МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ
ИМЕНИ М. ЕСБУЛАТОВА

БАЙСЕИТОВ БОЛАТ ТЕМИРБЕКОВИЧ

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВАМ В СЕТИ ИНТЕРНЕТ

Монография

Алматы, 2024

УДК 343.2/.7
ББК 67.408
Б18

Рекомендовано к печати Ученым советом Алматинской академии МВД Республики Казахстан им. М.Е. Есбулатова

Рецензенты:

Бимолданов Е.М. – заместитель начальника Алматинской академии МВД Республткт Казахстан имени М. Есбулатова, к.ю.н., полковник полиции

Пудовкин И.В. – начальник отдела по борьбе с киберпреступностью УКП ДП г. Алматы, подполковник полиции

Б18 Байсеитов Б.Т. Противодействие мошенничествам в сети Интернет: монография / Алматы: ООНИ и РИР Алматинской академии МВД Республики Казахстан им. М.Е. Есбулатова, 2024,-146 с.

ISBN 978-601-360-132-8

В монографии представлено противодействие мошенничествам в сети Интернет. На основе анализа научной литературы и правоприменительной практики раскрыта юридическая природа мошенничеств в сети Интернет, ее виды, а также предложены меры по совершенствованно действующего уголовного законодательства в сфере противодействия Интернет-мошенничествам.

Монография рассчитана на ученых-юристов, преподавателей, научных работников, практических сотрудников правоохранительных органов, а также для курсантов, слушателей и студентов.

УДК 343.2/.7
ББК 67.408

ISBN 978-601-360-132-8

Введение

Мошенничество возникло практически одновременно с появлением человечества и стоит признать, что этот вид деятельности успешно эволюционировал по всему миру. В поисках легкой добычи повсюду орудуют проходимцы разной масти, жулики, мошенники, вымогатели и прочая малопочтенная публика. Они проникли во все сферы жизнедеятельности человека, было бы странно, если Интернет выпал бы из сферы их интереса.

В последние годы мошенничество в Интернете развивается высокими темпами, а количество обманутых и пострадавших людей растет не по дням, а по часам. Хищение денег, кража конфиденциальной информации, личных данных, нарушение прав граждан, вымогательство, откровенный обман – можно долго перечислять методы и способы, которыми оперируют современные мошенники для «сравнительно не честного заработка денег, имущества и отъема законных прав у граждан».

Следует отметить, что защита прав, чести, достоинства и имущества гражданина Республики Казахстан закреплены Конституцией в статье 18 указанно, что:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства;

2. Каждый имеет право на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничения этого права допускаются только в случаях и в порядке, прямо установленных законом;

3. Государственные органы, общественные объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы докумен-

тами, решениями и источниками информации [1].

Но защищенные законом нашего государства права граждан, нередко, нарушаются различными преступными элементами, и в последнее время это особым образом выражено в сфере информационно-телекоммуникационных услуг, угроза, исходящая для пользователей данной сети, называется ничем иным как интернет-мошенничество.

Характерной особенностью интернет-мошенничества является то, что злоумышленников трудно поймать и привлечь к ответственности. Ведь физически они могут находиться даже на другом краю земного шара. И если они получают от своих жертв деньги с помощью электронных платежных систем, то вычислить их будет сложно. Даже если мошенников удастся вычислить и привлечь к ответственности (а их действия подпадают под юрисдикцию Уголовного кодекса любого государства), вернуть деньги пострадавшим не всегда удается.

Следовательно, лучший способ обезопасить себя от интернет-мошенников состоит в том, чтобы не попадаться на их уловки. Данную монографию мы посвятили проблеме выявления и раскрытия мошенничеств, совершенных в сети Интернет.

1. Проблемы выявления мошенничеств, совершаемых в сети интернет, причины и условия их распространения, анализ законодательства зарубежных стран и Республики Казахстан при квалификации и расследования уголовных правонарушений, связанных с Интернет-мошенничеством

Говоря о проблемах в какой-либо сфере деятельности, следует акцентировать внимание именно на тех, что интересуют сферу исследования. В этом случаи – это проблемы выявления мошенничеств, совершаемых в сети Интернет. В первую очередь необходимо выделить проблемы правового регулирования отношений с использованием сети Интернет, которые обусловлены особыми свойствами данной сети, что, по сути, является особым публичным пространством и в силу этого требует специального правового регулирования. Отсутствие такого регулирования негативно сказывается на развитии социальных и экономических процессов в обществе.

В результате исследований, которые проводились несколько раз, выяснилось, что всего 10% сотрудников правоохранительного аппарата считают, что их знания в сфере Интернет-технологий являются «достаточными», 30% – утверждают, что уровень их знаний находится на среднем показателе, остальные 60% – заявляют, что их познания в данной области можно оценить, как «слабые». На основании этой статистики, следует обратить особое внимание на подготовку конкретных категорий сотрудников, деятельность которых будет направлена на борьбу с преступлениями в сети Интернет, обеспечить совершенствование их знаний в сфере «киберпреступности», а также осуществлять выработку новых методов и средств противодействия данному виду преступности. В совокупности совершаемых во всемирной паутине преступлений можно выделить наиболее популярные, к которым в первую очередь относятся мошенничество [2].

Во вторую очередь, необходимо отметить следующее, сеть Интернет с одной стороны, является крупнейшим средством обмена информацией, с другой – ее особенности порождают стремительный рост преступлений, связанных с использованием информационно-телекоммуникационных технологий. В связи с этими проблемами выявления преступлений, совершенных в сети (в частности проблемы выявления Интернет-мошенничеств) особенности к которым относятся:

1) анонимность пользователей;
2) сложность идентификации пользователей;
3) низкая стоимость распространения информации;
4) высокая скорость распространения информации;
5) возможность охвата большой аудитории пользователей;
6) электронный характер документооборота в сети, что обусловливает необходимость применения специального программного и аппаратного обеспечения.

Все эти качества сети Интернет делают ее наиболее привлекательным средством для совершения мошеннических действий. Соответственно, главенствующее место среди преступлений, совершаемых в Интернет сегменте, занимает именно Интернет-мошенничество.

1.1. Проблемы квалификации мошенничеств, совершаемых путем обмана или злоупотреблением доверия пользователей информационно-коммуникационных систем

XXI век значительно отличается от предыдущих тем, что пользование и усовершенствование информационных технологий все больше набирает темпы. Информационные технологии настолько облегчили рутинную жизнь человека, что все манипуляции, действия мигом совершаются одним

нажатием кнопки, что значительно облегчают работу человека, не затрачивая на это большое количество времени. Поэтому практически все сферы жизни общества переходят на более высокую ступень развития, используя в своей деятельности техническое обеспечение в виде компьютеров и сети Интернет. Безусловно, информационные технологии не стоят на месте, уже невозможно представить какую-либо сферу где не используют компьютеры. Например, использование кредитных карт для хранения денежных сбережений, передача важной информации через Интернет или использование электронной цифровой подписи в какой-либо деятельности и т.д. Так можно привести множество примеров из жизни, где широко используется цифровая информация. Сейчас невозможно представить обычный досуг без компьютерных технологий, ибо они поглотили все сферы общественных отношений, но, к сожалению, параллельно с этими инновациями пришли проблемы, наносящие вред человеку в роли пользователя компьютерных технологий. В связи с этим появилась новая ступень преступности – преступность в сфере компьютерной информации.

Ни для кого не секрет что такое «фишинг». Это вид интернет-мошенничества, где главной целью является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Кроме того, сильно распространилось мошенничество с использованием информационных технологий. По этой причине возникла потребность ввести меры воздействия против преступников в данной области. Отсюда вытекает проблема, как квалифицировать такой вид преступлений? Она остается актуальной по сей день.

Пример «фишинг» можно рассмотреть в следующем. Мошенник создает возможность пользователю ввести личные данные, например, свою информацию о кредитных картах. Следует отметить, что все манипуляции лицо выполняет целиком и полностью сам, не догадываясь, что оно попадает

в ловушку мошенников.

Под мошенничеством, понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Это определение находит свое место в статье 190 Уголовного кодекса Республики Казахстан [3]. При этом, лицо которое попало в такую «ловушку» свободно передаѐт свое имущество либо право на него. Неоднократно, при таком типе мошенничеств лицо в отношении которого совершилось уголовное правонарушение узнаѐт об отрицательных последствиях произошедшего через некоторое время, например, когда посмотрел счет своей карты и увидел отсутствие средств. Тут получается, что отсутствует один из главных признаков состава преступления – добровольность».

Ниже представлены термины, которые встречаются в определении значения мошенничества: «злоупотребление доверием» и «обман». Отсюда вытекает вопрос: кто же здесь является объектом совершения обмана или лицом воспользовавшимся доверием? В нашем понимании это то лицо, которое совершило мошенничество, т.е. преступник который используя компьютерные технологии и информационно-телекоммуникационные сети, хитростью обманывает жертву и тем самым получает имущество. В качестве примера следует привести Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 года №6. «О судебной практике по делам о мошенничестве», в котором говорится об обмане или злоупотреблении доверием, как об объективной стороне состава мошенничества; наряду с этим, на месте объекта обмана изначально стоит человек, соответственно, потерпевшим лицом не будет являться ни компьютер, ни компьютерная информация [4]. При данном виде преступления нужна тесная связь между потерпевшим и преступником, так как изначально воздействие идет на психику личности, а действия компьютерной информации имеют аб-

солютно технический характер.

Таким образом, законодатель в п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан закрепляет следующее понятие (путем обмана или злоупотребления доверием пользователя информационной системы) [3] и в соответствии с данной нормой является возможным привлечение к ответственности лиц, совершающих уголовные правонарушения в сфере информационно-телекоммуникационных систем.

Если прибегнуть к мировой практике, то известно, что в Австралии такие деяния квалифицируются, как «имущественный вред, причинѐнный с целью извлечения незаконной выгоды для преступника или третьего лица, путѐм влияния на процессы автоматизированной обработки данных с помощью специальных программ, ввода, изменения или уничтожения данных, или иным способом, влияющим на процесс обработки данных». Главная мысль данного понятия заключается в том, что объектом является не сам компьютер, не процессы автоматизированной обработки данных, а различные программы, посредством которых лицо создает и совершает уголовное правонарушение.

При анализе состава преступления с использованием информационных технологий выявляются значимые разногласия, применяемые к преступлениям такого рода. Они выражаются как в объекте, так и в квалифицирующих признаках. Эта тема становиться одной из главных для уголовного законодательства во многих странах СНГ, на сегодняшний день [5]. Также следует сказать, что среди большинства ученных, нет единого мнения касаемо природы подобных преступлений. Следовательно, законодателю следует разработать правильный путь к решению этого вопроса, так как люди поддаются многим жизненным обстоятельствам и нередко совершают такого рода преступления.

Выходит, что понятие «компьютерное мошенничество» не оправдывает характеристику мошенничества и различного рода

хищения с использованием компьютерных технологий [6].

В связи с этим следует включить в качестве квалифицирующего признака понятие кражи, где смысл заключается не в обмане тех или иных потерпевших с использованием информационных технологий, а только так, как это сказано нормой ст. 190 УК РК «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» или же вводить дополнительные статьи, регулирующих ответственность за любые виды хищения с применением компьютерных технологий [3].

1.2. Причины и условия распространения мошенничеств в сети Интернет

Интернет представляет собой глобальную компьютерную сеть, основанную на принципе саморегуляции, автономности, самодостаточности.

Если оценивать возможности, которые глобальные информационные технологии предоставляют мошеннику для реализации его преступных замыслов, то можно выделить следующие обстоятельства, по которым мошенничество в Интернете развивается такими темпами:

Анонимность, во многом определяет специфику общения пользователей в глобальной сети. При этом не происходит личностно-визуального контакта, что снимает психологические барьеры и приводит к раскрепощенности [7, с. 29]. Практически невозможно установить личность человека, который хочет остаться незамеченным в виртуальном пространстве, пока существуют программы, маскирующие реальный IP – адрес, например, такие как (HideMyIP, SafeIP, HideALLIP, HideMy.nameVPN, Freegate) и многие другие

по которым можно идентифицировать местонахождение персонального компьютера преступника.

Технологии мобильного Интернета усугубляют ситуацию, поскольку преступник может свободно перемещаться в пространстве, используя различные точки доступа. Практический каждый человек имеет возможность воспользоваться доступом в Интернет за сравнительно небольшие деньги.

Еще одна специфическая особенность, **оперативность действий, производимых в Интернете**, «в режиме реального времени». Оперативность любых операций распространяется на всѐ пространство в Интернете, охватывающее страны и континенты [8, с. 7-8]. С помощью Интернета стало возможным общение людей из различных уголков планеты.

Применение новых технологий значительно облегчило задачу. При тиражировании и рассылки писем с помощью обычной почты, понадобилось бы затратить на почтовые расходы крупную сумму денег. Современные сетевые технологий не только упрощают, но и удешевляет совершение мошенничества.

Отсутствие социально-правового контроля со стороны общества за процессами информатизации. В начале рыночных реформ мы утратили остатки той системы социально-нравственного контроля за обществом, что прежде существовала в Советском Союзе [8, с. 85-93]. Являясь глобальной формой организации общественных отношений, Интернет обществом не контролируется. 1. Особенности современных сетевых технологий, предоставляющих возможности для успешного ведения преступной деятельности; 2. Отсутствие социально-правового контроля со стороны общества за процессами информатизации; 3. Недостатки в сфере правового регулирования; 4. Недостатки правоохранительной деятельности.

1.3. Исследование и анализ зарубежного законодательства в сфере противодействия Интернет-мошенничествам

Современный интернет представляет собой важный инструмент массовой коммуникации. Одновременно, это одна из самых быстро растущих площадок, где осуществляется торговля товарами и услугами.

В связи с ростом объемов купли-продажи посредством сети интернет, повышается «финансовая наполняемость» этой сферы. Как следствие, возникают дополнительные риски и угрозы для всех субъектов участвующих в этом, в том или ином статусе. Оплата товаров и услуг в сети интернет осуществляется посредством электронных платежей. Их объем по данным ООН увеличивается ежегодно на 30% [10]. Поэтому все более частыми становятся случаи совершения различных преступлений в данной сфере.

Банковские институты в большинстве развитых стран мира, многочисленные международные интернет-магазины, офисы крупных транснациональных компаний – постоянно публикуют правила безопасных финансовых операций в сети интернет. Тем не менее, данная мера не способствует эффективной профилактике и борьбе с преступлениями (в частности мошенничеством) в сфере интернет. Более того, общий объѐм противоправных деяний, посягающих на нарушения имущественных прав физических и юридических лиц неуклонно, возрастает.

По данным Гарвардской школы права, за последние пять лет количество преступлений, связанных с мошенничеством в сети интернет в среднем возрастает на 15-20% [11]. В данном контексте общественностью и властями многих развитых государств современного мира неоднократно поднимается вопрос, связанный с возможными ограничениями на доступ в интернет. Однако, такая авторитетная международная организация как ООН в начале 2011 года приняла важное

решение о включении права на доступ в интернет в список неотъемлемых прав личности [12, с. 22]. В результате, на правоохранительные органы большинства развитых, демократических стран современного мира легла дополнительная задача, связанная с обеспечением безопасности данной сферы. Задача настоящей статьи – исследовать специфику зарубежного законодательства, регулирующего мошенничество в интернете, на примере таких государств как Франция, Испания, Германия. Реализация указанной задачи видится возможной посредством сравнительно-сопоставительного анализа, уголовного кодекса обозначенных государств.

В уголовном кодексе Германии в 22 разделе сведены большинство мошеннических посягательств, которые могут предприниматься в сети интернет. А именно, «компьютерное мошенничество (ст. 263а), получение субсидии путем мошенничества (ст. 264), мошенничество при капиталовложении (ст. 264 а), обман с целью получения завышенной суммы страховки (ст. 265), получение выгоды путем обмана (ст. 265 а), мошенничество, связанное с получением кредита (ст. 265 б)» [13]. Проанализировав диспозиции данных статей можно сделать следующий вывод. Под мошенничеством в сети интернет в современной Германии понимается причинение вреда имуществу физических и юридических лиц с целью получения определенной (прежде всего имущественной) выгоды путем обмана.

Тем самым, законодатель не делает принципиальных различий между мошенничеством и мошенничеством в интернет сфере. Более того, в Уголовном кодексе Германии концепты обман и мошенничество используются в качестве синонимов, что определенным образом сужает понимание данных социально-правовых феноменов. Необходимо отметить, что там «злоупотребление доверием» в сети интернет выделяется в качестве самостоятельного имущественного преступления. Возможно, что такая специфика связана с необходимостью более четкой квалификации схожих деяний

(например, сравнивая содержание ст. 263 и ст. 265а можно прийти к выводу, что квалификация схожих деяний в сложных социально-экономических и информационных ситуациях может быть значительно затруднена).

Что касается Уголовного кодекса Испании, то преступления, касающиеся мошенничества в интернет сфере содержатся в его 13 разделе. Он содержит обширную перечень преступлений против собственности и экономического порядка. В ст. 248 Уголовного кодекса Испании мошенничество рассматривается как вариация обмана, суть которого состоит в введении в заблуждение другого лица в пользу преступника с целью распоряжаться его имуществом или имуществом иных лиц. Необходимо отметить, что законодателем особо выделяется ситуация, в которой мошенник «с целью наживы добивается неправомерной передачи наличного имущества, манипулируя информацией или используя другую подобную уловку» [14]. Тем самым, делается акцент на мошенничестве в интернет сфере. В ст. 255 указанная специфика детализируется более подробно. А именно, в качестве объектов преступного воздействия указываются различные институты телекоммуникации.

Таким образом, в Уголовном кодексе Испании мошенничество в интернет сфере институционализировано. При этом, необходимо отметить, что его трактовки носят больше абстрактно-теоретический характер в отличие от концептуализации данного явления в Уголовном кодексе Германии. Более того, Уголовный кодекс Испании многие виды интернет мошенничества не считает уголовно наказуемыми, т.к. они не приносят значительного ущерба имуществу физических и юридических лиц. Такая «либеральность» законодательства значительно отличается статей от УК Германии, которые регулируют отношения в этой сфере.

Уголовный кодекс Франции содержит раздел, который называется «Об обманном завладении» и главу «О мошенничестве и примыкающих к нему деяниях». Если подробно рас-

сматривать содержание указанного раздела и главы, то под мошенничеством французские законодатели понимают «обман физического или юридического лица, совершенный путем использования ложного имени, должности или положения, а также злоупотребления служебным положением, либо путем использования обманных действий в целях побуждения лица к передаче денежных средств, ценностей или иного имущества» [15]. При этом французские законодатели наряду с общим составом мошенничества выделяют специальные составы преступных деяний. К ним прежде всего, относятся мошенничество в интернете с использованием современных информационно-коммуникационных технологий, специализированных программ и оборудования.

Таким образом, за последние несколько десятилетий в Германии, Франции, Испании активно расширяются гражданские права и свобода в интернете. В соответствии с данной тенденцией вносятся поправки в законодательную базу данных стран. При этом, изменения, такие как расширение возможностей, открытость и прозрачность интернет услуг которая декларируется в многочисленных нормативных актах, регулирующих стремительно меняющееся интернет пространство, не всегда приводит к росту безопасности данной среды. Национальные законодательные рамки не всегда способны эффективно защищать интеллектуальную собственность, авторские права и торговые знаки, а также иную коммерческую информацию (в частности данные международных платежных систем). Это приводит к тому, что постоянно возрастает потребность в предупреждении использования информационно-коммуникационных технологий в противоправных деяниях. В связи с этим, для выработки оптимальных подходов к правовому регулированию, и улучшению безопасности в сети, необходимо тщательно изучить опыт зарубежных стран по регулированию общетеоретических вопросов мошенничества в сети интернет.

1.4. Исследование и анализ интернет мошенничеств в США

Ущерб от деятельности интернет-мошенников в США достиг рекордных $6,9 млрд – ФБР[16].Интернет-мошенники в 2021 году причинили американцам рекордный ущерб на 6,9 миллиарда долларов, годом ранее киберпреступникам удалось похитить «лишь» около 1,7 миллиарда – об этом сообщили в The Record со ссылкой на ежегодный отчѐт ФБР о преступлениях в Сети.

При подготовке доклада используются данные специального подразделения ФБР – Центра жалоб на преступления в Интернете (Internet Crime Complaint Center).

В общей сложности, в прошлом году в центр поступило 847 376 жалоб, большинство из них касалось случаев кибервымогательств, компрометации деловой переписки (Business E-mail Compromise, BEC), использования криптовалют в незаконных целях. По сравнению с 2020 годом количество обращений в центр выросло на 7%.

Так, ФБР получило 19 954 жалобы на BEC-атаки, жертвы которых лишились 2,4 миллиарда долларов. На мошенников, целями которых становились граждане, искавшие знакомств в сети, было подано 24 299 заявлений, а ущерб составил 956 миллионов долларов. 18 тысяч жалоб касались случаев шантажа с угрозой публикации откровенных материалов с участием потерпевших. В этой сфере злоумышленники «заработали» 13,6 миллиона долларов [16].

Как отмечается в докладе, тысячи случаев мошенничества на сайтах знакомств были связаны с использованием криптовалюты – преступникам удалось похитить у доверчивых американцев криптоактивы на 429 миллионов долларов.

Напомним, ранее о резком росте в США количества случаев мошенничества с использованием сайтов знакомств заявляли в Федеральной торговой комиссии США (Federal

Trade Commission, FTC).Также мошенники в США стали притворяться сотрудниками полиции и чиновниками.

ФБР предупредило американцев о распространении в стране особого вида мошенничества – злоумышленники выдают себя за сотрудников правоохранительных органов или чиновников, чтобы заполучить деньги своих жертв либо персональные данные (ПД), сообщили Минюст США.

Мошенники звонят своим жертвам с номеров телефонов, похожих на те, что используют правительственные агентства и правоохранительные органы. Затем настойчиво и агрессивно требуют от собеседника перевести деньги или отправить личную информацию под различными предлогами.

К примеру, злоумышленники сообщают что личные данные жертвы «всплыли» при расследовании преступления, обычно связанного с наркотиками или отмыванием денег. От обывателя требуют сообщить персональные данные, включая личный номер социального страхования и дату рождения.

Жертве грозят арестом, тюремным заключением и судебным преследованием, если тот или иной гражданин не заплатит за снятие обвинений или откажется сотрудничать для поимки «настоящих» преступников.

Деньги требуют переводить при помощи предоплаченных банковских карт, почтой, а также криптобанкоматов. При этом американцев, попавшихся на крючок мошенников, убеждают никому не сообщать о звонке [16].

Ещѐ раньше этот же социально-инженерный приѐм освоили русскоязычные мошенники, нацеленные на граждан РФ: после того, как потенциальные жертвы перестали «вестись» на звонки от имени сотрудников банка, жулики стали представляться сотрудниками полиции, якобы расследующими кражу денег.

1.5. Исследование и анализ Российского законодательства в области борьбы с интернет-мошенничеством

В соответствии со статьями 8 и 35 Конституции РФ право частной собственности принадлежит каждому человеку и является составляющей конституционного строя. Для большинства граждан обладание собственностью и осознание ее надежной правовой защиты со стороны государства вселяет уверенность в свое будущее [17, с. 16-20].

Признавая и защищая частную собственность, государство берет на себя обязанность обеспечить ее охрану путем принятия соответствующих законов. При этом оно следует общепризнанным принципам международного права, закрепленным в статье 17 Всеобщей декларации прав человека и статье 1 Протокола №1 от 20 марта 1952 года к Европейской конвенции о защите прав человека и основных свобод 1950г.

До ноября 2012 года все виды мошенничества в Интернете квалифицировались только по ст. 159 УК РФ – Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. И только 29.11.2012 года (N 207 – ФЗ), были введены в УК РФ новые статьи, 159.3. Мошенничество с использованием электронных средств платежа и статья 159.6. Мошенничество в сфере компьютерной информации [18].

Статья 159.6 УК РФ Мошенничество в сфере компьютерной информации, гласит: ч.1 Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно- телекоммуникационных сетей, – наказывается штрафом в размере до ста двадцати тысяч рублей или иного дохода осужденного за период до одного года, либо обязательными работами до трехсот шестидесяти часов

или исправительными работами до одного года, либо ограничением свободы до двух лет, либо принудительными работами до двух лет, либо арестом до четырех месяцев [19, с. 118].

Объективная сторона мошенничества состоит в хищении чужого имущества, равно приобретения права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [20]. Субъект – любое дееспособное лицо, достигшее 16-летнего возраста. Субъективная сторона – вина в виде прямого умысла и корыстная цель.

Законом предусмотрены как квалифицированный состав – мошенничества в сфере компьютерной информации, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба потерпевшему (ч. 2), так и особо квалифицированные составы данного преступления: деяния, совершенные с использованием своего служебного положения, ущерб равен сумме в размере – 1 млн. 500 тыс. рублей (ч. 3), а так же деяния, совершенные организованной группой либо в особо крупном размере – 6 млн. рублей (ч. 4).

В УК РФ есть и другие статьи, относящиеся к компьютерной преступности, которыми можно воспользоваться для привлечения к ответственности Интернет-мошенников: статья 272 УК РФ – неправомерный доступ к компьютерной информации; статья 273 – создание, использование и распространение вредоносных программ для ЭВМ; статья 274 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети; статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [18].

Управление «К» МВД РФ, которое занимается расследованием всех Интернет-преступлений, часто сталкивается с проблемами. Все инциденты, связанные с глобальной сетью, отличаются большой латентностью, поэтому представляется трудным их отследить.

1.6. Исследование и анализ законодательства Республики Казахстан в сфере квалификации уголовных правонарушений, связанных с Интернет-мошенничеством, а также их разграничение

Современный мир очень развит компьютерными технологиями и глобализацией информационных процессов. Наиболее ярким событием является появление международной сети Интернет, а также масштабное расширение ее использования во всех сферах социального общества.

Все чаще сеть Интернет используется для размещения противоправной информации, в т.ч. порнографии, объявлений о продаже оружия, наркотиков. Для их совершения используются программы и сервисы, позволяющие скрыть свои установочные данные, местоположение. Сфера применения компьютерных технологий в преступных целях весьма обширна. Объясняется это, прежде всего, их общедоступностью и простотой эксплуатации. Жертвами преступников становятся как частные лица, так и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Наиболее часто мишенями преступников становятся банки и их клиенты. По итогам 2021 года в нашей стране совершено свыше 21 тыс. мошенничеств и большая часть из них – это электронные хищения, совершенные в сфере информационно- телекоммуникационных систем, или иначе говоря, Интернет-мошенничества.

Следует отметить что «самыми распространенными видами Интернет-мошенничества являются размещение на различных месенджерах и торговых интернет-площадках объявлений о продаже товаров или оказании тех или иных услуг на примере OLX, Крыша KZ или Колеса KZ, Instagram, VK и т.д. Как правило, мошенники привлекают своих жертв невысокой ценой или

быстрым предоставлением товара. Покупателей просят внести частичную или полную предоплату на счета, обычно оформленного на третьих лиц. Ниже приведены виды интернет-мошенничеств, которые встречаются чаще всего.

Статистические данные по Интернет-мошенничествам, статья 190 Уголовного Кодекса Республики Казахстан за период с 2017 по 2022 гг.

Статистические сведения за 5 лет																	
Статья	**2017 год**			**2018 год**			**2019 год**			**2020 год**			**2021 год**			**5 мес. 2022 года**		
	Зарегистрировано	Раскрыто	Прерваны сроки	Зарегистрировано	Раскрыто	Прерваны сроки	Зарегистрировано	Раскрыто	Прерваны сроки	Зарегистрировано	Раскрыто	Прерваны сроки	Зарегистрировано	Раскрыто	Прерваны сроки	Зарегистрировано	Раскрыто	Прерваны сроки
ст.190 УК*(Интернет- мошенничество)*	2046	166	1759	4287	805	3535	7739	1290	6139	14175	2581	10709	21275	3804	17515	8152	1502	4750
ВСЕГО:	**2046**	**166**	**1759**	**4287**	**805**	**3535**	**7739**	**1290**	**6139**	**14175**	**2581**	**10709**	**21275**	**3804**	**17515**	**8152**	**1502**	**4750**

Для исследования, были использованы статистические данные по Интернет-мошенничествам предоставленные МВД Республики Казахстан квалифицируемые статьей 190 Уголовного Кодекса Республики Казахстан за период с 2017 по 2022 гг.

Согласно данным МВД РК, в 2017 году в Казахстане, количество зарегистрированных преступлений по ст. 190 УК РК, составило2046, из них раскрыто 166 и по 1759 прерваны

сроки. В 2018 году зарегестрированно4287 интернет-мошенничеств, из них раскрыто 805 и прерваны сроки по 3535 фактам, что на 22,41% больше чем в 2017 году. В 2019 году зарегестрированно 7739, из них раскрыто 1290 и прерваны сроки по 6139, что на 34,52% больше чем в 2018 году. В 2020 году зарегестрированно 14175, из них раскрыто 2581 и прерваны сроки по 10709, что на 64,36% больше чем в 2019 году. В 2021 году зарегестрированно 21275, из них раскрыто 3804 и прерваны сроки по 17515, что на 71% больше чем в 2020 году. В 2022 году за первые 5 месяцев зарегестрированно 8152, из них раскрыто 1502 и прерваны сроки по 4750, таким образом можно заметить быстро растущую и стремительными темпами развивающуюся динамику роста рассматриваемой категории преступлений.

Для получения дополнительных данных, в процессе исследования мы проводили анкетирования в период с 25.01.2022г. по 27.06.2022г. Опрос проводился как среди сотрудников ОВД из числа обучаемых слушателей Центра по подготовке специалистов по противодействию киберпреступности, так и среди студентов различных ВУЗов и случайных граждан города Алматы и Алматинской области.

Возраст респондентов: от 18 до 24 лет – 44%, 25-35 лет – 30%, 36-50 лет – 26%. Среди ответивших респондентов 65% – женского пола, и 35% – мужского пола.

Среди ответивших выделилась группа респондентов, которые не сталкивались с мошенничеством в Интернете в любой форме проявления и последствий – 23%.

Определение ситуации мошенничества в Интернете, с которыми респонденты сталкивались или встречались: 83% – SMS – оплатой и голосованиями, 72% – сталкивались с фальшивыми извещениями о выигрыше в лотерею, 71% – с мошенничеством в виде рекламы товаров и услуг, 68% – с попрошайничеством – 56%, имитаторами вирусов и антивирусов – 53%.

Среди техник, которые знакомы, но не встречались пользователям, большинство респондентов отметили взлом сайтов и DDoS-атаки: кража пароля от учетной записи пользователя – 52%.

Большинство, чаще всего сталкивались с мошенничеством в социальных сетях – 73%, в сообщениях, посылаемых на электронную почту – 73%, через переписку мгновенного обмена сообщениями – 61%, на сайтах с интересующей тематикой – 39%.

Сообщения мошенников в 42% случаев адресовалось пользователям лично, по имени, иногда указывалась и фамилия. Видно, что чаще всего мошенники пытаются осуществить акт мошенничества, используя такие коммуникативные каналы, через которые они могут обратиться в личной форме к пользователю.

Опыт столкновения респондентов с Интернет-мошенничеством: 21% респондентов – попадались на обман мошенников; 60% – вовремя поняли, что это действия мошенников, и не среагировали на сообщение; 19% – не попадались на обман Интернет-мошенников.

На вопрос, как удается избежать попадания на обман мошенников, 56% – не попадаются на обман, поскольку критически оценивают сайты, сообщения, предложения в Интернете;

54% – отмечают, что причиной является опыт других людей, которые стали жертвой мошенничества;

46% – не попадаюсь, потому что знаю основные техники и способы мошенничества;

35% – количество лет работы в Интернете.

Какие потери понесли пользователи, столкнувшиеся с мошенничеством.

60% – респондентов не понесли никаких потерь; около трети, понесли моральные потери – 27%; 11% – материаль-

ные потери, 2% – потеряли время, затраченное на устранение последствий (восстановление работы компьютера после атаки мошенников).

Некоторые пользователи попадались на обман не единожды, 48% – около половины респондентов жертвами мошенников становились 1 раз; 20% – от 2-4-х раз; 12% – становились жертвой более 4-х раз.

Среди причин, по которым анкетируемые попадались на обман мошенников: 58% – по невнимательности; из-за излишней доверчивости – 28%; из-за отсутствия опыта с мошенничеством – 14%.

Ответные реакций анкетируемых которые попались на обман мошенничества: 34% – ничего не предпринимали; лишь 13% ответивших обратились в правоохранительные органы; 4% – к администрации игрового сервера, где произошло мошенничество; 23% – обращались в банк, где была скомпрометирована кредитная карта; 26% – обращались в другие места: фирму по ремонту компьютеров, к друзьям; к юристу; к телефонному оператору, с номера которого мошенники вымогали деньги.

Из 5 респондентов, которые обратились в правоохранительные органы, удалось привлечь мошенника к ответственности только в единичных случаях. Большинство пострадавших пользователей не пытались привлечь мошенников к ответственности. Малая доля респондентов, которые предпринимали действия, чтобы вернуть потерянное использовали личные знакомства, юристов, локальные органы контроля в коммуникативном пространстве где произошло мошенничество.

Согласно уголовному кодексу Республики Казахстан от 3 июля 2014 года №226-V ЗРК, за мошенничества предусмотрено наказание в ст. 190 ч.2 п.4.

Статья 190. Мошенничество

1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, – наказывается штрафом в размере до одной тысячи месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с конфискацией имущества.

2. Мошенничество совершенное:

1) группой лиц по предварительному сговору;

2) исключен законом РК от 21.01.2019 №217-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования);

3) лицом использовавшего свое служебного положения;

4) путем обмана или злоупотребления доверием пользователя информационной системы;

5) в сфере государственных закупок, – наказывается штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере или привлечением к общественным работам на срок до одной тысячи часов, либо ограничением свободы на срок до четырех лет или лишением свободы на тот же срок, с конфискацией имущества, с лишением права занимать определенные должности, либо заниматься определенной деятельностью на срок до трех лет или без такового.

3. Мошенничество, совершенное:

1) в крупном размере;

2) лицом, уполномоченным на выполнение государственных функций, либо приравненным к нему лицом, либо должностным лицом или лицом, занимающим ответствен-

ную государственную должность, если оно сопряжено с использованием им своего служебного положения;

3) в отношении двух или более лиц;

4) неоднократно, – наказывается ограничением свободы на срок от трех до семи лет либо лишением свободы на тот же срок, с конфискацией имущества, а в случаях, предусмотренных пунктом 2), – штрафом от десятикратного до двадцатикратного размера похищенного имущества либо лишением свободы на срок от трех до семи лет, с конфискацией имущества, с пожизненным лишением права занимать определенные должности или заниматься определенной деятельностью.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они совершены:

1) преступной группой;

2) в особо крупном размере, – наказываются лишением свободы на срок от пяти до десяти лет с конфискацией имущества, с пожизненным лишением права занимать определенные должности или заниматься определенной деятельностью или без такового [20].

В действующем уголовном законодательстве Республики Казахстан существует ряд уголовных правонарушений, имеющих между собой определенное сходство, как по объекту посягательства, так и по другим элементам и признакам состава уголовных правонарушений. Уголовное правонарушение, предусмотренное ст. 190 УК РК, необходимо разграничивать с такими смежными составами уголовных правонарушений, как ст.ст. 188, 189, 195, 219 УК РК.

Таблица 1. Отграничение ст. 190 УК РК от ст.188 УК РК

Ст. 190 УК РК «Мошенничество»	**Ст. 188 УК РК «Кража»**
Объект преступления	
Непосредственный объект – отношения собственности. Предмет мошенничества – не только само имущество, но и право на него.	Непосредственный объект – отношения собственности. Предметом хищения может быть только имущество, произведенное трудом человека, или извлеченные им из природной среды предметы, способные удовлетворять индивидуальные или коллективные потребности, обладающие стоимостью и не исключенные из гражданского оборота.
Объективная сторона преступления	
Завладение чужим имуществом или приобретение права на чужое имущество путем обмана или злоупотребления доверием	Тайное хищении чужого имущества. Способ (обязательный признак) совершения кражи–тайное не насильственное изъятие (завладение) чужого имущества
Субъект преступления	
Физическое вменяемое лицо, достигшее 16-летнего возраста	Физическое вменяемое лицо, достигшее 14-летнего возраста
Субъективная сторона преступления	
Субъективная сторона идентична, в обеих статьях предусмотрена умышленная форма вины	

Таблица 2. Отграничение ст. 190 УК РК от ст.189 УК РК

Ст. 190 УК РК «Мошенничество»	**Ст. 189 УК РК «Присвоение или растрата вверенного чужого имущества»**
Объект преступления	
Непосредственный объект – отношения собственности. Предмет мошенничества – не только само имущество, но и право на него.	Непосредственный объект – собственность, т.е. совокупность общественных отношений по поводу владения, пользования или распоряжения имуществом. Предметом присвоения или растраты вверенного чужого имущества может быть произведенный трудом человека или извлеченные им из природной среды предметы, способные удовлетворять индивидуальные или коллективные потребности, обладающие стоимостью и не исключенные из гражданского оборота.
Объективная сторона преступления	
Завладение чужим имуществом или приобретение права на него путем обмана или злоупотребления доверием.	Присвоение либо растрата вверенного имущества.
Субъект преступления	
Физическое вменяемое лицо, достигшее 16-летнего возраста.	Специальный: вменяемое лицо, достигшее 16 лет, которому похищенное имущество было вверено в правомерное владение.
Субъективная сторона преступления	
Субъективная сторона идентична, в обеих статьях предусмотрена умышленная форма вины.	

Таблица 3. Отграничение ст. 190 УК РК от ст.195 УК РК

Ст. 190 УК РК «Мошенничество»	**Ст. 195 УК РК «Причинение имущественного Ущерба путем обмана или злоупотребления доверием»**
Объект преступления	
Непосредственный объект – отношения собственности. Предмет мошенничества – не только само имущество, но и право на него.	Непосредственный объект – отношения собственности. Предметом может быть любое имущество.
Объективная сторона преступления	
Завладение чужим имуществом или приобретение права на него путем обмана или злоупотребления доверием.	Причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием, но при отсутствии признаков хищения.
Субъект преступления	
Субъект преступления в обеих статьях – физическое вменяемое лицо, достигшее 16-летнего возраста.	
Субъективная сторона преступления	
Субъективная сторона идентична, в обеих статьях предусмотрена умышленная форма вины	

Таблица 3. Отграничение ст. 190 УК РК от ст. 219 УК РК

Ст. 190 УК РК	**Ст. 219 УК РК «Незаконное получение кредита или**
«Мошенничество»	**нецелевое использование бюджетного кредита»**
Объект преступления	
Непосредственный объект – отношения собственности. Предмет мошенничества – не только само имущество, но и право на него.	ч.1. Объектом преступления являются кредитные отношения в экономике, а также имущественные интересы граждан и юридических лиц. Предметом преступления являются кредит, дотации либо льготные условия кредитования, которые представляют собой более выгодные условия по сравнению с общими условиями для получения кредита, а также и его возврата. ч. 2. Объект преступления–интересы государства, выступающего в качестве кредитора. Предмет посягательства–государственный целевой кредит.
Объективная сторона преступления	
Завладение чужим Имуществом или приобретение права на чужое имущество путем обмана или злоупотребления доверием.	Незаконное получение индивидуальным предпринимателем или руководителем организации кредита совершается особым способом: путем предоставления банку или иному кредитору заведомо ложных сведений о своем хозяйственном положении либо финансовом состоянии. Обязательный признак – при-

	чинение крупного ущерба кредитору (ч.1). Использование государственного целевого кредита не по его прямому назначению (ч.2).
Субъект преступления	
Физическое вменяемое лицо, достигшее 16-летнего возраста.	Специальный, т.е. индивидуальный предприниматель или руководитель коммерческой или некоммерческой организации, независимо от ее организационно-правовой формы или формы собственности (ч.1). Специальный, т.е. индивидуальный предприниматель или руководитель коммерческой или некоммерческой организации, лицо вменяемое, достигшее 16 лет (ч.2).
Субъективная сторона преступления	
Выражена виной в форме прямого умысла и корыстной целью.	Характеризуется виной в форме прямого или косвенного умысла (ч.1); Совершается умышленно, с косвенным умыслом(ч.2).

Разграничение мошенничества в сфере гражданско-правовых отношений

Вопрос о разграничении мошенничества и гражданско-правовых отношений возникает в том случае, когда имеется некий договор. Неважно какой – устный или письменный, но он обязательно должен быть. В основе всегда лежат какие-то взаимные отношения двух сторон: одна сторона передает

деньги или имущество, другая – обязуется что-либо сделать или передать (продать) имущество. Таким образом, обязательства встречные.

При мошенничестве заинтересованное лицо желает завладеть имуществом или деньгами, договор служит лишь прикрытием преступных намерений лица. При нормальной ситуации гражданско-правовых отношений лицо намеревается исполнить свои обязательства по договору.

Проблема квалификации действий как мошеннических, заключается в следующем: необходимо установить и доказать умысел виновного на хищение денег до момента заключения сделки. Иначе говоря, надо установить, что виновный еще до момента вступления в правоотношения исполнять свои обязательства не собирался. Поскольку виновное лицо тщательно скрывает свои истинные преступные намерения, именно в этом заключается основная сложность.

Основной признак мошенничества, отличающий его от гражданско-правовых отношений – наличие обмана. Причем обмана не по срокам исполнения обязательства или иным моментам договора, а обмана, касающегося самого исполнения обязательства. Обман, в этом случае, состоит в сообщении заведомо ложных сведений относительно существенных моментов исполнения сделки, он может быть исполнен посредством совершения действий. Например, лицо продает квартиру, которая ему не принадлежит, берет деньги за поставку товаров, которых нет в наличии и которые не собирается поставлять и т.д. Умысел на мошенничество возникает заранее, обман является способом получения денег или имущества [22].

В пунктах 10 и 11 Нормативного постановления Верховного Суда Республики Казахстан «О судебной практике по делам о мошенничестве» от 29 июня 2017 года №6 указано, что:

1) для разграничения мошенничества от гражданско-правовых отношений следует учитывать, что при мошенничестве умысел направленный на хищение чужого имущества

или **приобретение права на чужое имущество путем обмана или злоупотребления доверием, возникает у виновного лица до и (или) в момент заключения договора**, предусматривающего получение чужого имущества или права на него.

В таких случаях обманные действия виновного должны являться причинной связи с фактом получения имущества или приобретения права на имущество, т.е. обманные действия должны предшествовать передаче этого имущества или приобретения права на него;

2) судам следует учитывать, что о наличии умысла, направленного на хищение путем мошенничеств при договорных обязательствах может свидетельствовать совокупность таких обстоятельств как, заведомое отсутствие у лица реальной финансовой и иной материальной возможности (материально-техническая оснащенность, трудовой коллектив и т.д.) исполнить принимаемое обязательство, или необходимой лицензии, разрешения на осуществление деятельности, направленной на исполнение обязательств по договору, использование лицом поддельных учредительных документов или гарантийных писем, сокрытие информации о наличии задолженностей или залога по имуществу, заключение заведомо неисполнимых договоров и др.

В тех случаях, когда договор между сторонами заключается с обоюдными намерениями 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, в нормативном постановлении недвусмысленно указывается, что преступный умысел виновного лица, направленный на хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, возникший до или в момент заключения граж-

данско-правового договора, является основанием для осуществления досудебного расследования. **Следовательно, наличие гражданско-правовой сделки в письменной форме не должно быть основанием для отказа в регистрации заявления о совершении преступления.**

Согласно п. 2 ст. 158 ГК РК [23] сделка, направленная на достижение преступной цели, противоправность которой установлена приговором (постановлением) суда, ничтожна. Таким образом, согласно ГК РК нет необходимости предварительно обращаться в суд с иском о признании сделки недействительной, чтобы потом обратиться в органы уголовного преследования с заявлением, например, о мошенничестве. Если в рамках уголовного производства вступившим в законную силу обвинительным приговором суда будет установлен факт мошенничества, прикрытый противоправной гражданско-правовой сделкой, такая сделка признается ничтожной.

Анализ Гражданского кодекса Республики Казахстан показывает, что гражданско-правовая сделка должна отвечать следующим условиям:

– выражение согласованной воли всех сторон сделки;

– соответствие сделки законодательству РК и подзаконным нормативным актам;

– сделка не должна противоречить основам правопорядка и нравственности;

– участниками сделки с обеих сторон могут быть лишь дееспособные и правоспособные лица;

– гражданин, совершая сделку, должен находиться в состоянии, позволяющем ему понимать последствия своих действий и руководить ими;

– сделка не должна заключаться под воздействием заблуждения, обмана, насилия или угрозы.

Невыполнение хотя бы одного из этих условий влечет за собой недействительность сделки. Если сопоставить условия

сделки со статьями гл. 6 Уголовного кодекса Республики Казахстан, для установления наличия признаков преступления достаточно выявить хотя бы одно из следующих условий:

– заведомое использование в сделке подложных либо полученных обманным путем подлинных документов;

– введение в заблуждение относительно предмета, объекта сделки;

– применение обмана относительно любых обстоятельств, существенных для сделки;

– применение насилия, угроз, использование беспомощного состояния заявителя для получения подлинных документов, удостоверяющих его право собственности или личность;

– совершение сделки от имени заведомо недееспособного либо заведомо неправомочного лица;

– заведомое нарушение одним из участников сделки порядка ее оформления и регистрации.

Это определяет круг исследовательских задач, необходимых для установления факта совершения уголовного правонарушения.

2. Самые распространенные виды Интернет-мошенничеств совершаемых в сфере информационно-телекоммуникационных систем

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

Мошенничество в интернет-магазине

Для обмана пользователей мошенники часто используют онлайн-магазины:

а) просят внести предоплату и после получения денег

исчезают.

Связаться с ними невозможно;

б) поставляют вместо заказного подделку. Претензии предъявлять некому.

Интернет-попрошайничество. **<u>Лжеблаготворительность</u>**

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

Интернет-попрошайничество

Куда выкладывают объявления?

-в благотворительные организации;
-на специальные онлайн-платформы;
-площадки для сбора на какие-либо проекты.

Три признака Интернет-попрошайничества:

1. Компания-однодневка, проработав недолго, закрывается и открывает под новым именем. И так – по несколько раз.
2. Отсутствие портфолио. Когда, кому, чем помогли? Каков результат? У настоящих благотворительных компаний отчётность хорошо налажена и выставлена на всеобщее обозрение.
3. Недостаточно информации. Следует насторожиться, если сайт содержит всего 2 страницы.

«Фишинг»

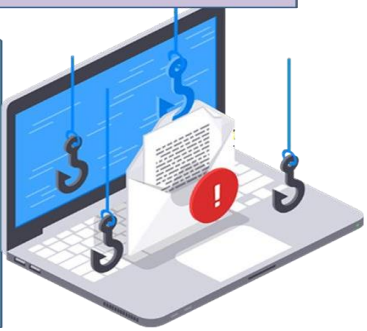
Фишинг – (англ. *Phishinotfishing* «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям.

ФИШИНГ

Отправка фальшивых сообщени через сервисы с целью получения доступа конфиденциальной информации

Чем опасен:

- теряет деньги;
- теряет контроль над своими аккаунтами в социальных сетях;
- есть риск раскрыть важную информацию о себе.



Взлом аккаунтов в соцсетях

«Кликджекинг» (англ. *Clickjacking*) – механизм обмана пользователей Интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу. Возможны применения различных технологий – от подписки на ресурс в социальной сети, до кражи конфиденциальной информации и совершения покупок в интернет-магазинах за чужой счѐт [24].

Интернет-мошенничество на биржах

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

Мошенничество на биржах

Традиционная схема действий мошенников:
- агрессивные продажи (сливание) акций. Они скупаются брокером по низкой цене, а продаются по завышенной;
- псевдо брокер-мошенник создает небольшую компанию, привлекает низкими сборами, горячими акциями, которые могут оказаться подделкой. Как только у трейдера появляются сомнения, брокерская компания ликвидируется;
- «Авансовый платеж»-схема реализуется, когда трейдер оказывается в невыгодной открытой позиции. Брокер-мошенник предлагает обменять имеющиеся бумаги на акции, чтобы получить дивиденды и возможность их выгодно перепродать;
- дополнительные платежи-схема, применяемая даже лицензированными брокерами. С клиентов постоянно под разными предлогами взимаются дополнительные платежи.

Неожиданный выигрыш в Интернете

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

Неожиданный выигрыш в Интернете

Пользователям рассылаются фальшивые извещения о выигрыше в лотерею, якобы проводимую среди случайных e-mailадресов/номеров телефонов, и предложения получить «бесплатные» подарки в качестве выигрыша. Для убедительности в таком письме может присутствовать фотография приза и всевозможные «атрибуты подлинности» лотереи, свидетельство о регистрации/лицензии и прочая фальшивая информация. Для получения выигрыша пользователю предлагается предварительно совершить платеж на некую сумму по указанным мошенниками счетам.

Интернет-казино

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

Интернет-казино

Пользователю заявляют о небывало высокой вероятности выигрыша. На самом деле игрок теряет свои деньги сразу. Возможны и другие сценарии: например, платная регистрация, либо невыплата выигранных денег.

Мошенники могут прикрываться адресами (названиями) настоящих казино, однако процедуру регистрации необходимо пройти на другом сайте.

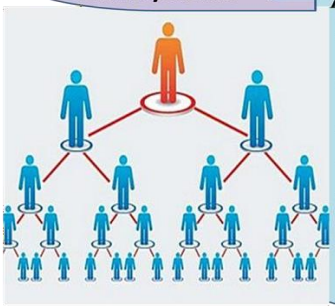
Создают точные копии клонов популярных игровых порталов. Название мошеннического сайта в таком случае, как правило, созвучно с оригинальным, однако все же отличается, например, недостающей или лишней буквой.

Финансовые пирамиды в Интернете

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

Шесть кошельков – человек получает электронное

Финансовые пирамиды в Интернете



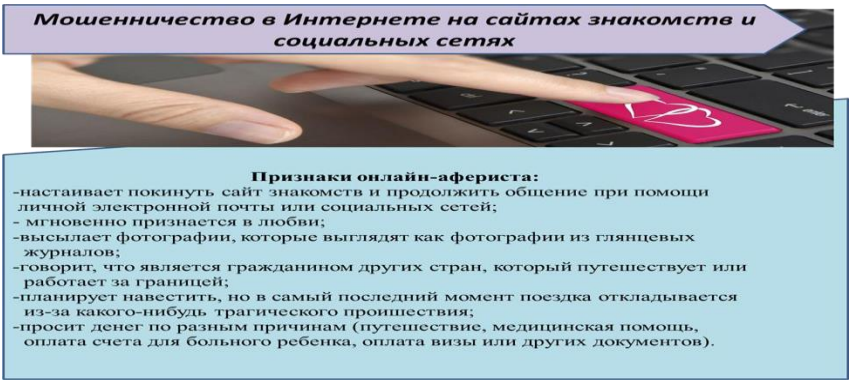
Признаки финансовой пирамиды

- у организации нет лицензии;
- вкладчикам обещают высокую доходность и призывают быстрее вкладывать деньги;
- выплаты клиентам вычитаются не из прибыли компании, а из вкладов предыдущих клиентов;
- вкладчика не информируют о возможных рисках;
- при банкроте компания ничего не выплачивает вкладчикам;
- скрывается информация о руководстве компании и ее реквизитах;
- вкладчиков требуют уплатить регистрационный сбор.

письмо с предложением отправить на каждый из шести кошельков по одному доллару. Далее он должен создать такое же послание и распространить его в сети, где последним, шестым номером будет вписан уже собственный номер электронного кошелька.

Интернет-мошенничество на сайтах знакомств и в социальных сетях

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

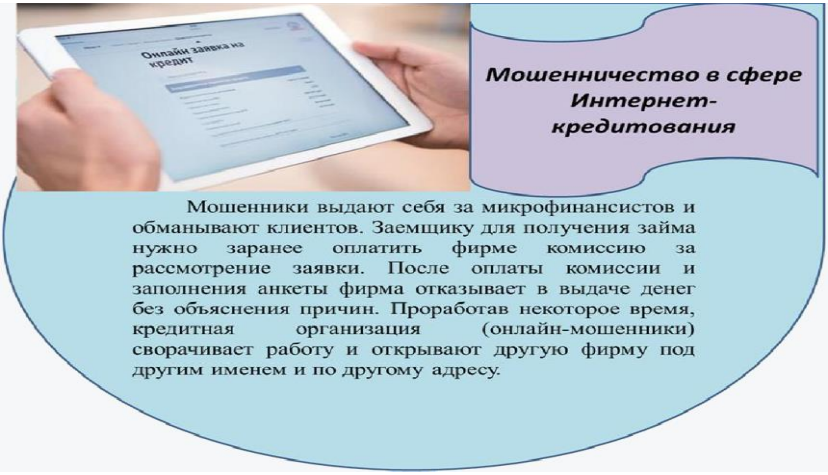


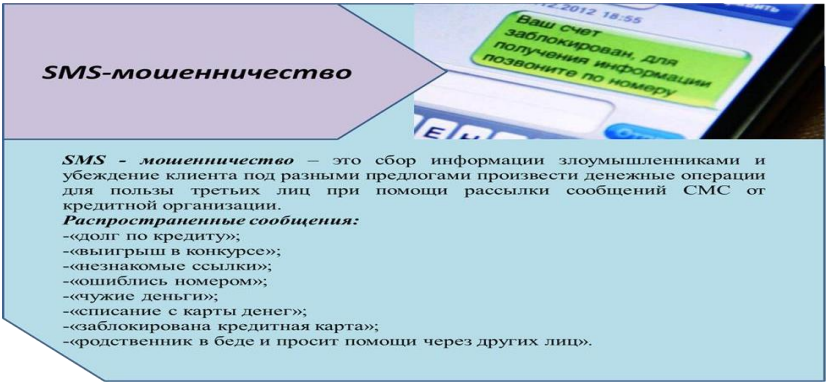
Заработок на обмене валют

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

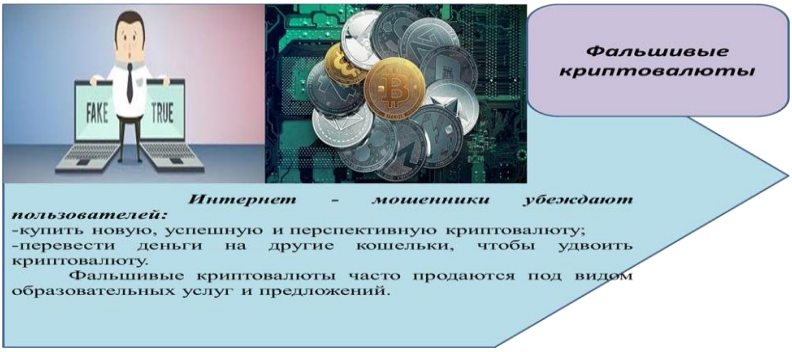
Мошенничество в сфере интернет-кредитования

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





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



Мошенничество при помощи SMS

«Нигерийские письма» – вид киберпреступности, который получил наибольшее развитие с появлением рассылок по электронной почте. Письма появились в Нигерии и распространялись по почте в бумажной форме. Мошенники, как правило, просят у получателя письма помощи в многомиллионных денежных операциях, обещая крупную сумму от процентов [25].

Интернет-мошенничество на фрилансе

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

В случаях, когда указанные деяния сопряжены с неправомерным доступом в информационную систему или сеть телекоммуникаций, содеянное подлежит квалификации по совокупности уголовных правонарушений по ст.ст. 190 и 205 УК РК, если в результате неправомерного доступа к компьютерной информации произошло уничтожение и модификация, нарушение работы ЭВМ, системы ЭВМ или их сети [26].

Мошенничество в Интернете на фрилансе

Предложения мошенников в Интернете на фрилансе:

- удаленная работа в Интернете без обмана;
- секретный заработок на тестировании платформ и сайтов;
- новый способ каждый в день зарабатывает;
- дополнительный доход не выходя из дома;
- заработок на тестах и заданиях;
-методика уникального заработка.

Объявления о выгодном заработке построены на следующих элементах:

- элементарные задачи и простота регистрации;
- обещание высокого дохода (обязательна конкретика);
- изображение банкнот и прочих материальных ценностей.

Кибersквоттинг. Кибersквоттинг (от англ. cybersquatting) – это способ заработка денег, который основан на анализе новостей рынка с целью выявления названий компаний и брендов новых товаров, для которых еще не зарегистрированы одноименные доменные имена. Обнаружив такой бренд, кибersквоттер регистрирует доменное имя на себя в надежде перепродать его впоследствии компании, владеющей соответствующим брендом [27].

Кибersквоттеры – это люди, которые регистрируют домен с целью их перепродажи [28].

Заработок кибersквоттера основан на следующих составляющих:

- *продажа доменного имени владельцу бренда;*
- *шантаж владельца бренда, который может быть основан на угрозах создать подложный сайт компании с информацией, порочащей ее честь и достоинство, или содержащий некорректную информацию о товарах.*

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

2.1. Дополнительное описание наиболее часто встречающихся схем Интернет-мошенничеств в сфере информационно-телекоммуникационных систем

Определение сочетанию терминов Интернет-мошенничество или (Электронное мошенничество и компьютерное мошенничество) – вид мошенничества с использованием Интернета. Оно может включать в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства. Интернет-мошенничество не считается отдельным преступлением, а включает ряд незаконных действий, совершаемых в киберпространстве. Однако оно отличается от кражи, поскольку в этом случае жертва добровольно и сознательно предоставляет преступнику информацию, деньги или имущество. Оно также отличается тем, что в нѐм участвуют правонарушители, разделенные во времени и пространстве.

Согласно отчѐту ФБР о преступлениях в Интернете за 2019 год, Центр жалоб о преступлениях в Интернете (англ. *Internet Crime Complaint Center*) получил более 467 тысяч жалоб. Жертвы потеряли более 3,5 млрд долларов из-за онлайн-мошенничества в 2019 году. Согласно исследованию, проведѐнному Центром стратегических и международных исследований (англ. *Centerfor Strategicand International Studies)* иMcAfee, киберпреступность обходится мировой экономике в 600 млрд долларов, что составляет 0,8% от общего мирового ВВП. Мошенничество в Интернете проявляется во многих формах: от почтового спама до онлайн-жульничества [29].

Рассмотрим непосредственно виды Интернет-мошенничеств:

Мошенничество с благотворительностью. Мошенник прикидывается представителем благотворительной организации, собирающей средства на помощь жертвам стихийного бедствия, террористической атаки, регионального конфликта или эпидемии. Также средства могут собирать без привязки к конкретному событию, а, например, на исследования рака,

СПИДа или вируса эбола, детские приюты. Мошенники могут выдавать себя за такие благотворительные организации, как Красный Крест или ООН. Мошенник просит пожертвования, часто ссылаясь на новостные статьи в Интернете, чтобы подкрепить свою историю о сборе средств. Жертвы таких мошенников – это благотворительные люди, которые верят, что помогают достойному делу, и ничего не ждут взамен.

Мошенничество с билетами. Мошенничество с билетами является одной из разновидностей мошенничества в интернет-маркетинге. Злоумышленники предлагают билеты на популярные мероприятия, такие как концерты, шоу и спортивные мероприятия. В результате билеты являются поддельными или не доставляются покупателям. Распространение онлайн-агентств по продаже билетов и существование опытных и нечестных продавцов подпитывают этот вид мошенничества. Многие из таких мошенников управляются британскими билетными рекламодателями, хотя они могут базировать свои операции и в других странах.

Ярким примером стало глобальное мошенничество с билетами на Олимпийские игры в Пекине 2008 года, осуществляемое зарегистрированной в США компанией «Xclusive Leisure and Hospitality», продававшей билеты через этот сайт были проданы поддельные билеты на сумму более 50 миллионов долларов. За аферой стоял британский продавец билетов Теренс Шепард [29].

Мошенничество с подарочными картами. В последнее время преступники всѐ чаще занимаются мошенничеством с использованием подарочных карт магазинов.

В частности, злоумышленники пытаются получить информацию, касающуюся подарочных карт, которые были выпущены, но не были использованы. Некоторые из методов кражи данных подарочных карт включают в себя ботов, которые запускают атаки методом «грубой силы» на розничные системы, которые их хранят. Сначала хакеры крадут данные подарочной карты, проверяют существующий баланс через онлайн-сервис магазина, а затем пытаются использовать эти

средства для покупки товаров или перепродажи на стороннем веб-сайте. В случаях перепродажи подарочных карт злоумышленники забирают оставшуюся сумму наличными, что также можно использовать как метод отмывания денег.

Мошенничество с платежными картами. Кардинг (от англ. carding) – вид мошенничества, при котором производится операция с использованием платежной карты или еѐ реквизитов, не инициированная или не подтверждѐнная еѐ держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчѐтных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространѐнным методом похищения номеров платежных карт на сегодня является фишинг (англ. phishing, искаженное «fishing» – «рыбалка») – создание мошенниками сайта, который будет пользоваться доверием у пользователя, например – сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт.

Одним из самых масштабных преступлений в области мошенничества с платежными картами считается взлом глобального процессинга кредитных карт Worldpay и кража с помощью его данных более 9 миллионов долларов США. В ноябре 2009 года по этому делу были предъявлены обвинения преступной группе, состоящей из граждан государств СНГ.

Украденная или потерянная карта может использоваться преступниками только до тех пор, пока владелец не сообщит своему банку о пропаже, либо в оффлайновых операциях. Большинство банков предоставляют круглосуточную телефонную линию для подобных сообщений.

Основной защитной мерой является наличие подписи на карте и требование подписывания чеков. В некоторых магазинах при оплате картой требуется предоставление документов, удостоверяющих личность. Однако требование документа в некоторых юрисдикциях является незаконным.

Существуют программные системы и комплекс организационных мер, направленных на предотвращение или усложнение возможных мошеннических операций. Например, крупная транзакция, совершенная далеко от места жительства владельца – как вариант – в другой стране, может быть признана несостоявшейся или даже привести к временному блокированию карты [29].

Мошенничества с банковскими картами. Банковские карты остаются главной целью преступников, которые используют и старые способы телефонного или интернет-мошенничества, и изобретают новые виды для кражи средств граждан. Давно известный, но тем не менее работающий способ:

– звонок из службы безопасности банка;

– сообщение о выигрыше в лотерею;

– СМС о том, что карта заблокирована.

Конечная цель мошенников всегда одна – узнать личные данные: номер карты, срок ее действия, CVC/CVV-код или коды из СМС – сообщения, с помощью которых они входят в личный кабинет онлайн-банка жертвы и переводят деньги со счетов либо оформляют на человека кредит.

В 2022 году стало известно о новом способе мошенничества с банковскими картами. Злоумышленники заманивают людей в фейковые инвестиционные проекты, а для того чтобы усыпить их бдительность, переводят на карту некоторую сумму денег, в среднем 10-15 тыс. рублей. У потенциальной жертвы возрастает доверие, снижается чувство осторожности, человек переводит мошенникам гораздо больше средств в надежде на высокий доход.

Операции без карты. Для проведения транзакции требуются лишь некоторые данные, написанные на карте. Обычно карта содержит (в виде надписи и на магнитной полосе): имя владельца, номер карты (PAN), месяц и год окончания срока действия, верификационный код (CVV2). Существуют операции, в которых не требуется физического наличия карты, а транзакция проводится лишь по данным. Мини-

мальный необходимый набор информации – номер карты, часто также требуется срок окончания, чуть реже – верификационный код. Злоумышленник может скопировать эти данные, если вступит в сговор с лицами, имеющими доступ к картам, например, с официантом или кассиром. Данные могут быть сфотографированы или восстановлены из видеозаписи. Также получение подобных данных возможно с помощью вируса, установленного на компьютере пользователя, методами социальной инженерии, (имитация звонка из банка) либо путѐм взлома интернет-магазинов или систем, обслуживающих карты. Затем преступники используют данные в операциях без присутствия карты.

Некоторую защиту от такого рода преступлений предоставляет внедрение оперативных уведомлений о проведении операций. Также частично от такого мошенничества защищают технологии 3-D Secure, Master Card Security Code, Verified by Visa, в которых для проведения операции требуется ввод дополнительного кода, получаемого в отделении банка, через банкомат, по SMS или с помощью аппаратного генератора кодов (токен) [29].

Скимминг. Частным случаем кардинга является **скимминг** (от англ.*skim* – снимать сливки), при котором используется **скиммер** – инструмент злоумышленника для считывания, например, магнитной дорожки платѐжной карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств:

– инструмент для считывания магнитной дорожки платѐжной карты – представляет собой устройство, устанавливаемое в картоприѐмник, и кардридер на входной двери в зону обслуживания клиентов в помещении банка. Представляет собой устройство со считывающей магнитной головкой, усилителем – преобразователем, памятью и переходником для подключения к компьютеру. Скиммеры могут быть портативными, миниатюрными. Основная идея и задача скимминга – считать необходимые данные (содержимое дорожки/трека) магнитной полосы карты для последующего вос-

произведения её на поддельной. Таким образом, при оформлении операции по поддельной карте авторизоционный запрос и списание денежных средств по мошеннической транзакции будут осуществлены со счета оригинальной, «скиммированной» карты.

– миниатюрная видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру ввода в виде козырька банкомата либо посторонних накладок, например, рекламных материалов – используется вкупе со скиммером для получения ПИН держателя, что позволяет получать наличные в банкоматах по поддельной карте (имея данные дорожки и ПИН оригинальной).

– Использование вредоносного кода, встроенного в банкомат. Дампы банковских карт записываются без использования спецоборудования и распознать такой способ обывателю невозможно, но встречается он крайне редко и в большинстве случаев преобладает среди маленьких банков. Дальше с помощью дампов создаются копии карт.

Данные устройства питаются от автономных источников энергии – миниатюрных батарей электропитания, и для затруднения обнаружения, как правило, изготавливаются и маскируются под цвет и форму банкомата.

Скиммеры могут накапливать украденную информацию о пластиковых картах, либо дистанционно передавать её по радиоканалу злоумышленникам, находящимся поблизости. После копирования информации с карты мошенники изготавливают дубликат карты и, зная ПИН, снимают все деньги в пределах лимита выдачи. Также мошенники могут использовать полученную информацию о банковской карте для совершения покупок в торговых точках [29].

По итогам 2020 года в Казахстане было зафиксировано 11 тыс. кибератак что – на 23,4% меньше по сравнению с аналогичным периодом прошлого года – 14,4 тыс. При этом стоит отметить, что снижение обусловлено в основном сокращением числа кибератак-ботнетов: минус 42% за год. Доля этого вида от общего количества атак составила 63,2%,

пишет ranking.kz. [30].

Ботнет.

Ботнет (англ. botnet, МФА: [ˈbɒtnɛt]; произошло от слов robot и network) – компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами автономным программным обеспечением. Чаще всего ботв составе ботнета является программой, скрытноустанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражѐнного компьютера. Обычно используются для не легальной или не одобряемой деятельности – рассылки спама, перебора паролей на удалѐнной системе, атак на отказ в обслуживани и (DoS- и DDoS-атаки) [31].

Специалисты напоминают, что ботнет – это сеть компьютеров, зараженных вредоносной программой, позволяющей злоумышленникам удаленно управлять чужими машинами без ведома их владельцев.

Фишинг. Фишинг (англ. Phishing от fishing «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей-логинами паролям. Это достигается путѐм массовых рассылок электронных писем от имени популярных брендов, а так же личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне не отличимый от настоящего, либо на сайт среди ректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приѐмами побудить пользователя в вести на поддельной странице свои логини пароль, которые он использует для доступа к определѐнному сайту, что позволяет мошенникам получить доступ как к аунтами банковским счетам [32].

Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои

учѐтные данные, пароль и прочее. Фишинговые атаки совершались в рассматриваемом периоде в РК 853 раза – на 12,1% больше, чем годом ранее (761 кибератак). Совершение фишинговых атак преследуется по закону.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг» [32].

Мошенники представляются сотрудниками банка.

На сегодняшний день особо распространенным видом мошенничества также является и то, когда мошенники представляются сотрудниками банка. Как устроен бизнес мошенников, звонящих как представители банка. Волна мошенничества с банковскими картами оставляет тысячи людей без копейки. Казалось бы, схема стара, как мир. Но почему она до сих пор работает?

Как работает этот вид мошенничества. Цель мошенников – завладеть деньгами. Для этого достаточно получить полные данные карты (номер, дата окончания срока действия и CVV/CVC-код), создать с неѐ перевод и подтвердить его кодом из SMS, которое придет на ваш телефон.

Самый популярный способ сделать это позвонить и представиться сотрудником банка. Повод может быть любой:

– агрессивный: ваша карта заблокирована;

– нейтральный: нам нужно уточнить ваши данные, подтвердите перевод с карты и т.д.;

– соблазняющим: вам пришел перевод на несколько тысяч, чтобы получить его, сообщите данные карты.

Количество вариантов зависит от фантазии организаторов схемы. Им выгодно менять формат, чтобы жертвы не привыкали.

Как мошенники узнают ваше имя и личные данные? Мошенникам даже не надо знать номер вашей карты. Достаточно номера мобильного. Часто по номеру мобильного можно узнать, как вас зовут. В различных мобильных приложениях часто отражается Ваше имя, отчество и первую букву фамилии. Иванов – имя и первую букву фамилии.

Откуда мошенники берут номера телефонов для обзвона. Раньше данные банковских карт выманивались в основном одним человеком. Нередко они при этом находились под заключением. Также их карты были зарегистрированы на подставных лиц.

Сейчас же таким видом мошенничества занимаются целые колл-центры. Данные массово распространяются – телефоны берут на сайтах бесплатных объявлений, в социальных сетях. Чаще всего их распространяют сами сотрудники банков. В этой информации обычно есть ФИО, номер телефона и часть номера карты.

Наконец, мошенники используют «дыры» в ПО. Через них похищают либо данные клиентов, либо воруют деньги. В интернете можно найти информацию о том, что, один известный банк только недавно закрыл дыру, которая позволяла сделать перевод без согласия клиента. Не требовалось даже CVV – только номер карты, телефона и одноразовый код из SMS. Такие уязвимости в системе приносят кому-то стабильный доход.

Как работают «чѐрные» колл-центры мошенников: Набрать персонал в такой колл-центр несложно. У таких сомнительных организаций есть подготовленная методичка и скрипты, отточенные на реальных людях.

Рекламу подобных вакансий часто появляется в интернете и социальных сетях, с подобным тексом: – Требуется сотрудник в новый колл-центр, работа в финансовой сфере, зарплата от $1000 + бонусы‖. Работать в подобные колл-центры идут люди, которые хотят быстрых и легких денег.

Люди из мест лишения свободы тоже порой работают на такие колл-центры. Особенно если уже имели опыт в данных аферах.

Как делятся доходы в черных колл-центрах: Люди, работавшие в подобных схемах, анонимно сообщали, что «прозвонщик» получает до 20%от суммы, если работает один. Если один человек сделку открывает, второй – закрывает, то оба получают по 10%. Остальные деньги – зарплата организаторов схем, оплата – крыши‖, закупка оборудования, аренда офисов. Деньги нужны на покупку данных: уникальная база обойдется в пару тысяч долларов, доступ к общей вдвое дешевле. Деньги выводят через карты, оформленные на случайных людей. «Дропы» снимают их в банкоматах.

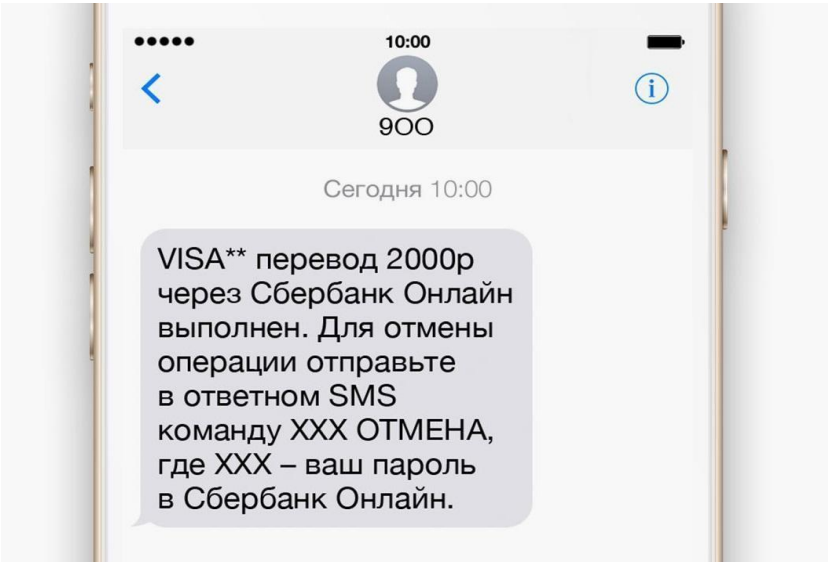
Но в последнее время мошенники чаще используют криптовалюту. Она не имеет правового статуса во многих странах и часто не позволяет отследить транзакции (особенно если это анонимная монета вроде Monero или ZCash либо используется сервис-миксер).

В крупном городе может быть несколько десятков фирм, которые занимаются такого рода мошенничеством. В большинстве случаев сложно понять, что с вами разговаривает мошенник, потому что это подготовленные специалисты, которые работают по заранее подготовленному тексту.

Для создателей таких схем обмануть и украсть у клиентов банков – просто бизнес. Который не стоит на месте, а растет и развивается.

Совершенствуются скрипты. Оттачиваются приемы психологического давления. Покупаются все более подробные базы. Работают с наиболее уязвимыми в обществе людьми.

Простой эксперимент: можно позвонить десяти пожилым знакомым, представиться сотрудником банка и попросить назвать данные карты.



Часто колл-центры маскируют настоящие номера банков похожими комбинациями букв и цифр. В результате 900 превращается в 9ОО – 9 и две буквы – О‖, например.

Мошенники используют заранее записанные фрагменты, чтобы убедить своих жертв в серьѐзности системы. Вот пример:

Но это история не про высокие технологии. А про методы социальной инженерии. И про доверие к человеку, наделенному пусть маленькой, но властью. Тем более если он делает вид, что хочет помочь.

Раньше «разводилы» работали топорнее, давили авторитетом, угрожали.

Теперь это – команда профессионалов‖.

Каждый из работников таких злоумышленных колл-центров будет готов потратить на «клиента» 10-20 минут времени или больше.

Что делать, если кажется, что звонок из банка был мошенническим?

Если хоть немного появляются сомнения в том, что вам звонит сотрудник банка, нужно немедленно положить трубку. А затем перезвонить в банк – номер горячей линии указывается на самой карте. Также он есть на официальном сайте банка и в мобильном приложении.

1. Если у мошенников могут быть данные карты, нужно незамедлительно заблокировать еѐ, по средствам телефонного звонка в банк или в мобильном приложении. Такие же действия нужно предпринять, если на мобильный телефон приходит SMS от банка о странном списании средств или при обнаружении подозрительной покупки в истории транзакций мобильного приложения.

2. Как правило, сотрудники банка никогда не спросят номер карты и CVV/CVC-код или PIN-код.

Специалист может уточнить лишь последние четыре цифры карты, чтобы понять, с какой именно из ваших карт предстоит работать. Сотрудники крайне редко задают дополнительные вопросы – только если вы забыли ответ на секретный вопрос и хотите сменить пароль.

Сотрудники банков в редких случаях звонят, если случилось что-то с картой или если нужно предложить новую услугу.

3. Стоит помнить, что все решения, кроме блокировки карты, можно принять позднее. Поэтому, выдохните и положите трубку. А потом перезвоните сами в банк по номеру, который указан на вашей карте.

4. Самым достоверным и безопасным способом защититься и получить информацию, является обратиться в отделение банка. Там сотрудники помогут вам решить проблему.

Главное: если мошенники таким образом выудят деньги, вернуть их будет практически невозможно.

Удаленный рабочий стол Remote Desktop Protocol (RDP). Все еще встречаются случаи, когда порт TCP 3389 открыт для доступа снаружи для технических целей. Напри-

мер, при обслуживании сторонней организацией программы «1С-Бухгалтерия», либо для нужд администрирования. Дело в том, что за портами удаленного доступа постоянно ведется наблюдение. Хакерами регулярно сканируются публичные сети и выполняется подбор паролей к целевым хостам. Далее злоумышленник вручную выполняет шифрование, предварительно отключив все протоколирующие и восстановительные механизмы системы (журналирование, создание теневых копий файлов).

Кроме того, при ручном проникновении хакеры часто прибегают к помощи утилиты Mimikatz, позволяющей при необходимости повысить привилегии доступа для запуска шифровальщика с административными правами. Mimikatz – инструмент для перехвата паролей открытых сессий в Windows, реализующий набор функций Windows Credential Editor. Он способен извлекать аутентификационные данные зарегистрировавшегося в системе пользователя в открытом виде [33].

Киберпреступники с помощью хакерских атак и шифровальщиков получили в качестве выкупа $144 миллиона в криптовалюте за последние 7 лет. Основная доля приходится на биткоины, которые были потом отмыты с помощью миксеров и бирж.

Хакерские атаки, в результате которых шифруются данные на компьютерах, а за их дешифровку киберпреступники требуют выкуп, входят в число крупнейших киберугроз последних лет. Вымогатели атаковали информационную инфраструктуру аэропортов и больниц, проникая в старые, уязвимые машины и блокируя доступ к важным данным. Большинство вымогателей требуют выкуп в криптовалютах, а самой популярной криптовалютой несмотря на отсутствие анонимности остается биткоин. Несмотря на то что правоохранительные органы советуют не выплачивать выкуп, так как часто вымогатели не выполняют свои обещания и вместо дешифровки жертва получает письмо с новым требованием выкупа, за последние годы киберпреступники заработали несколько десятков миллионов долларов на подобном мошенничестве.

Можно привести популярный пример из Соединенных Штатов Америки, специальный агент ФБР Джоэл Де Капуа поделился результатами исследования относительно крипто-вымогателей во время конференции RSA 2020. Он рассказал, что с октября 2013 по ноябрь 2019 год крипто-вымогатели получили $144 млн в криптовалюте. Полученные в качестве выкупа биткоины и другие криптовалюты немедленно отправлялись в миксеры или продавались на биржах. Он также добавил, что у поведения компаний, которые соглашаются на выкуп, есть причина: юр. лица, ставшие жертвами шифровальщиков, могут подать заявку на получение страховки [34].

Звонки из правоохранительных органов, особенно часто с ОВД мошенники осуществляют звонки гражданам под видом сотрудников полиции. Этот вид мошенни-

чества существует очень давно, но все еще остается актуальным в 2022 году. Мошенники звонят под видом сотрудника МВД, представляются лейтенантом полиции или работником следственного управления и сообщают гражданину, что прямо сейчас с его счета происходит хищение средств или на его имя, оформляют кредит. Для спасения денег или недопущения оформления кредита следует перевести средства на «безопасный счет» или самостоятельно оформить кредит и тут же вернуть его, опять же на якобы специальный счет. Иногда потенциальной жертве предлагают дойти до банкомата, снять средства и передать их «сотруднику полиции», который участвует в спецоперации по поимке преступников.

Для того чтобы избежать последствий от такого вида интернет-мошенничества необходимо выполнить следующие действия:

– немедленно положить трубку;

– если на телефон поступают СМС, не отправлять ответные сообщения;

– проверить состояние счетов, карт в мобильном или онлайн-банке;

– при возникновении сомнений, подозрений – самостоятельно позвонить в банк и проконсультироваться о дальнейших действиях.

Очень важно знать! Сотрудники банка никогда не выясняют количество денег на счете или в каких еще банках у клиента открыты счета, не спрашивают CVC, CVV-код, не предлагают перевести деньги куда-либо.

Ложные сайты – Создание ложных интернет-сайтов в настоящее время является одним из основных видов мошенничества, совершаемых посредством использования сети Интернет, которая является самой большой торговой площадкой в мире, с неограниченным территориальным пространством. Огромное количество торговых площадок, посредством которых у потребителя имеется возможность выбрать

себе товар на разных сайтах и приобрести его по низкой цене, оплатив безналичным расчетом. Эти расширенные функции и доверие потребителей дает злоумышленникам возможность создавать сайты-двойники известных торговых платформ при помощи фарминга.

При совершении фиктивной покупки покупатель перечисляет свои деньги мошеннику, либо передает конфиденциальные данные своей банковской карты. Как правило фиктивные ресурсы очень быстро прекращают свою работу, и установить владельца данного ресурса сложно в силу того, что регистрация сайта осуществляется дистанционно и полностью анонимно, поэтому даже специальные службы бывают бессильны.

Вредоносные программы – Другой разновидностью дистанционного мошенничества является создание вредоносных программ, с помощью которых похищаются персональные данные пользователей. Вредоносные программы устанавливаются на электронные гаджеты с целью получения доступа к данным о банковских картах и счетах пользователей.

Возможность бесконтактной оплаты – напрямую связанна с закреплением в устройствах сведений о банковских картах и счетах, предоставляет мошенникам создавать и под различными предлогами принуждать потерпевших устанавливать данные программы на свои устройства. После установки, программа, заполучив необходимые сведения через Интернет передает необходимые данные злоумышленнику, который получает доступ к финансам потерпевшего и распоряжается ими по своему усмотрению.

Похищение персональных данных. В отличии от предыдущего вида, похищение персональных данных может использоваться из хулиганских побуждений, с целью повреждения используемого устройства. Похищение персональных данных может сопровождаться похищением сведений,

порочащих честь и достоинство пострадавших. Ярким примером такого преступления является похищение фотографий личного содержания известных лиц кино и музыкальной индустрии. Злоумышленники, заполучив подобного рода компрометирующие сведения, начинают шантажировать жертву, требуя денежных переводов под угрозой публикации полученных сведений.

Фиктивные сделки. Оформление фиктивных сделок с помощью Интернет ресурсов, связано прежде всего с различными сферами жизни общества, как правило купли-продажи товаров и вещей или покупки чего-либо в интернет-магазине. При таком способе обмана злоумышленник получает от жертвы денежные средства, под предлогом предоплаты или оплаты доставки, а после либо не отвечает, либо исчезает.

Мошенничество с криптовалютами. В последние годы в ряде государств СНГ увеличивается незаконная деятельность финансовых пирамид, большая часть из них привлекает средства в криптовалюте или рекламируют вложения в различные несуществующие криптовалютные активы.

Однако, криптовалюта – уже привычное явление для общества, по сравнению с не так давно появившимся, набирающим популярность технологией NFT, с появлением которой вышли новые виды мошенничества в Интернете. В частности, мошенники начали распространять вредоносные программы для нелегального майнинга криптовалют и кражи средств с крипто-кошельков через уникальные токены NFT и мобильные приложения.

В начале 2022 года были зафиксированы такие новые виды мошенничества, как «криптовалюта в подарок». Злоумышленники делают фишинговые рассылки и сайты-подделки с предложениями вместо традиционных наскучивших подарков удивить друзей и близких презентом в виде криптовалюты. Однако, если человек перечисляет деньги за

псевдокрипту, вывести деньги с ресурса не удастся.

Еще один сценарий – предложение удвоить объем своей крипты, послав на некий кошелек любую сумму и получив обратно в два раза больше. Часто такие сообщения рассылаются в социальных сетях от имени известных личностей, например, Илона Маска, с посланем, что он хочет сделать подарок для своих пользователей. Очевидно, что, получить назад и в два раза больше уже у потребителей не получится [35].

Чтобы обезопасить себя от такого рода Интернет-мошенничеств, необходимо быть грамотным в социальных сетях, уметь различать правдивую информацию и всегда перепроверять источник. Поскольку большинство граждан все же не очень хорошо ориентируется в вопросах криптовалют, стать жертвой мошенников очень просто.

2.2. Влияние Интернет-мошенничества на пользователей информационно-телекоммуникационных сетей, систем и технологий

Как правило, на уловки Интернет-мошенников попадаются пользователи, которые не знакомы с правилами безопасности пользования Интернетом и не разбираются в принципах информационной безопасности. Люди, относящиеся к такому классу пользователей, очень легко идут на контакт с Интернет- мошенниками и без опасений передают всю необходимую от них информацию, не подозревая об угрозе и последствиях. Жертвы мошеннических действий, а также пользователи, знания которых недостаточны для защиты своих личных данных, зачастую перестают пользоваться и доверять ресурсам, находящимся в сети: различным Интернет-покупкам таким как: Интернет-магазины, площадки с объявлениями, личным кабинетам банковским услугам и т.п.

Рассмотрим пример, как мошенничество может

влиять на пользователей Интернета и целые системы.

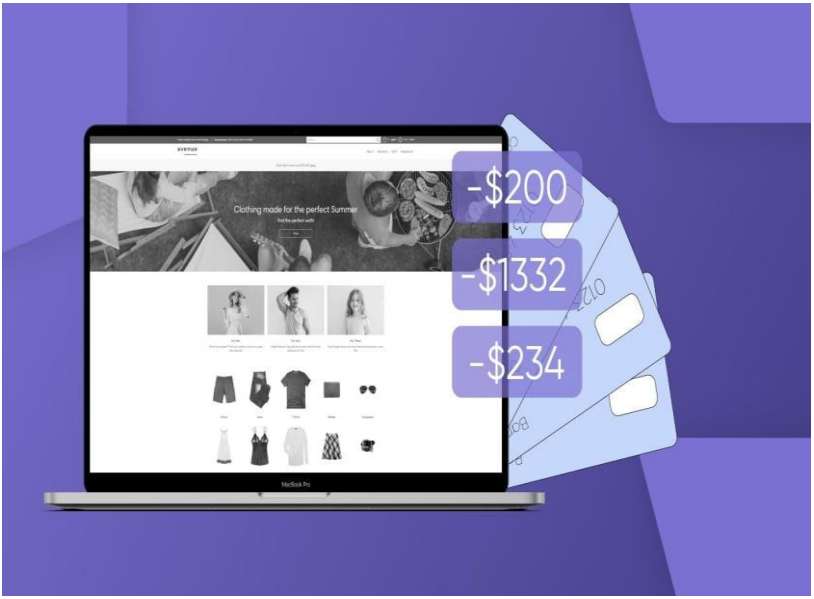
Что такое «**фрод**», и как мошенничество влияет на ecommerce-бизнес

Мошенничество в сфере e-commerce с каждым годом становится все более «совершенным», и онлайн-ритейлеры вынуждены бороться с этой серьезной проблемой. Какова причина столь многократного распространения фрод-транзакций по всему миру за последний год и какие действия, могут быть предприняты, чтобы минимизировать потери от операций мошенников.

Что такое «фрод»?

Фрод (eng. Fraud) – это мошеннические операции, в частности, в сети Интернет. Существуют разнообразные виды мошенничества, большая часть которых нацелена на получение или использование данных банковской карты другого человека [36].

Последние несколько лет сфера e-commerce переживала экспоненциальный рост мошеннических атак. Повсеместная цифровизация консолидировала данные, упростила процессы и значительно повысила эффективность администрирования, но, таким образом, предоставила мошенникам огромные возможности – преимущественно за счет широкого распространения онлайн-шопинга.



Почему интернет-магазины так привлекательны для мошенников?

Мошенничество в электронной торговле – невероятно прибыльное дело, если оно грамотно спланировано и успешно выполнено. Интернет-магазины с возможностью оплаты на сайте – очевидная цель для киберпреступников, поскольку им намного проще скрыться за ложными сведениями и скрыть следы мошенничества. Увеличение количества международных транзакций еще больше упростило этот процесс,

добавив уровни сложности в виде языковых барьеров и доставки на большие расстояния [36].

К сожалению, часто компании электронной коммерции не знают насколько они уязвимы, пока не подвергаются первой атаке. Цифровое развитие – это неизбежный процесс, а развитие киберпреступности – растущая проблема, с которой ни одна организация не может справиться в одиночку. Однако, онлайн-магазины часто пренебрегают действиями по снижению fraud – заказов по ряду причин. Одна из самых распространенных – простое непонимание. Если бы интернет-магазины действительно понимали ущерб, который мошенники могут нанести их компаниям, они были бы более склонны к разработке эффективных стратегий в борьбе с мошенниками.

Рассмотрим простой пример. В результате скимминга/фишинга или любых других противоправных действий реальный держатель банковской карты сам того не зная, передает злоумышленникам данные своей карты, достаточные для совершения покупки в интернет-магазине.

Злоумышленник оформляет онлайн-покупку и приобретает товар либо услугу.

Держатель карты, узнав о несанкционированном списании, заявляет о пропаже денег в банк, выпустивший карту. Банк, в свою очередь, инициирует chargeback, то есть возврат списанных средств. Возвращать эти средства должен интернет-магазин.

Если товар уже был получен злоумышленником, то интернет-магазин «попадает» трижды:

– лишается товара, который уже был отправлен;

– возвращает деньги держателю карты + платит комиссию за открытие диспута;

– процент диспутов в платежной системе увеличивается, что может грозить заморозкой денежных средств или полным запретом принимать онлайн-платежи.

Некоторые компании неохотно вкладывают средства в программное обеспечение и платформы для улучшения безопасности из-за стоимости, что является парадоксальным, но важным фактором, объясняющим почему цифровое мошенничество стало столь успешным.

Еще один важный фактор – это многоканальность электронной коммерции. Продажи через сторонние веб-сайты, такие как «Amazon, eBay и Alibaba», а также через мобильные приложения более уязвимы, потому что у мошенников больше шансов перехватить платежные данные. Сочетание непонимания, отсутствия желания инвестировать, развития киберпреступности и инфраструктуры электронной коммерции вырастило культуру компьютеризированной преступности, которая затрагивает почти все интернет-магазины, даже без их ведома [36].

Влияние мошенничества на индустрию онлайн-платежей

Что происходит, когда онлайн-бизнес (или любой дру-

гой бизнес) становится жертвой мошенничества? Наиболее очевидное последствие – потеря доходов и ресурсов. Во многих случаях мошенничество остается незамеченным, что делает данные о трафике и других показателях магазина некорректными. Не сумев защитить себя от мошенничества по какой-либо причине, жертва может оказаться в очень тяжелом положении.

Мошеннические атаки не только наносят ущерб самим интернет- магазинам, но и могут негативно повлиять на потребителей. Ничего не подозревающие клиенты, совершая покупки на фиктивных сайтах, становятся жертвами кражи данных и их использования для совершения покупок у реальных продавцов. Все это может саботировать отношения между покупателями и бизнесом, что плохо отразится на репутации компании в целом.

С какими видами мошенничества сталкиваются интернет-магазины? Хотя кража банковских карт и реквизитов счетов для совершения платежей являются наиболее распространенным методом мошенничества, но киберпреступники также охотятся за номерами телефонов, датами рождения, адресами и т.д.

Как онлайн-ритейлерам защитить бизнес от мошенничества?

На данный момент невозможно полностью оградить себя от мошенничества в сфере электронной коммерции. По мере развития технологий меняются и тактики, используемые для проникновения в цифровой бизнес. Мошенники, конечно, предусмотрительны, но часто оставляют следы. Знание того, что как они работают и как их обнаружить, – мощное оружие в борьбе с мошенничеством.

Антифрод – это система мониторинга и предотвращения мошеннических операций, которая в режиме реального времени проверяет каждый платеж, прогоняя его через десятки, а порой сотни фильтров. Механизмы антифрода работают таким образом, чтобы проследить, нет ли в пла-

теже чего-либо «необычного». Задача системы – проверить каждую транзакцию, найти «подозрительные» моменты и вынести решение – отклонить платеж или пропустить его.

Система антифрода состоит из нескольких компонентов:

– автоматический мониторинг транзакций, включающий в себя множество настраиваемых фильтров;

– механизмы аутентификации держателя карты и валидации карты;

– мониторинг транзакций в «ручном» режиме для крайних случаев.

Платежная система может включать в себя сотни различных фильтров, и чем больше сфера бизнеса подвержена мошенническим действиям, тем больше фильтров включается и каждый из них настраивается более детально под конкретный интернет-магазин или онлайн-сервис. Системы фрод-мониторинга работают не совершенно, поэтому, чтобы избежать возможных неприятных ситуаций, необходимо проверять заказы вручную.

Поверхностными сигналами фрода могут служить:

– необычно крупные заказы;

– множественные заказы за короткий период времени;

– подозрительные адреса электронной почты;

– IP в черном списке;

– несоответствие между billing и shipping адресом.

Следует особенно внимательно отслеживать такие проявления в периоды высокой активности, например, в «черную пятницу» или в период Рождества.

Первым делом необходимо внимательно изучить поле с данными владельца карты – совпадает ли почта и имя, платежные и почтовые данные. Если почта написана на латинице, но вы видите русское слово, вам следует обратить внимание – гражданам зарубежных стран это не характерно. Если шипинг и биллинг адреса разные, вам следует связаться с покупателем в ближайшее время и запросить чек или скриншот

транзакции из приложения банка [36].

Таким образом, динамический комплексный подход к борьбе с мошенничеством должен включать:

– Проверка адреса (AVS);
– CVV-проверка;
– Геолокация;
– Технология 3D Secure;
– Проверка прокси;
– Проверка IP в черных списках.

Все эти инструменты делают процесс оценки транзакции на fraud более качественным.

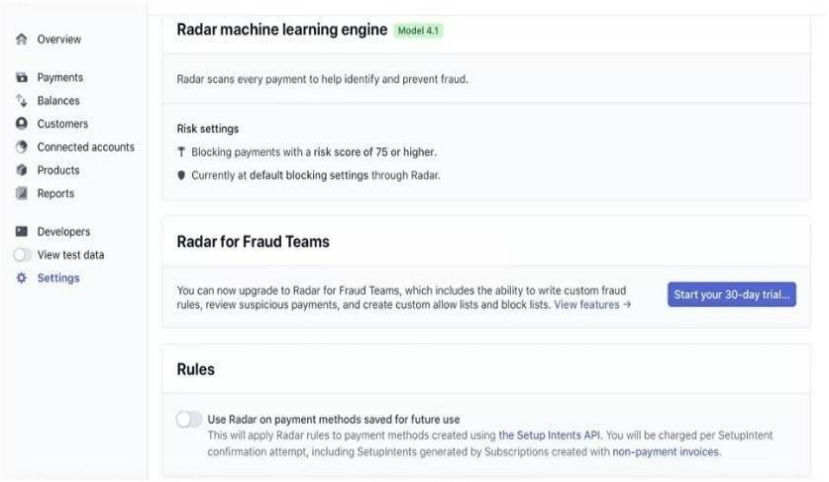
Для эффективной аналитики fraud-транзакций используются как внутренние механизмы платежных систем, так и сторонние сервисы. В зависимости от платежной системы уровень эффективности антифрод системы сильно варьируется. В качестве примера, рассматривается возможность одной из наиболее надежных и популярных международных систем Stripe.

Систему Stripe отличает высокая скорость обработки платежей и безопасность, а с точки зрения бизнеса – очень удобные средства интеграции с сайтами и интернет-магазинами. Встроенная в Stripe антифрод система Radar предоставляет возможность эффективно оценивать уровень риска каждого платежа с учетом данных о миллионах платежей во всем мире в режиме реального времени.

Возможности StripeRadar в борьбе с фродом

Stripe Radar помогает обнаруживать и блокировать мошенничество для любого типа бизнеса с помощью машинного обучения, которое базируется на данных миллионов компаний по всему миру. Сервис встроен в Stripe и не требует дополнительной настройки для начала работы.

В основе Stripe Radar лежит адаптивная система машинного обучения, которая оценивает уровень риска каждого платежа в режиме реального времени. Система использует сотни фильтров при обработке каждого платежа и постоянно анализирует данные о миллиардах транзакций, проходя-



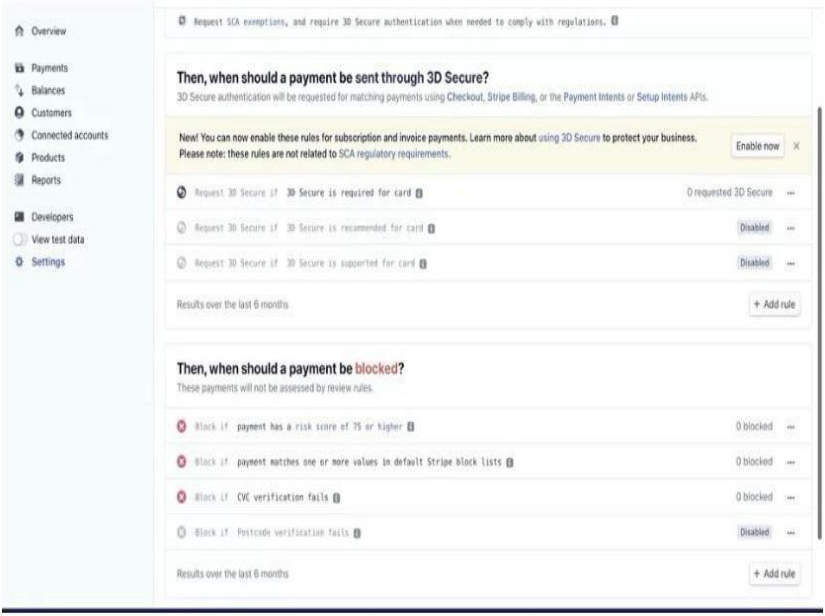
щих через платежную систему Stripe по всему миру с целью предсказать вероятность мошенничества наиболее точно [36].

Stripe Radar является самой гибкой и быстро реагирующей системой, постоянно учится на новых проявлениях фрода и особенностях транзакций, а также учитывает фидбек всякий раз, когда платежи ложно указываются как мошеннические.

Stripe Radar с наименьшей долей вероятности (в сравнении с другими антифрод-системами) будет блокировать платежи реальных покупателей. Radar отличает мошенников от клиентов благодаря применению Dynamic 3D Secure к платежам с высоким риском [36].

Алгоритмы Radar быстро адаптируются к меняющимся методам мошенничества – система постоянно подстраивает-

ся под ваш бизнес с учетом ежедневного сбора данных и аналитики платежей по всему миру.



Таким образом, фрод-мониторинг позволяет своевременно обнаруживать и предотвращать мошеннические действия. Проверка каждой транзакции позволяет свести к минимуму риск мошенничества. Сегодня для обнаружения фрода платежные системы используют полностью автоматизированные решения, которые анализируют риски и блокируют подозрительные транзакции. В качестве примера была рассмотрена международная платежная система Stripe и встроенная в нее адаптивная система машинного обучения Stripe Radar, которая оценивает уровень риска каждого платежа [36].

3. Особенности выявления, раскрытия и расследования фактов мошенничества совершаемых в сети Интернет

3.1. Особенности выявление фактов мошенничества совершаемых в сети Интернет

Мошеннические посягательства на собственность в структуре преступности, находящейся в компетенции полиции, составляют около 10,5%, из них раскрываются не более 27% [37]. Это один из немногих видов преступлений, продолжающих сохранять устойчивую тенденцию роста на фоне некоторой стабилизации общей преступности. Анализ современной криминальной ситуации в стране свидетельствует о том, что происходит ее качественное перерождение [38, с. 48].

Исследование в данной области выявило ряд типичных схем мошеннических действий. Во-первых, это все виды бесконтактных мошенничеств, когда преступники обманывают потерпевших, находясь в другом городе, регионе или даже в другой стране, посредством сети «Интернет» и сотовой связи.

Рост числа интернет-магазинов, создание систем предоставления банковских услуг посредством глобальной сети, развитие платежных систем, способствует тому, что люди доверяют безналичным расчетам, забывая об осторожности.

Мошенники, стремясь обезличить себя, используют современные технические средства и программное обеспечение, ими активно используются возможности сети «Интернет» и сотовой связи. Потерпевшим приходят СМС под видом розыгрыша лотерей, блокирования банковских карт, сведений о совершении преступлений или административных правонарушений близкими родственниками. В большинстве случаев жертвы преступлений сами оставляют сведения мошенникам в сети «Интернет», используя различные

социальные сети и программы, путем ввода персональных данных, сведений о кредитных картах [39, с. 219]. Например, фигурант уголовного дела, позвонив автору объявления, размещенного в сети «Интернет», под предлогом перевода денег за покупку товара выманил у потерпевшего реквизиты его банковской карты и одноразовые пароли доступа в личный кабинет онлайн-банкинга.

Во-вторых, это давно распространенные, типичные способы мошенничества, когда путем обмана и злоупотребления доверием преступники похищают денежные средства граждан, которым обещают содействие в получении кредита, приобретении жилища из числа арестованных квартир, покупке стройматериалов, оборудования или доставке автомашин, также возможна помощь в трудоустройстве на высокооплачиваемые должности в нефтегазовые компании, правоохранительные органы, частные медицинские клиники, строительные компании или решение вопроса о не привлечении к уголовной ответственности подозреваемого в преступлении или содействие в возврате прав, при банкротстве граждан [40, с. 140].

Таким образом, в настоящее время можно выделить следующие характерные признаки современного мошенничества:

– в его структуре преобладают преступные действия, посягающие на личную собственность граждан;

– способы совершения обмана достаточно разнообразны и чрезвычайно изменчивы;

– высокий уровень групповых мошеннических посягательств (до 50%), высокий уровень их организованности;

– межрегиональный и международный характер действий мошенников, раздел сфер преступного влияния, постепенное преобразование мошеннических групп в структурные звенья организованных преступных сообществ;

– отличительны по социально-демографическим, уго-

ловно-правовым, нравственно-психологическим характеристикам от среднестатистического корыстного преступника портрет мошенника, усиление «интеллектуализации» данной криминальной среды за счет привлечения новых участников;

– виктимное, порой неправомерное поведение части потерпевших;

– высокая латентность данного вида преступления.

Анализ оперативной обстановки в сфере борьбы с мошенническими посягательствами свидетельствует о том, что использование преступниками достижений технического прогресса (IP-телефония, зарубежные интернет-ресурсы, динамические IP-адреса, «Skype» и др. с созданием своеобразных диспетчерских пунктов, зашифрованных схем передачи информации, позволяющих им исключить визуальные контакты с потерпевшими), электронных платежных систем, средств мобильной связи значительно снижает для них риск быть задержанными в момент совершения преступления, в связи с чем, наиболее организованные группы мошенников в основном переходят на бесконтактный способ совершения преступлений.

Подобные способы совершения преступлений повышают безопасность преступной деятельности и увеличивают стремление расширить географию преступлений, создавая организованные группы.

Преступления данного вида самые трудоемкие в плане раскрытия. Практически не раскрываются по «горячим следам». Это существенно усложняет применение оперативными сотрудниками классических методов проведения оперативно-разыскных мероприятий (далее – ОРМ). На первый план выходят ОРМ, связанные с использованием технических средств, такие как прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации.

При этом, использование типовых алгоритмов при вы-

явлении способов мошенничества, в данном случае позволит лишь убедиться в том, что имеют место указанные действия, а не выявить конкретных лиц, совершающих преступления.

Документирование совершаемых преступлений, во многих случаях крайне затруднительно, а установление злоумышленников зачастую сложно, а порой и невозможно, что влечет проблемы в сборе доказательной базы.

Все это требует со стороны правоохранительных органов качественного нового подхода к организации работы по изобличению преступной деятельности мошенников и привлечению их к уголовной ответственности.

Понятие оперативно-разыскной деятельности (далее – ОРД) неразрывно связано с ее задачами, одной из которых является выявление преступлений.

Выявление преступлений означает добывание информации об их подготовке, совершении и последствиях. Это вызвано тем, что преступник, совершая общественно опасные деяния, с целью избежать наказания практически всегда стремится скрыть сам факт преступления.

Исходя из этого, в любом государстве всегда существует определенное число латентных преступлений, выявление которых составляет определенную сложность. К таким наиболее тщательно замаскированным относятся преступления, связанные с интернет-мошенничеством.

Об уровне латентности мошенничеств можно судить по тому, что, по результатам исследований, реальный его показатель превосходит статистические данные в пять раз. Особенно характерна латентность для мошеннических посягательств на личную собственность граждан.

Это обстоятельство обусловлено несколькими факторами. Главный из них – нежелание самих потерпевших обращаться в правоохранительные органы с заявлением о совершенном в отношении них преступлении. Зачастую это объясняется их доверчивостью, неосмотрительностью, бес-

печностью или алчностью.

Первоначальным этапом выявления преступлений является поиск первичной информации. Необходимо знать, что имеется ряд причин, подчеркивающих необходимость поиска информации на информационных ресурсах в сети «Интернет» именно в рамках ОРД, так как одной из причин является то, что электронная информация, содержащая признаки преступления или сведения, позволяющие установить обстоятельства совершенного преступления, затруднительно (а порой и невозможно) обнаружить в рамках процессуальной деятельности.

Специфика электронной информации такова, что она может быть уничтожена, прежде чем получит процессуальное закрепление. При этом уничтожение информации легко выполняется не только при физическом контакте с ней преступника, но и на расстоянии, с использованием сети Интернет».

Кроме этого, своевременное обнаружение и блокирование криминальной информации, создаваемой при помощи аппаратно-программных средств и распространяемой по информационно-телекоммуникационным сетям, позволяет пресечь совершаемые преступления и предупредить новые.

Практика показывает, что в сетевом пространстве существуют ряд объектов, на которые необходимо обратить внимание и на которые осуществляются посягательства, а именно:

– сайты социальных сетей, интернет-магазины, сайты различных банков и т.д.;

– сайты, через которые проходит и распространяется информация, происходит реализация товаров и услуг;

– сайты и форумы сетевого общения криминальных лиц (различные открытые и закрытые форумы).

При этом мошенники применяют следующие методы и технологии при совершении преступлений:

– сокрытие электронной информации о своих действиях:

1) путем передачи (в т.ч. кодирования) электронных посланий. При этом используются компьютеры и электронные записные книжки для хранения следующей информации: номеров банковских счетов, баз данных потенциальных потерпевших, данных связи с сообщниками и т.д.;

2) путем использования неконтролируемых средств электронной связи. Телефоны, факсы, компьютеры применяются и непосредственно при проведении незаконных операций для передачи информации, на какой счет пересылать полученные деньги. С этой целью используются спутниковые телефоны, «клонированные» сотовые телефоны (т.е. сотовые телефоны, идентификационные коды которых, присвоенные законным пользователям, были перехвачены и записаны в сотовые телефоны преступников), телефонные карточки с предварительной оплатой, широкополосные радиочастоты, чат-комнаты в сети «Интернет» с ограниченным доступом;

– отмывание доходов от мошеннических действий с помощью электронных переводов.

Сеть «Интернет» обладает тремя специфическими свойствами, которые могут способствовать отмыванию денег: свободным доступом, анонимностью отношений между клиентом и финансовым учреждением, высокой скоростью совершения электронных сделок;

– информационное противодействие мероприятиям, проводимым органами внутренних дел.

Для выявления информации, представляющей оперативно-разыскной интерес, в первую очередь используется поиск по информационным ресурсам сети «Интернет», с применением разного рода поисковых систем (Google, Yandex, Rambler и т.п.). Информация, представляющая оперативный интерес, содержится в сетевом пространстве, на криминогенных объектах как в виде следов противоправной

деятельности, так и в виде сообщений лиц, осведомленных об обстоятельствах подготовки или совершения преступления, а также в виде ссылок на сетевые сайты и адреса, где могут быть размещены различные запрещенные к распространению сведения.

На данной стадии собираются сведения, поступающие, прежде всего, от источников оперативной информации. Поиск информации может осуществляться и в рамках изучения информации, размещаемой в сети

«Интернет». Так, изучение преступной деятельности лиц, занимающихся мошенничеством, показывает, что его особенностью является активный поиск в виде SMS-рассылок (например, информация о том, что родственник или знакомый попал в сложную жизненную ситуацию).

Также необходимо особое внимание уделять информации, получаемой в результате мониторинга интернет-сайтов и интернет-форумов.

В сети «Интернет» может осуществляться рассылка сообщений на аккаунты по «Skype» с указанием абонентских номеров сотовой связи, приложением инструкции о проведении платежей через электронные системы оплаты.

На стадии выявления сведений, представляющих оперативный интерес, большое значение имеет информационный обмен. Практически все службы и подразделения органов внутренних дел регулярно получают сведения о мошеннических действиях. Также искомую информацию можно добыть при взаимодействии с оперативными подразделениями всех правоохранительных органов.

При выявлении лиц, занимающихся интернет-мошенничеством, оперативным сотрудникам следует иметь в виду, что таким образом осуществляют преступную деятельность хорошо организованные группы, где прослеживается иерархическая организация, когда все функции участников преступной деятельности четко распределены. При этом со-

блюдается жесткая дисциплина, продумана система безопасности, имеется контроль за деятельностью лиц, занимающих низшие ступени в подобной организации.

Говоря о способах выявления Интернет-мошенничеств следует в первую очередь указать на трудности их определения.

Процесс разоблачения интернет-мошенников состоит из мероприятий, необходимых для обнаружения случаев совершения обмана, злоупотребления, прочих сомнительных деяний. Мошенничество отличается от остальных видов преступлений тем, что выявить его не так просто, как хотелось бы. Способы выявления мошенничества заключаются в определении явных признаков, связанных с преступлением, обнаружении факторов обмана.

В результате скоординированных действий борцов с преступностью рано или поздно преступники делают просчеты и допускают ошибки в своих действиях.

На что необходимо обращать внимание при выявлении фактов интернет-мошенничества:

1. Проверьте электронный адрес. Прежде чем переходить по ссылкам из письма или отвечать на него, повнимательнее взгляните на адрес отправителя. Он состоит из двух частей: имени и собственно адреса электронной почты. Имя можно указать какое угодно, мошенники нередко пользуются этим и вписывают в это поле название организации, за которую выдают себя.

А вот подменить сам адрес – тот, который с собачкой – гораздо труднее, поэтому именно здесь злоумышленники могут проколоться. В большинстве мошеннических писем адрес либо вообще не будет иметь ничего общего с названием компании, которой они притворяются, либо будет похож на настоящий, но не идентичен ему – с заменой одного или нескольких символов (например, буквы «о» на цифру «0»), какими-нибудь лишними словами в домене и так далее.

Заметили опечатки и несоответствия или увидели, что e-mail отправителя – непонятный набор, в этом случаи не отвечайте на письмо, не кликайте по ссылкам, а лучше всего сразу отправьте его в «Спам».

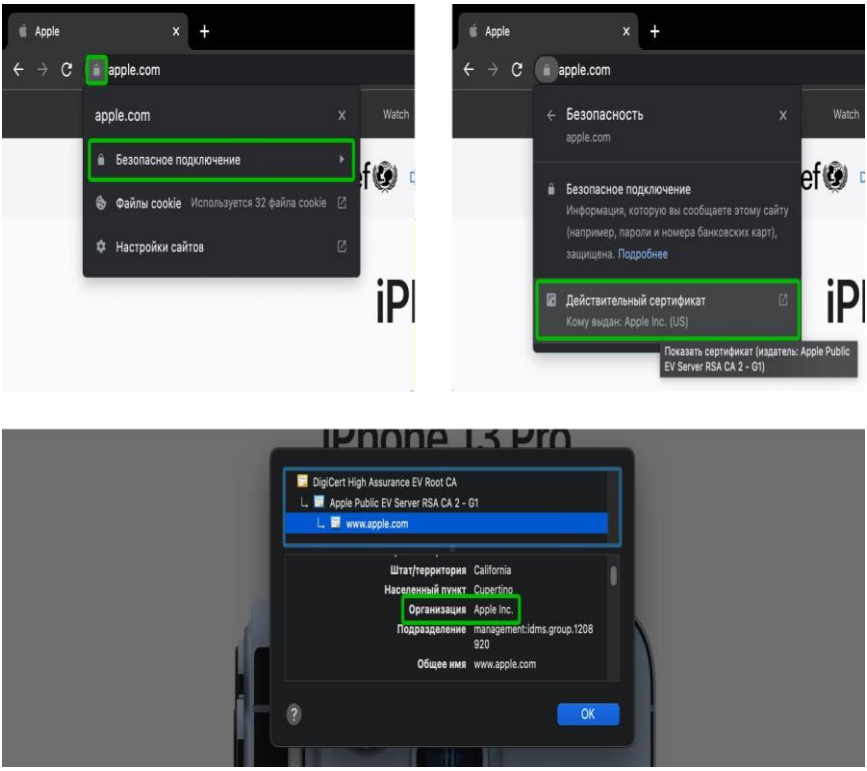
2. Изучите ссылки в письме. Если в письме есть гиперссылки или кнопки с надписью: «Получить скидку», «Забрать подарок», «Подробнее» и так далее, на которые вам намекают нажать, то стоит сразу проверить, что за ними скрывается.

Если вы наведете курсор на ссылку или кнопку, то увидите адрес веб- ресурса, на который создатели письма хотят вас отправить. Найдите через поисковик официальный сайт компании и сравните его URL со ссылкой из письма. Если адреса различаются - например, в ссылке из письма указан другой домен (скажем org или во все какой-нибудь xyz вместо нормального .ru или .com), – то открывать страницу не стоит.

Заодно, пока официальный сайт под рукой, имеет смысл открыть его и посмотреть, упомянуты ли там скидки, подарки или акции из письма. Если никаких данных о специальных предложениях там нет, то, скорее всего, с вами связались мошенники.

3. Загляните в сертификат безопасности сайта. Некоторые символы настолько похожи, что подмену практически не видно невооруженным взглядом. Поэтому есть еще один быстрый способ проверить, кому принадлежит сайт – уже после того, как вы туда зашли. Разберем на примере Google Chrome, в других браузерах названия пунктов меню могут немного отличаться.

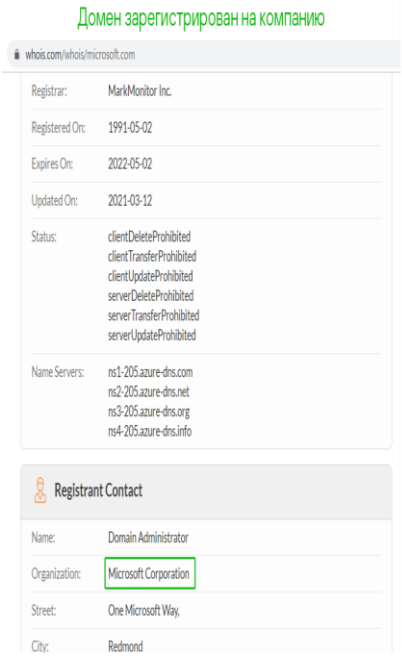
Нажмите на «замок» слева от URL-адреса. В появившемся окне выберите безопасное подключение, нажмите на действительный сертификат, убедитесь, что рядом с пунктом кому выдан, указана именно та компания, которая владеет сайтом.

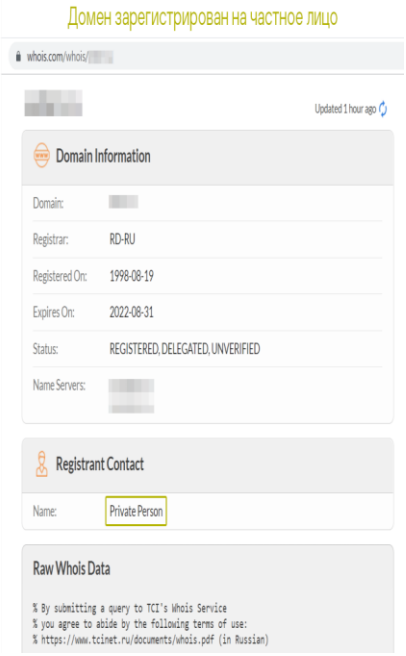


Как проверить SSL-сертификат сайта. «Замок» – это знак того, что данные на этот сайт (и с него) будут передаваться безопасно, в зашифрованном виде, и что независимая организация заверила это сертификатом. Его мы как раз и смотрели. Получить такой сертификат в принципе несложно, но, не на имя чужой компании. Поэтому если в сертификате указано название организации, то ему обычно можно верить (следует убедиться, что оно правильное).

А если замка нет! Значит, данные не защищены, и их могут перехватить не только владельцы сайта, но и посторонние пользователи, так что вводить конфиденциальную информацию на таком сайте точно не стоит.

4. Проверьте, кем и когда зарегистрирован сайт. Получить дополнительную информацию о сайте можно с помощью специального сервиса «whois». Он предоставляет данные обо всех существующих IP-адресах и доменных именах. Введите адрес интересующей вас страницы в соответствующее поле и проверьте, когда и на кого был зарегистрирован домен.





Разница между корпоративным и частным доменами в данных whoi, дату регистрации домена можно найти в строке Registered On. Если сайт выдает себя за официальный ресурс известной компании с многолетней историей, а по данным сервиса домену всего пара месяцев, то очень вероятно, что вы на странице мошенников.

Также полезно посмотреть, на кого зарегистрирован домен. Контактную информацию владельца можно найти в

разделе Registrant Contact. Для сайтов серьезных компаний там будет как минимум указано название организации, а часто еще и ее адрес, телефон и другие данные.

Если же сайт делает вид, что он принадлежит крупной компании, но в поле, в котором указано, на кого зарегистрирован домен, вы видите только надпись Private Person (частное лицо), то ресурсу доверять не стоит. Нужно уточнить: в самом факте регистрации домена частным лицом нет ничего страшного, но это крайне подозрительно в том случае, когда сайт утверждает, что принадлежит огромной корпорации.

5. Ознакомьтесь с содержимым сайта. Изучите сайт поподробнее: если он состоит из одной или двух страниц, очень вероятно, что вы столкнулись с мошенниками. Именно такие сайты, не требующие значительных вложений, злоумышленники использовали, чтобы продавать несуществующие билеты в театр, заставить жертву оплатить поход в частный кинозал или поучаствовать в лотерее якобы от Гослото. На официальных вебресурсах компаний всегда есть несколько разделов с полезной информацией – новости, подробная информация об организации и ее услугах и так далее.

6. Изучите юридические данные компании. Чтобы внушить доверие жертвам, мошенники могут указать на своем сайте в разделе «Контакты» или «О компании» какие-нибудь юридические данные, например, ИНН – обычно чужой или вымышленный.

Проверьте указанный ИНН на сайте официальной налоговой службы – так можно узнать, кому компания принадлежит и чем занимается. Если вы видите, что деятельность компании не совпадает с тем, что заявлено на сайте – велика вероятность, что сайт «не самых честных правил». Раздел с информацией о компании на мошенническом сайте. Даже адрес – без номера дома. Также можно проверить в базах или просто в поиске разные другие данные – номера лицензий, адреса, телефоны и так далее. Если результат такой проверки

выглядит подозрительно, с сайтом лучше не иметь дела.

7. Добавляйте важные сайты в закладки. Все сайты, которые вы часто посещаете, добавьте в панель закладок и открывайте только оттуда – так вы исключите риск случайно зайти на мошеннический ресурс. Прежде всего это касается тех сайтов, на которых вы вводите личные данные, будь то соц-сети, онлайн-банки, крипто-биржи или почтовые клиенты. Добавить ресурс в закладки можно, нажав на «звездочку» в правой части адресной строки.

8. Проявляйте особенную осторожность при платежах и переводах. Конечно, необязательно так тщательно изучать сайт, на который вы зашли, чтобы почитать статьи или посмотреть видеоролики. Однако те, где вы планируете вводить платежные данные, нужно проверять каждый раз. Не выглядит ли странным адрес сайта? Нет ли на странице орфографических ошибок или странных элементов дизайна? Есть ли у страницы SSL-сертификат? Вводите данные своей карты только в том случае, если все в порядке.

9. Положитесь на профессионалов. Даже самые внимательные пользователи порой совершают ошибки. Но есть и хорошая новость: проверку сайтов можно автоматизировать. Для этого используйте надежное решение с защитой от спама, фишинга и онлайн-мошенничества - оно вовремя предупредит об опасности и заблокирует угрозу.

3.2. Особенности раскрытия фактов мошенничества совершаемых в сети Интернет

При совершении интернет-мошенничеств, зачастую применяются средства, позволяющие скрыть реальную личность правонарушителя (VPN/VPS-сервисы для анонимизации интернет-трафика, виртуальные номера мобильных телефонов и адреса электронной почты, анонимные электронные и крипто-валютные кошельки). Персональные данные

пользователя (ФИО) заменяется на никнейм (цифровой псевдоним), количество которых у злоумышленников может достигать нескольких десятков, дата рождения указывается вымышленная. Локация (место нахождения компьютера или иного технического устройства, при помощи которого совершается интернет-мошенничество) также маскируются, в том числе посредством подложных IP- адресов.

Указанные обстоятельства существенно осложняют раскрытие таких преступлений.

Раскрытие интернет-мошенничеств, как правило, осуществляется после регистрации сведений в ЕРДР процессуальным путем (в рамках досудебного расследования) посредством производства негласных следственных действий (далее – НСД).

Порядок проведения НСД регламентирован главой 30 Уголовно-процессуального кодекса Республики Казахстан.

При раскрытии и расследовании интернет-мошенничеств, в основном, осуществляются следующие НСД (ст. 231 УПК):

1) негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации;

2) негласные контроль, перехват и снятие информации, передающейся по сетям электрической (телекоммуникационной) связи;

3) негласное получение информации о соединениях между абонентами и (или) абонентскими устройствами.

В соответствии со статьей 232 УПК, перечисленные НСД производятся по поручению органа досудебного расследования уполномоченным (оперативным) подразделением правоохранительного органа (ОВД) с использованием форм и методов оперативно-розыскной деятельности.

Лицо, вынесшее поручение, несет ответственность за его законность и обоснованность в соответствии с законом

Республики Казахстан.

Порядок получения и исполнения поручения по НСД, а также порядок представления результатов НСД, их исследование и оценка закреплены в нормах Правил проведения негласных следственных действий *(утверждены совместным приказом Министра внутренних дел Республики Казахстан от 12 декабря 2014 года №892, Министра финансов Республики Казахстан от 12 декабря 2014 года №565, Председателя Агентства Республики Казахстан по делам государственной службы и противодействию коррупции от 12 декабря 2014 года №62, Начальника Службы государственной охраны Республики Казахстан от 15 декабря 2014 года №146 и Председателя Комитета национальной безопасности Республики Казахстан от 18 декабря 2014 года №416 Министра внутренних дел РК от 12 декабря 2014 года №892)»*.

3.3. Особенности расследования фактов мошенничества совершаемых в сети Интернет

Процесс расследования уголовных дел в отношении интернет-мошенничеств направлен на выявление и закрепление криминалистический значимой информации, подлежащей трансформации в качестве доказательств по делу. Элементы, формирующие следственную ситуацию, тесно взаимосвязаны. Каждый из них частично содержит информацию о другом, что и позволяет выдвигать обоснованные версии и проводить целенаправленное расследование.

Между тем для разработки криминалистической методики расследования мошенничеств, совершенных в сфере информационных технологий, как и других преступлений, существенное значение имеет установление типичных следственных ситуаций, выявление факторов, наиболее полно отражающих сущность данного преступления.

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

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

Одним из необходимых условий для начала досудебного производства является наличие законного повода, представляющего собой установленный законом источник информации о готовящемся, совершаемом или совершенном правонарушении, на основе которого следователь *(дознаватель)* принимает решение о наличии или отсутствии признаков соответствующего правонарушения, подлежащего обязательной регистрации в Едином реестре досудебных расследований *(далее – ЕРДР).*

Часть 1 ст. 180 УПК РК предусматривает следующие поводы к началу досудебного расследования:

1) заявление физического лица, либо сообщение должностного лица государственного органа или лица, выполняющего управленческие функции в организации, об уголовном правонарушении либо безвестном исчезновении лица;

2) явка с повинной;

3) сообщения в средствах массовой информации;

4) рапорт должностного лица органа уголовного преследования о подготавливаемом, совершаемом уголовном правонарушении [41].

Порядок приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также порядок ведения Единого реестра досудебных расследований определяются

Приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014г. №89, утвердившим «Правила приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» [42].

Законодатель предусматривает два вида поводов к началу досудебного расследования:

– формальный *(первичный)*, предусмотренный ч. 1 ст. 179 УПК РК, влекущий необходимость проверочных *(в том числе и неотложных следственных)* действий и фиксацию в книге учета информации *(далее – КУИ)* до регистрации в ЕРДР с возможностью отказа от досудебного расследования;

– процессуальный *(законный)*, предусмотренный ч. 1 ст. 180 УПК РК, обязательный для регистрации в ЕРДР с последующим принятием к производству и досудебным расследование [43, с. 200-202].

Типичные поводы по рассматриваемой категории уголовных дел относятся ко второй группе, ограничиваясь заявлениями граждан либо рапортом должностного лица. Практика показывает, что довольно часто в качестве повода выступают заявления физических лиц, активно пользующихся услугами интернет-магазинов, безналичными расчетами посредством банковских платѐжных систем, в то время как явка с повинной или сообщения в СМИ для интернет-мошенничества – крайне редкие явления.

Уголовно-процессуальный кодекс Республики Казахстан *(ч. 1 ст. 179 УПК РК)* связывает начало досудебного расследования с формальным моментом: достаточно регистрации заявления, сообщения об уголовном правонарушении в ЕРДР либо проведения первого по времени неотложного следственного действия. Тем самым констатируется, что последующее, после регистрации принятия дела к производству, означает положительное разрешение возникшего правового конфликта и не требует принятия отдельного про-

цессуального акта о его начале. Подобная процедура распространяется на случаи, содержащие признаки уголовного правонарушения, за исключением дел частного обвинения, поскольку жалобы по последним подаются непосредственно в суд *(ч. 1 ст. 408 УПК РК).*

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

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

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

3) определение подследственности преступления;

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

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

6) проверка по криминалистическим учетам наличия уголовных дел, расследуемых по аналогичным фактам, в целях выяснения вероятности их соединения в одно производство;

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

После получения и закрепления информации, дающей основание подозревать конкретное лицо в совершении интернет-мошенничества и его допроса в качестве подозревае-

мого, задачи первоначального этапа досудебного расследования считаются выполненными.

С учетом того, что в Республике Казахстан мошеннические действия в сети Интернет чаще всего совершаются на общеизвестных сайтах таких как,

«OLX», «Колеса» и «Крыша KZ», сотрудниками «Центра по подготовке специалистов по противодействию киберпреступности» совместно с представителями ТОО «Колеса» и «Крыша KZ», разработан определенный алгоритм действий для сотрудников правоохранительных органов по получению более объемной и полезной информации от ТОО «Колеса» и «Крыша KZ», в целях повышения эффективности по выявлению, раскрытию и расследованию Интернет-мошенничеств.

При написании монографии были проанализированы и обобщены требования ряда действующих государственных стандартов, область распространения и сфера действия которых установлены для текстовых документов.

Общие требования по организации и порядку оформления запросов, для оказания помощи представителям правоохранительных органов Республики Казахстан при составлении запросов и их оформлении в соответствии с внутренними стандартными процедурами ТОО «Колеса» и «Крыша KZ».

1. Как можно использовать данные, предоставленные ТОО Колеса и что они означают:

1) IP адрес – это уникальный сетевой адрес объекта в Интернете: компьютера, сайта, сервера и так далее. Например, если в ответе на запрос, указан IP адрес, то это значит, что в момент размещения объявления пользователь использовал именно этот IP адрес. На некоторых сайтах, например, «https://2ip.ru/whois/» можно получить информацию о провайдере, который предоставил этот адрес. Используя дату и время подачи объявления – можно направить запрос к провайдеру с требованием предоставить информацию по место-

расположению номера телефона, компьютера или сервера, которые были задействованы при размещении объявления.

2) Дата публикации, переноса в архив, удаления – эти данные помогут составить запрос к провайдеру. А также могут быть использованы для подтверждения того, когда именно объявление было размещено.

3) Электронная почта – поможет найти информацию у почтовых сервисов, какие данные были использованы при регистрации той или иной электронной почты. Также, часть пользователей использует личные данные (такие, как имя, фамилия, дата рождения, номера телефонов) при составлении электронных адресов.

4) Номер телефона – это номер, который был указан пользователем с помощью подтверждения номера по смс сообщению. Пользователь запрашивал код на этот номер и в форме авторизации на одной из наших площадок, указал 4-значный код, чем подтвердил владение этим номером. В рамках пункта 24 проекта «Правил регистрации абонентских устройств», абонентские устройства сотовой связи, обслуживающийся в сети оператора сотовой связи до 1 января 2019 года, регистрируются им автоматически в локальной системе и передаются в базу данных идентификационных кодов. Если абонент самостоятельно не прошел процедуру регистрации своего абонентского устройства до 1 января 2019 года, то в таком случае устройство зарегистрировано автоматически на тот ИИН, на который зарегистрирован абонентский номер, находящийся в устройстве

5) Имя в комментариях – информация, которую пользователи заполняется автоматически, также пользователи могут заполнить ее по желанию, и она не всегда соответствует действительности.

6) Другие объявления в личном кабинете пользователя – в других объявлениях пользователя могут быть ис-

пользованы дополнительные номера телефонов, по которым также можно предоставить информацию или запросить информацию у операторов сотовой связи, о владельце данного номера телефона.

7) Фотографии, которые были загружены в объявления – на фотографиях, загруженных пользователем, иногда можно различить ГРНЗ авто (на Колесах и Маркете), фасад здания или помещения, который продают или сдают в аренду (на Крыше и Маркете).

8) Способ оплаты или способы пополнения личного кабинета – если пользователь пополнял личный счет кабинета с карты, в таком случае может быть предоставлен номер карты (первые 6 и последние 4 цифры), наименование банка, время пополнения или оплаты услуг.

1.1 Направление запросов правоохранительными органами для получения содействия в рамках следственных мероприятий

Для получения полноценного ответа на запрос, рекомендуется при составлении обратить внимание по каким параметрам мы можем вести поиск.

Ниже параметры, указав которые мы можем найти объявление или пользователя.

1.2 По каким параметрам может быть произведен поиск и предоставление информации Kolesa Group (kolesa.kz, krisha.kz, market.kz)

– ID (номер) объявления;

– Ссылка на объявление;

– Номер телефона, указанный в объявлении или при регистрации;

– Электронная почта;

– ID (номер) личного кабинета;

– Скриншот с объявлением (на скриншоте должна быть отображена информация по объявлению, указанная выше);

– данные из объявления: рубрика, марка, модель, год

выпуска авто на Kolesa.kz;

– данные из объявления: количество комнат, город, район/микрорайон, цена, дополнительные параметры в обязательных для заполнения полях на krisha.kz;

– текст объявления (чем оригинальнее был текст в объявлении, тем больше шансов, найти, то, что нужно)

1.3 По каким параметрам НЕ может быть произведен поиск информации

1. **Фамилия и имя** – при регистрации на сайте такая информация не требуется, а поле – имя в комментариях‖ заполняется самостоятельно пользователем и не всегда соответствует действительности.
2. **ИИН** – при регистрации на сайте такая информация не требуется,
3. **Информация, которая находится в архиве –** информация в архиве хранится в течение 2 лет с момента ухода объявления в архив.
4. **Название компании** – при регистрации на сайте такая информация не требуется.
5. **ГРНЗ** – фотографии могут быть не загружены в объявление, это не обязательно требование. Номера могут быть закрашены пользователем в любой программе. Поля для заполнения ГРНЗ нет. Информация с фотографией не считывается системой, по ней нельзя найти информацию.
6. **Vin код** – поле необязательно для заполнения. Указывают по желанию пользователя и не всегда информация может соответствовать действительности.
7. **Фотографии, картинки** – поиска по картинке нет в системе.
8. **Номер дома, номер квартиры** – необязательно поле для заполнения, для указания номера квартиры нет отдельного поля. Эту информацию автор объявления может указать по желанию самостоятельно, но информация может не соответство-

вать действительности.

1.4 Информация, которая может быть предоставлена

1. Номер телефона в объявлениях или личном кабинете.
2. Электронная почта, указанная при подаче объявления.
3. Объявления, которые были размещены за последние 2 года (live, archive, delete).
4. IP адрес, зафиксированный в момент размещения объявления, просмотра объявления или переписки в личных сообщениях.
5. Дата регистрации /первой авторизации на kolesa.kz, krisha.kz, market.kz.
6. Дата размещения объявления (в хранилищах live, archive, delete).
7. Средняя цена за квартиру, в таких разделах: продажа квартир, домов и аренда квартир, домов, для сравнения используются такие параметры, как год постройки дома, комнатность, район расположения и тип строения.
8. Средняя цена по авто, учитывая марку, модель и год выпуска (данные за каждый месяц).
9. Рубрика, раздел, цена, обязательные заполненные поля в объявлении.
10. Фотографии, если были загружены в объявление по запросу.
11. История операций (выписка по счету) в личном кабинете по запросу.
12. Способ оплаты или пополнения в личном кабинете, квитанции об оплате со счета личного кабинета (если были) по запросу.
13. Имя в комментариях (заполняется пользователем самостоятельно и не всегда достоверно).
14. Дата удаления объявления (в хранилищах live, archive,delete) kolesa.kz, krisha.kz, market.kz

15. Жалобы на объявления по номеру телефона, электронной почте, если были зафиксированы в базе kolesa.kz, krisha.kz, market.kz.

16. Звонки по номеру телефона в службу заботы о пользователях по номерам: +7 (777) 552-13-39, +7 (727) 331-11-86 и +7 (775) 031-11-86 (в формате mp3) kolesa.kz, krisha.kz, market.kz

17. Письменные обращения в службу заботы о пользователях по почте ok@kolesa.kz, (kolesa.kz, krisha.kz, market.kz)

18. Письменные обращения в службу заботы о пользователях по номеру Whatsapp: +7 (777) 552-13-39 (kolesa.kz, krisha.kz, market.kz)

19. ОС устройства, с которого было размещено объявление. для kolesa.kz, krisha.kz, market.kz

20. Дата переноса объявления в архив (в хранилищах live, archive, delete) kolesa.kz, krisha.kz, market.kz

21. Дата изменения в объявлении только для kolesa.kz, krisha.kz, market.kz

1.5 Информация, которая НЕ может быть предоставлена

1. Фамилия, Имя, Отчество.

2. ИИН пользователя.

Вин код авто, если пользователь не указал его в объявлении о продаже авто.

3. Фото с ГРНЗ, если пользователь не загрузил фото в объявление.

4. Объявления, которые ушли в архив или были удалены больше 2 лет.

5. Изменения по цене – какая цена была на момент подачи.

6. Изменения, внесенные в объявление – какие имен-

но изменения были

7. Внесены пользователем в ранние версии объявления.

8. Количество просмотров в архивных/удаленных объявлениях.

9. Данные по пользователям, которые просматривали объявления.

10. Удаленные из объявления фотографии – мы не храним такую информацию.

1.6 Информация по срокам обработки запросов отправке и получению

ТОО «Колѐса» обязаны отвечать на все запросы, оформленные в соответствии с требованиями действующего законодательства РК в течение 15 (пятнадцати) календарных дней, за исключением случаев, когда в запросе указан иной срок. При этом стороны могут отдельно согласовать сроки предоставления информации.

Запрос может быть представлен как в бумажном варианте, так и в электронном (скан версия) формате.

Запрос по электронной почте может быть оформлен как с официальной почты ведомства, так и с личной почты лица, зарегистрированного в ЕРДР.

Запрос должен быть оформлен на официальном бланке ведомства, содержать контакты ведомства исполнителя запроса, содержать собственноручную подпись уполномоченного лица, и должен быть заверен печатью.

Ответ на запрос может быть предоставлен на электронную почту, указанную в запросе, а также может быть выдан с нарочным по необходимости в бумажном виде с печатью и подписью.

3.4. Обстоятельства, подлежащие доказыванию на первоначальном этапе расследования

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Мошенничество, совершаемое путем обмана или злоупотребления доверием пользователя информационной системы – это те же действия, но совершенные с помощью Интернета.

Данный вид мошенничества является относительно новым, и в то же время, распространенным и опасным видом преступления. Это связано, в первую очередь, с возможностью глобального *(т.е. выходящего за границы отдельно взятого государства)* использования компьютерных технологий, позволяющих скрыть действительный источник распространяемой информации и лица, получающего денежные средства потерпевших *(например, путем использования интернет-кошелька).*

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

– место, время, условия, способ совершения мошенничества;

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

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

– характер и размер причиненного ущерба;

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

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

– данные о мошеннической преступной группе и иных лицах, участвовавших в ее действиях *(состав, численность,*

техническая оснащенность, техническая специализация);

– данные о личности потерпевшего, обстоятельства контакта с мошенником [41].

Названные обстоятельства принято называть главным фактом, поскольку от доказанности или недоказанности этих обстоятельств напрямую зависит решение вопроса об уголовной ответственности – главного вопроса уголовного дела [44, с. 136].

В первую очередь, следует установить, какое событие произошло. Видов и схем мошенничества в сети Интернет разнообразное количество [45, с. 15-19].

Основные признаки мошенничества в Интернете – навязчивая реклама, обещающая огромный доход без вложения знаний и большого труда; требование ввода ваших персональных данных на сомнительных ресурсах; требование отправки SMS *(которые в действительности являются платными)*, например, за скачивание необходимой литературы; заманчивые предложения, приходящие через почту от незнакомых людей *(письма счастья* и т.д.

Легкий заработок в Интернете. Сайты с бесплатной музыкой, финансовые пирамиды, онлайн-казино, сайты знакомств, техника в полцены – почти всегда это мошенничество. Предложения под прикрытием официальных компаний или организаций с переводом денег на счета физических лиц.

Наиболее известными способами совершения данного вида преступления являются фишинг, киберсквоттинг, тайпсквоттинг, мошенничество с помощью платежных систем *(программного обеспечения)*, иные способы интернет-мошенничества. Способов совершения интернет-мошенничеств большое количество. Это связано в первую очередь, с существенным расширением спектра услуг, предоставляемых в сфере информационных технологий.

С помощью этих сведений можно выяснить, не совершены ли другие мошенничества, аналогичным способом и

кто их мог совершить. Кроме того, установление способа интернет-мошенничества позволяет выдвинуть версии о лицах его совершивших, определить возможные места нахождения следов преступления.

Предметом мошенничества в сети Интернет являются не наличные денежные средства, а виртуальные, то есть данные банковских карт, счетов, переводы денежных средств с помощью платежных систем. При получении денежных средств, ввиду отсутствия контакта между злоумышленником и жертвой, установить преступника в таком случае маловероятно.

Под обманом понимается как сознательное искажение истины *(активный обман)*, так и умолчание об истине *(пассивный обман).* В обоих случаях обманутая жертва сама передает свое имущество мошеннику.

Характеризуя личность потерпевших, нужно иметь в виду, что нередко сами жертвы, движимые корыстными побуждениями и стремлениями обойти существующий порядок, действуют нечестным путем, в результате чего становятся жертвами мошенников. С другой стороны, жертвами мошенников оказываются люди простодушные, излишне доверчивые или неискушенные, которые поддались эмоциям и потеряли бдительность.

Данные о преступнике, по данной категории дел на первоначальном этапе получить очень сложно. Как правило, узнать мошенников можно по манере общения и интересу к личным данным, данным платежных карт. Все зависит от способа мошенничества.

Мошенники – своего рода «элита» преступного мира, «талантливые артисты», находчивые и изворотливые, проворные в действиях, нешаблонно мыслящие. Они, так называемые «белые воротнички», образованы, не злоупотребляют спиртным и наркотиками, отличаются психологической устойчивостью, оптимизмом, конформизмом, самоконтро-

лем, добротой и отзывчивостью.

Как правило, *выделяют две категории злоумышленников:*

– мошенники, не имеющие постоянного места жительства и работы, неоднократно судимые за мошенничество и другие преступления против собственности;

– мошенники-рецидивисты, совершающие в основном мелкие мошенничества, чаще всего их жертвами становятся частные лица.

В части 2 ст.113 УПК РК говорится о необходимости выявления обстоятельств, способствовавших совершению преступления. Хотя в данной норме говорится об установлении только этой группы обстоятельств, необходимо учесть, что доказыванию подлежат и причины преступления.

В частности, необходимо выяснить причины возникновения у лица антиобщественных взглядов и привычек; причины, вызвавшие формирование умысла на совершение деяния или пренебрежительного отношения к интересам других лиц и общества в целом; обстоятельства, облегчившие реализацию антиобщественных установок лица, сделавшие возможным совершение данного преступления и т.п.

В случае рецидива необходимо установить его причины, а также обстоятельства, способствовавшие совершению лицом нового преступления.

Практический интерес представляет характеристика личности лиц, совершающих преступления в сфере мошенничества, путем обмана или злоупотребления доверием пользователя информационной системы. С помощью «пола, возраста, семейного и социального положения, образования, профессии и других – выясняется преступная активность различных слоев населения, прослеживаются возрастные и половые особенности лиц, совершивших преступления и т.д.» [46, с. 108].

Типовые особенности личности интернет-мошенника по исследуемой категории дел позволяют правоохранитель-

ным органам в процессе проведения расследования определить круг подозреваемых в совершении преступления, разработать потенциальные модели их поведения, предугадать дальнейшие действия и сформировать алгоритм действий следствия в процессе раскрытия преступления и сбора доказательств для их предъявления в суде.

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

Необходимо отметить, что интернет-мошенники, в большем количестве случаев не имеют постоянного места работы, порядка 83,4% преступников не имели постоянный источник дохода, что объясняет причину большой доли корыстных посягательств среди общего количества преступлений, совершаемых в сети Интернет. Большинство интернет-мошенников имеет определенный набор специальных знаний *(принципы работы информационно- телекоммуникационных сетей, их уязвимость)* и пользуются этим, используют вредоносные программы и вирусы. В Интернете есть много возможностей заработка, в том числе и с помощью применения таких знаний. Предложения могут носить как легальный *(создание интернет-сайтов, настройка почтовых серверов и т.д.)*, так и нелегальный характер *(например, написание вредоносных программ под конкретные задачи).* Выяснение способа заработка преступника, позволяет получить также информацию о лицах, с которыми он взаимодействовал, т.е. установить всех членов преступной группы.

Личность интернет-мошенника отличается следующими особыми характеристиками:

– четко и профессионально формулирует задачу, однако отличается хаотическим бытовым поведением;

– имеет весьма развитое формально-логическое мышление, однако именно оно нередко подводит его в реальной жизни;

– старается говорить четко, точно и однозначно, регулярно переспрашивает, используя уточняющие вопросы;

– говорит преимущественно на компьютерном жаргоне, который малопонятен непрофессионалам.

Мошенничеством в глобальной сети Интернет занимается широкий круг лиц, среди которых встречаются специалисты высокой квалификации и дилетанты. Преступники отличаются разным уровнем образования и социальным статусом.

Они делятся на две категории:

1) лица, находящиеся с потерпевшим в деловых или трудовых отношениях;

2) лица, не имеющие связей с потерпевшим.

Первую группу представляют сотрудники, которые злоупотребляют своим служебным положением: операторы, программисты, инженеры, технический персонал, клерки, работники, обеспечивающие безопасность, сотрудники контролирующих структур, лица, решающие организационные вопросы. Преступные действия могут осуществлять и бывшие сотрудники организаций, применяющие имеющуюся у них информацию в целях совершения мошеннических операций с физическими и юридическими лицами, пользующимися интернет-услугами.

Вторую группу составляют лица, обладающие большими познаниями в сфере современных компьютерных технологий и руководствующиеся в основном корыстными мотивами. Сюда же можно отнести и профессиональных специалистов, которые воспринимают меры безопасности, установленные на компьютере, в качестве вызова уровню своего профессионализма. Нередко они приобщаются к мошенниче-

ской деятельности, осознанно совмещая интеллектуальные и материальные стимулы своих преступных действий.

Мошенничество в сети Интернет нередко совершают и сотрудники организаций, занимающие руководящие посты, поскольку преимущественно они являются высококвалифицированными специалистами, имеют достаточный уровень компьютерной подготовки и профессиональных знаний, навыков и умений, а также по роду своей деятельности получают доступ к большому объему информации и могут давать указания своим подчиненным, однако не несут прямую ответственность за функционирование самой компьютерной системы.

По данным в интернете, стало известно, что интерпол – разработал собственную классификацию интернет-мошенников. Данная классификация достаточно официальна и поможет при определении причастности лица к совершению уголовного правонарушения при расследовании интернет-мошенничеств [47].

Интернет-мошенники могут быть разделены на несколько видов:

– «любопытные» – это люди, которые не имеют злого умысла и совершают свои деяния из-за любопытства и неграмотности;

– «профессионалы» – те, кто совершает противоправные действия, руководствуясь злым умыслом;

– «фобы» – люди с нарушениями психики, страдающие неврастенией или теми или иными формами зависимости;

– «хулиганы» – те, кто действует, основываясь на хулиганских побуждениях;

– «воры» – это люди, которые взламывают компьютерные системы, движимые желанием на этом заработать;

– «мусорщики» – это мошенники, внимательно изучающие содержимое корзин и прочий интернет-мусор, желая собрать таким способом персональные данные пользователей;

– «учителя» – мошенники, которые «обучают» других, менее квалифицированных коллег работать в сети, объясняют им, к чему может привести нарушение регламента работы;

– «подглядывающие» – злоумышленники, несанкционированно проникающие на различные сайты, используя информацию, предоставленную им зарегистрированными пользователями;

– «инсайдеры» – люди, получающие инсайдерскую информацию и передающие ее кому-либо «на сторону» (обычно руководствуются корыстными целями);

– «аукционщики» – мошенники, организующие «липовые» распродажи и аукционы, приманивая пользователей привлекательными ценами или интересными лотами, которых на самом деле не существует;

– «нигерийцы» – злоумышленники, которые незаконно присваивают себе чужое по «нигерийскому методу»: берут средства «на хранение» или как «депозит», обещая высокие проценты по нему;

– «вымогатели» – мошенники, распространяющие вредоносные вирусы, способные заблокировать компьютеры пользователей, а затем вымогающие с них деньги на «починку» устройства;

– «домушники» – злоумышленники, которые используют в корыстных целях носители информации;

– «перехватчики» – те, кто перехватывает данные в Интернете и далее используют их в своих корыстных интересах;

– «Санта-Клаусы» – злоумышленники, которые используют для проникновения в систему аккаунты уже зарегистрированных в ней клиентов;

– «демпингующие» – люди, обманывающие пользователей, предлагая им сделки по купле-продаже несуществующих товаров по ценам ниже рыночных;

– «саботажники» – мошенники, которые саботируют

нормальную работу сети, используя для этого организационные или программные методы;

– «оседлавшие троянца» – злоумышленники, сознательно распространяющие вирусы типа «троянского коня» для того, чтобы решать таким образом собственные задачи, например, распространять вирусную рекламу;

– «аналитики» – люди, тщательно изучающие все сообщения системы для получения в дальнейшем доступа к ней на незаконных основаниях;

– «отпетые фрилансеры» – злоумышленники, которые наживаются на людях, работающих по фрилансу. Они не оплачивают заказы, выполненные доверчивыми копирайтерами, или предлагают выгодную надомную работу, для устройства на которую нужно внести депозит.

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

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

Ситуации, свидетельствующие о причастности лица к совершенному преступлению, означают появление оснований подозрения, что должно исключить для заподозренного лица статус свидетеля *(за исключением свидетеля, имеющего право на защиту)* и повлечь приобретение им процессуального положения подозреваемого с соответствующими правами и

обязанностями.

О том, что лицо совершает мошенничество, могут свидетельствовать следующие ситуации, рекламируемые на сайтах Интернета:

– предоставление кредита организацией, не имеющей лицензии, или отсутствие в договоре пункта о гарантиях возврата денег;

– необоснованно высокий процент вознаграждения;

– условия, предусматривающие телефонный звонок или СМС сообщение для получения кодового слова (пароля);

– выплата небольшой суммы якобы для конвертации валют;

– необходимость найти гаранта или поручителя либо нового участника финансовой операции;

– реклама товара, реализацией которого занимается не фирма-изготовитель, а интернет-магазин;

– перевод денег на киви-кошелек;

– просьба выручить из конфликтной ситуации путем предоставления финансовых средств, например, после непродолжительного интернет знакомства и т.д.

3.5. Типичные следственные ситуации и особенности производства отдельных следственных действий

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

Типичные следственные ситуации играют важную роль в формировании методик расследования, позволяют разрабатывать направления по их разрешению, тем самым деятельность следователя становится целенаправленной. Ти-

пичные следственные ситуации формируются при изучении материалов следственной практики. Практика расследования интернет-мошенничеств позволяет разделить следственные ситуации в зависимости от содержания исходной информации [48, с. 271-274].

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

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

– способы совершения и сокрытия преступления;

– свидетели;

– материально фиксированные следы преступления;

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

– местонахождение похищенного имущества, денежных средств.

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

– способы совершения и сокрытия преступления;

– свидетели;

– материально фиксированные следы преступления;

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

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

– способы совершения и сокрытия преступления;

– свидетели;

– материально фиксированные следы преступления;

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

иных операций;

– местонахождение похищенного имущества, денежных средств или их части [49, с. 36-47].

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

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

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

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

4) допрос подозреваемых;

5) проверка подозреваемых по базам криминалистических учетов;

6) выемка:

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

– документов, отражающих работу субъекта с компьютерной информацией;

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

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

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

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

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

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

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

Примерами таких ситуаций могут быть следующие:

1) выявленный факт совершения интернет-мошенничества когда:

– отсутствует информация о личности правонарушителя;

– не установлены свидетели;

– отсутствует информация о способе совершения преступления;

– не обнаружены материально фиксированные следы;

– не установлено местонахождение похищенного имущества.

2) выявленный факт совершения интернет-мошенничества когда:

– имеются данные о способе совершения преступления;

– установлены свидетели;

– отсутствуют сведения о личности преступника;

– отсутствуют материально фиксированные следы совершения преступления

Изучение уголовных дел данной категории показало,

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

Для второй группы следственных ситуаций обычно планируют и осуществляют следующие первоначальные следственные действия, оперативно-розыскные и организационные мероприятия:

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

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

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

4) назначение судебной компьютерно-технической и других экспертиз;

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

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

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

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

9) обыски на рабочих местах и по месту жительства

подозреваемых.

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

Если полученная в ходе расследования информация считается достаточной для вынесения постановления о признании подозреваемым и квалификации его деяний конкретному лицу, то начальный этап расследования признается оконченным, и расследование переходит к последующему этапу – проведение последующих следственных действий и негласных следственных действий *(оперативно-розыскных мероприятий).*

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

3.6. Тактика производства отдельных следственных действий

Производство допроса при расследовании интернет-мошенничества.

Основной целью допроса является получение и процессуальная фиксация в протоколе показаний допрашиваемого лица об обстоятельствах, имеющих значение для правильного разрешения уголовного дела. Учитывать, что на всех допрашиваемых лиц распространяется положение ст. 27 Конституции РК:

– никто не обязан давать показания против самого себя, супруга *(супруги)* и близких родственников, круг которых определяется законом.

При производстве допроса строго руководствоваться требованиями главы 26 УПК РК, устанавливающей порядок

и правила производства допроса.

Основанием для допроса является наличие данных *(информации полученной в результате других следственных действий, либо по объективным выводам (логическим умозаключениям) следователя),* что лицо обладает сведениями, которые могут иметь значение для дела.

Планировать и производить допрос рекомендуется с учетом следующих стадий:

– подготовительная;

– предварительная;

– стадия свободного рассказа,

– вопросно-ответная стадия;

– заключительная стадия.

Подготовительная стадия допроса включает в себя:

– определение круга обстоятельств, требующих установления *(предмета допроса)*;

– определение круга лиц, подлежащих допросу;

– определение времени и способа вызова лиц на допрос;

– тщательное изучение и анализ обстоятельств дела *(рекомендуется составить перечень наиболее важных установленных обстоятельств дела и обстоятельств, которые необходимо выяснить, а также выписать фамилии, адреса, систематизировать вещественные доказательства, которые будут предъявлены допрашиваемому, освежить в памяти планы и схемы места происшествия и т.д.)*;

– изучение личности лица, которое предполагается допросить *(с целью выявления его физических, психических, интеллектуальных особенностей и эффективного планирования допроса)*;

– составление плана допроса *(для грамотного построения тактики допроса с целью получения правдивых показаний)*;

– планирование допроса основывается на известных

обстоятельствах дела и особенностях личности допрашиваемого;

– выбор технических средств звукозаписи и видеозаписи *(использование данных средств рекомендуется использовать во всех случаях производства допроса).*

Предварительная стадия заключается в заполнении анкетной части протокола допроса.

Следователю *(дознавателю)* необходимо:

– представиться *(назвать свою фамилию, имя и отчество, должностное положение).*

– удостоверить личность допрашиваемого *(ознакомиться с документом, удостоверяющим его личность)*;

– разъяснить, по какому поводу и в качестве кого вызван допрашиваемый, а также порядок проведения следственного действия и его права *(ст.ст. 64, 65, 71, 78, 79 УПК РК)*;

– объяснить порядок составления и подписания протокола, возможность внесения правок, дополнений и замечаний *(ч. 6 ст. 212 УПК)*;

– уведомить допрашиваемого о применении технических средств, а также участии иных лиц *(им также разъясняются порядок и их права)*.

После завершения допроса по анкетной части протокола допрашиваемому предлагается в форме свободного рассказа сообщить о происшедшем.

Основная (рабочая) стадия допроса состоит из двух этапов: Этап свободного рассказа.

В стадии свободного рассказа применяются такие приемы, как формирование мыслительной задачи допрашиваемого *(помощь в формулировании мысли)*, напоминание, сопоставление и др.

Допрос начинается с рассказа допрашиваемого. Подозреваемому и обвиняемому предлагается рассказать все из-

вестное об обстоятельствах, вызвавших подозрение или составляющих содержание обвинения.

Перебивать и вмешиваться в рассказ допрашиваемого следует только в следующих случаях:

– при отклонении от темы;

– при попытке повторного разъяснения уже высказанных показаний *(многократное разъяснение одних и тех же обстоятельств)*;

– детального разъяснения несущественных обстоятельств дела.

При выявлении следователем ложности показаний на стадии свободного рассказа, перебивать допрашиваемого и указывать ему на этот факт не рекомендуется. Такие ложные показания целесообразно зафиксировать (для возможности задать изобличающие лож вопросы в последующем); факт выявленной и процессуально закрепленной лжи со стороны допрашиваемого указывают на его попытки ввести следствие в заблуждение и воспрепятствовать установлению истины по делу.

Вести протокол на стадии свободного рассказа не следует, так как это будет отвлекать следователя и допрашиваемого. Следователь *(дознаватель)* может делать важные заметки по ходу рассказа допрашиваемого, записывать необходимые вопросы для того, чтобы задать их по окончании рассказа и т.д.

Выслушав показания в форме свободного рассказа, следователь приступает к очередной стадии допроса – вопросно-ответной.

Вопросно-ответный этап.

Рекомендации к постановке следователем вопросов допрашиваемому:

– вопрос должен быть конкретным, касающимся какого-либо одного обстоятельства, лаконичным и не допускающим двусмысленного толкования;

– необходимо избегать вопросов, на которые возможны предположительные ответы;

– формулировка вопроса должна полностью исключить возможность извлечения из его содержания информации, необходимой для ответа;

– следует заранее подумать, в какой последовательности будут выясняться вопросы *(как правило, один вопрос должен вытекать из другого и иметь ясную логическую структуру)*;

– вопрос задается в прямой форме;

– вопросы должны формулироваться с учетом умственного и культурного развития, допрашиваемого [50, с. 63-74].

Заключительная стадия.

В стадии фиксации показаний следователь задает допрашиваемому уточняющие и контрольные вопросы, предлагает уточнить показания, подлежащие занесению в протокол, предоставляет возможность допрашиваемому записать свои показания и т.д.

Эффективным средством получения правдивых показаний является предъявление допрашиваемому доказательств. Время, последовательность использования при допросе доказательственной информации рекомендуется планировать с учетом ее содержания и степени возможного психологического воздействия. К распространенным формам оперирования такой информацией относятся: оглашение показаний; предъявление вещественных доказательств, ознакомление с документами; предъявление заключений экспертов и другое.

Допрашиваемое лицо должно быть ознакомлено с протоколом допроса путем личного прочтения либо оглашения его следователем. Протокол, дополнения и уточнения к нему подписываются всеми участниками допроса.

Законом предусмотрена возможность применения для фиксации хода и результатов допроса технических средств,

таких, как фото и киносъемка, аудио и видеозапись.

Аудио- и видеозапись являются эффективными тактическими средствами *(против изменения показаний допрашиваемым, а также при подозрении в фальсификации протокола следователем).*

По окончании допроса с применением технических средств аудио и видеозапись полностью воспроизводятся допрашиваемому, который своим заявлением удостоверяет ее правильность.

Допрос потерпевшего

Допрос потерпевшего является основным источником получения информации при раскрытии преступления. Тактическая грамотность при его проведении позволяет выдвинуть версии о произошедшем преступлении.

При допросе потерпевшего необходимо, прежде всего, получить информацию о личности мошенника, для чего устанавливают следующие обстоятельства:

– знаком ли потерпевший с мошенником, как состоялась знакомство, кто при это присутствовал;

– как представился мошенник, показывал ли он какие-либо документы;

– в чем выразился ущерб потерпевшему.

Вопросы, направленные на установление конкретного способа совершения интернет-мошенничества и сокрытия следов преступления:

–кому принадлежала инициатива знакомства;

–что происходило после очередной пересылки и особенно, после последней *(переставал работать сайт мошенника и т.п.)*;

–после знакомства с интернет-мошенником, отмечал ли потерпевший случаи заражения своего компьютера вредоносными программами? Если такие случаи были, то сохранилась ли об этом информация на компьютере жертвы;

–проводил ли потерпевший чистку компьютера от не-

нужной информации;

–не посылал ли потерпевший интернет-мошеннику дополнительную информацию о себе *(например, фотографии, какую-либо финансовую информацию и т.д.)*;

–есть ли у потерпевшего знакомые, которые контактировали с преступником;

Вопросы, направленные на установление ущерба:

–когда, каким способом и в каком количестве потерпевший передавал денежные средства мошеннику;

–есть ли свидетели, которые могут подтвердить факт отправки денежных средств интернет-мошеннику;

–сохранились ли документы, подтверждающие перевод денег.

Вопросы, направленные на получение информации о личности подозреваемого, а также о возможных соучастниках:

–имела ли место переписка с мошенником и какими способами она велась;

–что потерпевший знает о преступнике;

–сколько раз потерпевший контактировал с интернет-мошенником;

–зафиксирована ли информация о мошеннике в каких-либо носителях информации, принадлежащих потерпевшему *(например, присланные мошенником фотографии, сохранѐнные в одной из папок на компьютере потерпевшего)*;

–какую информацию о себе предоставлял мошенник;

–сообщал ли интернет-мошенник о местах *(в т.ч. интернет-сайтах и форумах)*, в которых он бывал;

–есть ли у потерпевшего и мошенника общие знакомые, общее учебное заведение, общее прошлое и т.д.;

–проверяла ли жертва информацию, сообщенную мошенником;

–почему потерпевший поверил мошеннику и передал ему денежные средства;

–случались ли персональные встречи с интернет-

мошенником, в том числе посредством видео-чатов? Если общение происходило при помощи видео-чата, то остались ли какие-либо свидетельства этого *(скриншоты (снимки экрана), аудио- и видеозаписи общения)*;

–интересовался ли мошенник во время переписки наличием у потерпевшего специальных познаний в какой-либо области, особенно, в области компьютерных технологий.

Допрос свидетеля

Допрос свидетеля осуществляется с соблюдением правил ст. ст. 208-215 УПК РК. Предметом свидетельских показаний могут быть любые фактические обстоятельства, относящиеся к данному делу, в т.ч. обстоятельства, характеризующие личность подозреваемого и взаимоотношения свидетеля с ним. Свидетель дает показания об обстоятельствах как воспринятых им непосредственно, так и воспринятых им со слов другого лица.

Особенностью допроса свидетеля по делам о мошеннических действиях во многом обуславливается его отношением к потерпевшему, подозреваемому, степенью заинтересованности в исходе дела, что должно найти существенное отражение при выборе тактических приемов допроса. По указанным категориям свидетелей можно классифицировать на следующие группы:

– родственники и знакомые потерпевшего;

– родственники, знакомые, друзья лица, совершившего мошеннические действия;

– свидетелей совершенных мошеннических действий, которых также в свою очередь можно разделить на:

а) непосредственно наблюдавших процесс совершения мошеннических действий;

б) знающих о событии совершенного мошенничества с чьих-либо слов (потерпевшего, лиц, непосредственно наблюдавших мошеннические действия, либо со слов лица, совершившего мошеннические действия).

Во время допроса свидетелей каждый раз необходимо выяснять:

– интересовался ли кто-нибудь компьютерной информацией, программным обеспечением, компьютерной техникой данного предприятия, организации, учреждения, фирмы или компании;

– появлялись ли в помещении, где находится компьютерная информация, посторонние лица, зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции;

– не было ли сбоев в работе программ, похищений носителей информации и отдельных компьютерных устройств;

– зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации;

– кто из сотрудников работал внеурочно, кто интересовался информацией, не относящейся к их непосредственной деятельности;

– зафиксированы ли в последнее время случаи срабатывания средств защиты компьютерной информации;

– каким образом приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

– каким образом на предприятии, в организации, учреждении или фирме осуществляется работа с информацией, как она поступает, обрабатывается и передается по каналам связи;

– кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ к сети, кто из пользователей имеет право на работу в сети, полномочия этих пользователей по работе с информацией;

– как осуществляется защита компьютерной информации, какие средства и методы защиты применяются и др.

При допросе свидетелей из числа разработчиков системы и, как правило, поставщиков технического и программного обеспечения следует выяснить, каким образом были преодолены средства защиты, узнать идентификационный номер законного пользователя, код, пароль для доступа к ней, получить сведения о других средствах защиты и т.д.

У сотрудников кредитных организаций необходимо установить круг обязанностей, процедуру осуществления платежей, наличие договора с потерпевшим как держателем платежной карты, обращения ее блокировке, о выписке по лицевому счету, о проверке правомерности списания денежных средств со счета, сумме причиненного ущерба и документах это подтверждающих.

Допрос подозреваемого.

К данному следственному действию необходимо подходить с особой тщательностью. Перед допросом должны быть изучена личность подозреваемого, его прошлый опыт, наличие и характер собранных доказательств, нормативно-справочная документация и получены консультации специалиста информационных технологий [51, с. 87].

Допрос подозреваемого предполагает некоторые законодательно закрепленные особенности. Так, перед началом допроса следователь (дознаватель) сообщает подозреваемому в совершении какого уголовно наказуемого деяния он подозревается и выясняет, признает ли подозреваемый себя виновным полностью или частично либо отрицает свою вину в совершении уголовного правонарушения *(ст. 216 УПК РК).*

В ходе допроса необходимо получить показания по каждому пункту подозрения. Для проверки показаний целесообразно периодически задавать контрольные вопросы. Участвующий в ходе допроса защитник не вправе настраивать подозреваемого на негативную позицию, в противном случае необходимо поставить вопрос о замене такого защитника.

Если подозреваемый полностью подтверждает правильность возникшего в отношении него подозрения и признает себя виновным в предъявленном подозрении, на допросе возникают бесконфликтные ситуации. В таком случае, тактические приемы направлены на получение достаточно полных и точных показаний. Несмотря на благоприятную ситуацию, допрос должен проводиться столь же тщательно и детально, как и при отрицании допрашиваемыми своей вины. Важно не само признание, а сведения о фактах, обстоятельствах, соответствующих действительности. Признание не должно дезориентировать следователя и снижать его активность в поиске доказательств [52, с. 260].

Некоторые внешне бесконфликтные ситуации в действительности являются мнимо-бесконфликтными. Подозреваемый создает подобную ситуацию с целью обмануть следователя, чтобы тот потерял бдительность и снизил тактическую активность, не искал объективные доказательства, подтверждающие их признательные показания, от которых они в судебном заседании намерены отказаться. Кроме того, мнимо-бесконфликтная ситуация дает возможность подозреваемым скрыть еще не известные следствию факты и сообщников преступных деяний, поскольку многие следователи ограничиваются достигнутым и завершают расследование [53, с. 96-98].

В ходе досудебного производства, подозреваемые лица зачастую занимают негативную позицию, отрицают свою вину. По этой причине в процессе допроса возникают конфликтные ситуации, когда они дают полностью ложные, частично ложные показания или же вообще отказываются от дачи показаний.

При возникновении конфликтной ситуации, надо постараться установить психологический контакт с допрашиваемым, после чего применять иные, наиболее эффективные тактические приемы, соответствующие сложившейся обстановке и личности подозреваемого.

В случае возникновения конфликтной ситуации особенно эффективна вопросно-ответная форма допроса.

Необходимо объяснить подозреваемому, отказывающемуся от дачи показаний, что его позиция не является препятствием к продолжению расследования, что он тем самым лишает себя возможности защищаться от предъявленного подозрения.

Во время допроса подозреваемого всегда следует помнить, что подозрение его в совершении преступления может оказаться ошибочным, что иногда сам факт задержания может сломить его волю и подозреваемый может оговорить себя.

Если подозреваемый дает ложные показания, то в процессе допроса возникают конфликтные ситуации, противодействовать данного рода ситуациям в уголовном процессе призваны ряд тактических приемов.

Наиболее эффективным в указанном случае может являться тактический прием – *предъявление доказательств, уличающих их во лжи.* При этом, стоит учитывать, что подозреваемому следует предъявлять только такие доказательства, которые достаточны для подтверждения подозрения в совершенном им преступлении. Иные доказательства, которые относятся к обстоятельствам, расширяющим объем подозрения, на данном этапе лучше не предъявлять, чтобы облегчить установление психологического контакта, не позволить подозреваемому замкнуться, уйти в себя [54, с. 66].

Еще одним действенным приемом является использование слабых мест личности, под которыми понимаются особенности психики личности *(вспыльчивость, склонность к переживаниям и т.д.).* В гневе либо при сильном волнении допрашиваемый может сказать то, что в обычном состоянии не сказал бы, либо отойти от избранных показаний и начать говорить правду. Данный прием эффективен при хорошей осведомленности следователя *(дознавателя)*с особенностями личности подозреваемого и выработкой при помощи этих сведений тактики воздействия на его эмоции. Если этот прием применять необдуманно, можно сорвать следственное действие, доведя допрашиваемого до сильного душевного волнение или более серьезного психотравмирующего состояния.

К тактическим приемам похожего действия относятся – *создание напряженности и форсированный темп допроса.* Они могут создать волнение у подозреваемого, которое может сбить его с избранных ложных показаний, при этом быстрый темп допроса не позволит ему обдумать свои ответы и даст возможность следователю (дознавателю) получить правдивые показания.

Если подозреваемый при применении указанных приемов продолжает придерживаться ложных показаний, то целесообразно по прошествии некоторого количества времени применить такие тактические приемы как *создание определенного представления об осведомленности следователя (дознавателя) и повторность*.

Первый из указанных приемов заключается в том, что следователь преднамеренно сообщает подозреваемому определенные факты или сведения, узнав о которых допрашиваемый приходит к выводу, что органам уголовного преследования известна реальная картина преступления и начинает давать правдивые показания.

При применении приема – повторность, можно получить положительный эффект с расчетом на то, что допрашиваемый оказывается не в состоянии на очередном допросе повторить показания в точности, что и на предыдущем [55].

Можно также предложить допрашиваемому дать показания в обратном порядке.

При допросе подозреваемого следует выяснить:

– обстоятельства возникновения умысла на хищение денежных средств;

– время, характер и способ хищения;

– порядок действий по приготовлению к совершению преступления (приобретение телефона, sim-карты, открытие банковского *(лицевого)*счета, перечень подключенных услуг сотового оператора, поиск сообщников, офисного помещения, приобретение и размещение в нем средств вычислительной техники и мобильной связи, необходимых для орга-

низации доступа соучастников преступления в информационно-телекоммуникационную сеть «Интернет», создание вредоносных программ, приобретение и установка вредоносного программного обеспечения, получение информации о системе;

– время и источник получения информации о потерпевших и состоянии их счетов, наличие средств на их банковских счетах;

– наличие навыков, позволяющих создавать вредоносное программное обеспечение, алгоритмы работы этих программ;

– как в его пользовании оказался абонентский номер, к которому «привязана» услуга «мобильный банк»;

– каким образом узнал о том, что к абонентскому номеру «привязана» услуга;

– пользовался ли ранее мобильным банкингом;

– процесс хищения денежных средств *(даты, обстоятельства совершения преступлений, характер и содержание sms-сообщений, виды использованных вредоносных программ)*;

– сумма похищенных денежных средств, круг соучастников, роль каждого из них;

– причины совершения преступления;

– способы сокрытия преступления *(уничтожение телефонных аппаратов, sim- карты, оформление счетов, телефонных номеров на третьих лиц, по подложным документам)*;

– каким образом распорядился похищенными средствами *(пополнял счет мобильного телефона, расплачивался за покупки, обналичивал)*;

– сообщал ли кому-либо о том, что совершает хищение, если обналичивал, указать в каком месте *(помещения кредитных организаций, общественные и иные места, где установлены банкоматы и т.д.)* [56, с. 31].

К материалам уголовного дела следует приобщать копии документов, подтверждающих полученные сведения *(распечатки sms-сообщений, сведения о движении денежных средств по счету мобильного телефона, чеки, подтверждающие факт оплаты за товар или услуг, чеки и иные документы, подтверждающие факт обналичивания денежных средств, если осуществлялся перевод денежных средств на другой счет, то приобщаются сведения о движении денежных средств по данному счету и т.д.).*

Производство обыска и выемки

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

Производство обыска и выемки при расследовании интернет-мошенничеств, связано с получением доказательств способа совершения преступления, совершенного с использованием компьютерной техники и телекоммуникационных сетей. Таким образом, главной целью производства обыска при расследовании мошенничества с использованием сети Интернет является обнаружение и изъятие электронных носителей, на которых осталась информация, касающаяся как самого мошенничества, так и лиц, совершивших это преступление *(информация об их нахождении или перемещении)*, предметы, являющиеся результатом преступления *(например, контрафактные компьютерные программы)* и документы, содержащие важную информацию для дела *(квитанции; блокнот с личными записями; документы о переводе, обналичивании денежных средств и т.д.)*. По делам об интернет-мошенничестве поисковые мероприятия при

производстве обыска отличаются специфическими особенностями и делятся на две стадии *обзорную и детальную.*

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

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

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

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

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

На детальной стадии обыска следователю необходимо:

– при осмотре работающего компьютера: с помощью специалиста, следует провести поиск компьютерной информации, имеющей значения для расследуемого преступления, в осматриваемом компьютере. Если информация, касающаяся расследуемого мошенничества с использованием сети Интернет, найдена, то необходимо определить, где именно она находится. После проведения осмотра компьютера он по всем правилам выключается, упаковывается и изымается. При осмотре неработающего компьютера: зафиксировать его месторасположение, а также *(если есть)* его периферийных устройств; определить и зафиксировать соединения компьютера с телекоммуникационными сетями, периферийным оборудованием и иными устройствами;

– при обнаружении на месте обыска и выемки мобильного телефона, смартфона или планшетного компьютера для поиска в них нужной информации, относящейся к расследуемому преступлению, совместно со специалистом, можно применить мобильный комплекс по сбору и анализу цифровых данных. В случае, если нет возможности предварительно исследовать информацию в мобильном устройстве,

следователь, по имеющимся у него сведениям, принимает решение о необходимости его изъятия. После производства обыска и выемки вся обнаруженная компьютерная техника, содержащая искомую информацию по расследуемому интернет- мошенничеству, перед изъятием должна быть правильно упакована и опечатана. По окончании обыска и выемки составляется протокол следственного действия и описи к нему.

Особенности назначения экспертиз

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

При назначении экспертизы следователь не должен допускать, с одной стороны, необоснованного промедления, а с другой – неоправданной поспешности. Успех экспертного исследования во многом зависит от полноты и своевременности представления следователем необходимых объектов и образцов для проведения экспертизы, а также правильной постановки вопросов. Экспертиза назначается немедленно после того, как собраны все необходимые для исследования объекты.

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

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

– принятие решения о необходимости назначить экспертизу;

– вынесение мотивированного постановления;

– подбор объектов, представляемых в распоряжение эксперта;

– выбор эксперта или экспертного учреждения;

– постановку вопросов, выносимых на разрешение;

– материалы уголовного дела.

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

1) Судебно-техническое исследование документов – для установления подлинности использованных документов, печатей, штампов;

2) Судебная экспертиза документов;

3) Судебно-экспертное исследование почерка и подписей – для установления личности исполнителя рукописного текста и подписи на документе, выполненной путем подражания;

4) Судебно-бухгалтерская экспертиза – для получения источника доказательств в ходе исследования хозяйственных операций;

5) Фоноскопическая экспертиза – для исследования данных контроля и записи телефонных переговоров;

6) Судебно-экспертное исследование средств компьютерной технологии – для исследования компьютерных устройств, машинных магнитных носителей информации и программных продуктов.

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

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

Судебно-экспертное исследование средств компью-

терной технологии

Объектами экспертизы являются:

1) Аппаратные объекты:

– различные виды персональных компьютеров *(настольные, портативные, карманные и т.д.)* с основными блоками *(системные блоки, мониторы)*, внутренними узлами, деталями, комплектующими и т.д. *(далее – ЭВМ)*;

– периферийные устройства различного вида и назначения;

– 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.)*;

– различные 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 документы *(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 исследование компьютерной, вычислительной технике *(периферийным устройствам, магнитным носителям)*, различные справочные данные, инструкции пользователя, а также материалы дел.

Задачи, решаемые в рамках данной методики, относятся к задачам диагностического, классификационного, идентификационного и ситуационного характера.

При производстве данной экспертизы решаются следующие вопросы:

1) По аппаратным средствам:

– каковы технические характеристики представленной компьютерной техники;

– возможно ли использование представленного технического комплекса для осуществления тех или иных функциональных задач *(например, выхода в 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 представленном системном блоке;

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

– находится ли данное программное обеспечение в работоспособном состоянии;

– каковы дата и время установки программного обеспечения *(указывается название);*

– имеются ли в предоставленных системных блоках

программы, приводящие к неправомерному доступу к охраняемой законом компьютерной информации, внесению изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ;

– 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 знаков, бланками юридических лиц и оттисками печатей);*

– имеются ли на представленных магнитных носителях ранее удаленные файлы *(указываются названия)*;

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

– каково дата и время создания файлов *(указываются названия).*

Заключение

Интернет-мошенничество – это явление, проникшее из реального мира в мир виртуальный. Мошенничество в Интернете по определению идентично мошенничеству из реального мира: это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Однако Интернет-мошенничество подчиняется законам виртуального пространства, режиму «Интернет – времени», физической удаленности пользователей друг от друга, анонимности пользователей в сети. Благодаря данным свойствам, привлечь к ответственности мошенников оказывается весьма затруднительно.

Интернет-мошенники используют все возможные каналы коммуникации в Интернете, чтобы найти потенциальных жертв. Сами сообщения мошенников являются формами коммуникации между ними и пользователями Интернета.

В процессе написания монографии был собран и изучен большой объем зарубежного и отечественного материала, также статистические данные касающиеся Интернет-мошенничеств. Вместе с тем, были определены проблемы в сфере компьютерной информации. Также были установлены факторы, влияющие на совершения мошенничеств в сети Интернет, мотивы, способствующие совершению этих преступлений. Определены причины и условия широкого распространения мошенничества в Интернете – как показывает практика, одна из главных причин, это безнаказанность мошенников. В свою очередь жертвы мошенников не обращаются в правоохранительные органы, считая это бесполезным, так проявляется высокий уровень латентности данных преступлений. Проблема усугубляется тем, что электронный платеж сложно проследить, в некоторых случаях незначи-

тельность ущерба не позволяет осуществить досудебное производство. И, пока эта ситуация не изменится, исправить положение с мошенничеством в Интернете представляется затруднительным.

Описательная часть монографии указывает на то, что, авторским коллективом описаны и рассмотрены самые распространенные виды Интернет-мошенничеств, их влияние на пользователей информационно-телекоммуникационных сетей, систем и технологий, а также особенности выявления, раскрытия и расследования фактов мошенничества, совершаемых в сети Интернет.

При написании монографии на тему «Противодействие мошенничествам в сети Интернет» выполнены все поставленные задачи:

– Раскрыта система развития Интернет-мошенничества как современного, цифрового преступного явления;

– Раскрыты основные виды, схемы и способы мошенничества;

– Указанно, какое влияние оказывает мошенничество на пользователей Интернета;

– По отдельным видам интернет-мошенничества составлены рекомендации по безопасному поведению и использованию сети Интернет.

Цель при написании данной монографии достигнута. Продукт нашей деятельности позволяет ознакомится с основными правилами безопасного использования сети Интернет. Позволяет рассказать об этом родственникам и друзьям, чтобы уменьшит риск быть обманутым в Интернете.

Результат данной работы должен удовлетворить изучающих данную тематику лиц, поскольку при написании данной монографии поставленные цели были достигнуты и читатели могут приобрести новые ценные знания, которыми

соответственно можно будет делиться с другими и применять самим.

В данной работе предлагается ряд практических рекомендаций по обеспечению безопасности в сфере Интернет-мошенничеств. Пользователям сети Интернет следует расширять знания касательно возможностей Интернета, а главное, в области виртуального пространства, в силу которых неосведомленный пользователь оказывается уязвимым перед мошенниками. Говорится о необходимости создания вебсайтов посвященных информированию пользователей Интернета об основных техниках мошенничества. Информация того же рода должна освещаться в СМИ. Правоохранительным органам необходимо законодательно урегулировать и усилить меры ответственности за виртуальное мошенничество, усилить деятельность правоохранительных органов по контролю за безопасностью в Интернете и расширить их полномочия для более высокого уровня контроля сети Интернет.

Разработанные рекомендации и методы профилактической работы по предупреждению и профилактике, а также, по эффективному выявлению, раскрытию и расследованию фактов Интернет-мошенничества, данные рекомендации помогут снизить уровень преступности данного вида в нашей Республике.

Список использованной литературы

1. Конституция Республики Казахстан от 30 августа 1995 года, с изменениями и дополнениями по состоянию на 15 мая 2022 года.
2. Источник: https://referatbooks.ru/referat/moshennichestvo-v-seti-internet-e-problemyi-vyiyavleniya/
3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК., с изменениями и дополнениями по состоянию на 15 мая 2022 года.
4. https://adilet.zan.kz/rus/docs/P170000006S
5. Антонов И.О., Шалимов А.Н. Актуальные проблемы расследования мошенничества с использованием компьютерной информации. [Электронный ресурс]. Научная электронная библиотека – Режим доступа: URL: http://cyberleninka.ru/article/n/aktualnye-problemy-rassledovaniya-moshennichestva- s-ispolzovaniem-kompyuternoy-informatsii
6. Алферова Ю.О. Проблемы квалификации компьютерного мошенничества. – Научная электронная библиотека. Режим доступа: URL: http://cyberleninka.ru/article/n/problemy-kvalifikatsii-kompyuternogo- moshennichestva.
7. Журавлева Е.Ю. Основные категории пользователей среды сети Интернет/ «Социология и Интернет:2014-2015. – С. 29.
8. Залесский П. Интернет: российская аудитория в анфас и в профиль // Медиа – альманах. 2015. №7-8. – С. 17.
9. Корытникова Н.В. Интернет как средство производства сетевых коммуникаций в условиях виртуализации общества//Социологические исследования. 2007. №2. – С. 85-93.
10. Официальный сайт ООН // http://www.un.org/ru/sections/what-we- do/protect-human-

rights/index.html, дата обращения 18.05.2022.

11. Официальный сайт Гарвардской школы права // http://glavred.info/archiv/2011/05/06/155043-9.html, дата обращения 22.05.2022.

12. ООН признала право на доступ в Интернет неотъемлемым // Российская газета. Федеральный выпуск. 7 июня2011 года. – С. 22.

13. Уголовный кодекс Федеративной Республики Германии: по состоянию на 2021г. / пер.с нем. Н.С. Рачковой; науч. ред. Д.А. Шестакова. СПб., 2021. – С. 242.

14. Уголовный кодекс Испании / пер. с испанского В.П. Зыряновой, Л.Г. Шнайдер; под ред. Н.Ф. Кузнецовой, Ф.М. Решетникова. – М.: Юрлит, 2021. – С. 260.

15. Уголовный кодекс Франции: с изменениями и дополнения на 1 января 2016 г. / пер. с фр. Н.Е. Крыловой; науч. ред. Л.В. Головко, Н.Е. Крыловой. – СПб., 2021. – С. 280.

16. Ссылка на официальный источник – https://d-russia.ru/ushherb-ot- dejatelnosti-internet-moshennikov-v-ssha-dostig-rekordnyh-6-9-mlrd-fbr.html

17. Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. №1 (68). – С. 16-20.

18. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 28.06.2022)

19. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. №1 (55). – С. 118.

20. Кудрявцев В.Н. Общая теория квалификации преступлений. – М., 1999.

21. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК., с изменениями и дополнениями по

состоянию на 15 мая 2022 года.

22. Коваль С., Мищук Л., – Калининград. «Мошенничество или гражданско- правовые отношения» Интернет ресурс: http://kaliningradadvocate.ru/2018/08/06.

23. Гражданский кодекс РК от 27 декабря 1994 года №268-XIII. Электронный ресурс: http://adilet.zan.kz/rus/docs/K940001000_.

24. Электронный ресур: https://wiki.rookee.ru/clickjacking/.

25. Интернет ресурс:http://lurkmore.to/%D0%9D%D0%BD0%B5_%D0%BF%D

26. Борчашвили И.Ш. Комментарий к УК РК. Особенная часть (том 2) – Алматы: Жетiжарғы, 2015 –- С. 1120.

27. Киберсквоттинг. Интернет ресурс.https://promopult.ru/library/%D0%9A%D

28. Кто такие киберсквоттеры. Интернет ресурс: https://uh.ua/kb/otvety/bezop

29. https://zephyrnet.com/ru/fbi-подсчитал-467-тыс.-жалоб-на-киберпреступность – в-2019-г.-на-общую-сумму-3-5-млрд-убытков/

30. ranking.kz.

31. https://ru.wikipedia.org/wiki/Ботнет

32. https://ru.wikipedia.org/wiki/Фишинг

33. https://winitpro.ru/index.php/2013/12/24/poluchenie-v-otkrytom-vide-parolej- polzovatelej-avtorizovannyx-v-windows/

34. https://cryptos.tv/fbr-doxody-kriptovymogatelej-dostigli-144-millionov/

35. https://zen.yandex.ru/media/zaim/novye-sposoby-moshennichestva-v-2022- godu-6220c0977d589c04fca144f2

36. Интернет ресурс: https://easypayments.online/blog/fraud-v-ecommerce

37. *Бембеева Г.В. Криминалистическая характеристика*

мошенничеств. 2014;

38.*Дайчмаи И. Интерпол. Всемирная система борьбы с преступностью. – М.: Рипол Классик. 2018г. – С. 48.*

39.Журавлева Е.Ю. Основные категории пользователей среды сети Интернет/ «Социология и Интернет:2014-2015. – С. 219;

40.Зайцев О. Мошенничество в Интернете и защита от него //Компьютер Пресс. 2017.№7. – С. 140;

41.Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014г. №231-V (с изменениями и дополнениями по состоянию на 01.04.2021г.) // интернет ресурс: online.zakon.kz/

42.Приказ Генерального Прокурора Республики Казахстан // «Об утверждении «Правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» от 19 сентября 2014г. №89 // Режим доступа:http://adilet.zan.kz/rus/docs/V14W0009744

43.Хан А.Л., Биндюкова Т.С. О некоторых теоретических проблемах начала досудебного расследования / Актуальные проблемы борьбы с преступлениями и иными правонарушениями //Мат.-лы четырнадцатой международ.науч.-практ. конф. /Под ред. А.А. Андреева. – Барнаул, 2016. Ч.1. – С. 200-202

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

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

46.Каиржанов Е. Криминология. Общая часть. – Алматы: Республиканский издательский кабинет, 1995. – С. 108.

47.Мошенничество в Интернете (Интернет-

мошенничество) Электронный ресурс https://allforjoomla.ru/info/306-internet-moshennichestvo

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

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

50. Коновалова В.Е. Психология в расследовании преступлений. – Харьков, 1978, – С. 63-74.

51. Кучуков К.М. Расследование мошеннических действий. – Алматы – 1999. – С. 87.

52. Герасимов И.Ф., Драпкин Я.Л. И др. Криминалистика: Учеб.для вузов; 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – С. 260. Электронный ресурс:

53. Гамаюнова А.В. Тактические приемы допроса обвиняемого (подозреваемого) в условиях конфликтных ситуаций. Тактика допроса при проверке алиби. Актуальные проблемы права: материалы III Междунар. науч. конф. (г. Москва, ноябрь 2014г.). – М.: Буки-Веди, 2014. – С. 96-98.

54. Комарков В.С. Тактика допроса: Учебное пособие. – Харьков: Изд-во Харьковского юрид. ин-та, 1975. – С. 66. Электронный ресурс: crimlib.info/images/f/f8/Честь_Псб_Комарков_Допрос.doc.

55. Белкин Р.С. Криминалистика: учебник для вузов. – М.: НОРМА, 2001. – С. 990. Электронный ресурс: www.be5.biz/pravo/k023/35.html.

56. Куприянов Е.И., Крашенинников С.В. Особенности производства отдельных следственных действий при расследовании преступлений, связанных с хищением денежных средств с счетов банковских карт посредством использования электронных платежных систем. /Российский следователь, 2018. – С. 31.

СОДЕРЖАНИЕ

Беттеу:
Туренова Б.Ю.

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу және редакциялық-баспа
жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 30 шілде 2024ж. жіберілді.
Пішімі 60х84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 5,1
Таралымы 500.