0%90%20%D0%91.%D0%91/3.2/rus_UNIX%20and%20Linux%20Forensic%20Analysis%20DVD%20Toolkit_2.pdf

ПРИЛОЖЕНИЕ

УТВЕРЖДАЮ
Начальник кафедры
уголовного процесса и криминалистики
Костанайской академии МВД
Республики Казахстан
имени Шракбека Кабылбаева,
полковник полиции
_____ С. Едресов

«24» 12 2021 года

А К Т
о внедрении методических рекомендаций по вопросам расследования и производства следственных действий по уголовным правонарушениям в сети Интернет в учебный процесс

Комиссия в составе:

председателя – заместителя начальника кафедры уголовного процесса и криминалистики, к.ю.н., полковника полиции Кадацкого С.Н.

и членов комиссии:

старшего преподавателя кафедры уголовного процесса и криминалистики, магистра юридических наук, подполковника полиции Арыстанбаевой Б.Б.;

преподавателя кафедры уголовного процесса и криминалистики, магистра юридических наук, майора полиции Даирова С.М.;

составила настоящий акт о том, что методические рекомендации по вопросам расследования и производства следственных действий по уголовным правонарушениям в сети Интернет, подготовленные доцентом кафедры следственно-оперативной работы 1-го Института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктором философии (PhD), ассоциированным профессором (доцентом), советником юстиции Медиевым Р.А. и магистрантом Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Секеновой Б.Б., используются при проведении занятий по следующим дисциплинам кафедры: «Уголовно-процессуальное право Республики Казахстан», «Криминалистика».

Председатель комиссии: С. Кадацкий

Члены комиссии: Б. Арыстанбаева

С. Даиров