АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

ИБАДИЛЛАҰЛЫ ҰЛАН

Интернет-хищение чужого имущества: уголовно-правовые и криминологические аспекты

Диссертация на соискание степени
магистр юридических наук по образовательной программе
7М04203 «Юриспруденция» (научное и педагогическое направление)

Научный руководитель:
доцент кафедры Специальных
юридических дисциплин
Института послевузовского
образования Каженов Е.Е.,
кандидат юридических наук,
советник юстиции

г. Косшы, 2022 г.

ТҮЙІНДЕМЕ

Бұлжұмыста автор Интернет-ұрлықтың қылмыстық-құқықтық және криминологиялық аспектілерін, атап айтқанда Интернет-алаяқтық жасауды қарастырды. Диссертациялық зерттеудің мақсаты Интернет-ұрлық жасау процесіндегі теориялық және практикалық аспектілерді талдау болып табылады, оның негізінде қылмыстық заңнаманы, сондай-ақ оны қолдану практикасын жетілдіру жөнінде ұсыныстар әзірленді.

РЕЗЮМЕ

В настоящей работе автор рассмотрел уголовно-правовые и криминологические аспекты Интернет-хищений, в частности, совершение Интернет-мошенничеств. Целью диссертационного исследования является анализ теоретических и практических аспектов в процессе совершения Интернет-хищений, на основе которых выработаны предложения по совершенствованию уголовного законодательства, а также практики его применения.

RESUME

In this paper, the author considered the criminal-legal and criminological aspects of Internet theft, in particular, the commission of Internet fraud. The purpose of the dissertation research is to analyze theoretical and practical aspects in the process of committing Internet theft, on the basis of which proposals have been developed to improve criminal legislation, as well as the practice of its application.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящей диссертации применяют следующие термины с соответствующими определениями:

Алгоритм — совокупность четко сформулированных правил, определяющих последовательность решения тех или иных задач за конечное число шагов.

Аппаратные средства — электронное и механическое оборудование в компьютерной технике (в отличие от компьютерных программ). В обиходе аппаратные средства порой называют «компьютерное железо»

АРМ — автоматизированное рабочее место, оснащенное комплексом устройств, позволяющих автоматизировать часть выполняемых работником производственных операций. Основу любого АРМ составляет компьютер

База данных — совокупность больших объемов (массивов) информации, хранение и обработка которых осуществляются с помощью компьютерной техники

Байт — наименьший элемент компьютерной памяти объемом 8 бит.

Бит — минимальная единица информации, принимающая значение 0 или 1

ОВД – органы внутренних дел

РК – Республика Казахстан

УПК РК – Уголовный процесс Республики Казахстан

УК РК – Уголовный кодекс Республики Казахстан

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

МВД	– Министерство внутренних дел
МРП	– месячный расчетный показатель
ОВД	– Органы внутренних дел
пп.	– подпункт
п.	– пункт
РК	– Республика Казахстан
СНГ	– Содружество Независимых Государств
СССР	– Союз Советских Социалистических Республик
ст.	– статья
тыс.	– тысяча
УК	– Уголовный кодекс
УПК	– Уголовно-процессуальный кодекс
ч.	– часть

ВВЕДЕНИЕ

Актуальность темы исследования. Республика Казахстан является развитым государством, отдельной передовой задачей определяет внедрение информационных технологий во все сферы жизнедеятельности [1].

Нынешнее время предполагает использование передовых технологий всеми гражданами нашей страны. Однако применение в жизни человека различных «ноу-хау» подразумевают как возникновение положительных и отрицательных аспектов.

Положительной стороной является использование в жизни рядового гражданина различных средств связи, глобальной сети и т.д. В то же время такое использование может спровоцировать возникновение «плохих» мыслей у человека, переступивших черту закона. Здесь необходимо отдельно выделить тот факт, что, к сожалению «цифровая» жизнь человека предполагает возникновение и распространение Интернет-преступности, здесь остановимся на хищениях в сети Интернет.

Интернет – это прежде всего, система связанных между собой компьютерных сетей, где главной целью является сохранение и трансляция информации. В литературе можно встретить такие понятия, как «Всемирная сеть», также «Глобальная сеть» или на так-называемом разговорном стиле «Всемирная паутина» [2].

О плюсах использования такой сети известно всем, однако о отрицательных сторонах использования такой сети мы подробно раскроем далее.

Использование цифровых технологий предоставляет ряд преимуществ, среди которых: форсирование обмена информацией, упрощение доступа населения к государственным и коммерческим услугам, появление новых возможностей и дальнейшее развитие и создание цифровых продуктов.

Республика Казахстан выбрала активную позицию в вопросах использования электронно-информационных технологий, как в деятельности государственных органов, так и в иных сферах.

Все же нельзя не сказать о том, что сеть дает плохие возможности для осуществления преступного умысла.

Далее приведем статистические данные, указывающие на распространение сети Интернет в нашем государстве - охват населения широкополосным доступом к сети интернет к концу 2020 года превысил показатель в 99%. В стране активнее используется мобильный, нежели фиксированный, Интернет, за счет распространения которого в селах ведомство и рассчитывает до конца года резко увеличить количество пользователей. «Сейчас 18 млн. человек уже имеют доступ к сети 3G/4G, до конца года количество сел с доступом к мобильному широкополосному доступу увеличится до 5 тыс. 163 сел при том, что в стране существует 6 тыс. 341 сельский населенный пункт. И в целом охват населения ШПД посредством 3G/4G составит 99,3% населения [3].

Как видим из приведенного выше, показатель растет, что приводит к возрастанию потенциальных жертв кибепреступности [3, с. 10].

Таким образом, количество информационных пользователей неустанно растет, что приводит к росту потенциальных жертв Интернет-преступности. Прежде всего, причиной тому стал доступ к Интернет-технологиям всего населения мира, в том числе и жителей нашего государства [4].

Все же не можем отметить тот факт, что Интернет-ресурсы являются орудием связи лиц, совершающих правонарушения. Такое общение между соучастниками преступлений создает потенциальную угрозу для информационных пользователей «Всемирной сети».

Достаточно распространенно совершение различного рода хищений чужого имущества, преступлений, связанных с экстремизмом и терроризмом и т.д.

Значительная латентность такого рода преступлений, в процент которой входит также совершение Интернет-хищений. Как правило, причиной такой латентности является наличие признака международности и соответственно уровень таких преступлений достаточно опасен [5].

У большого числа населения создается неправильное понимание относительно Интернет-преступности, что таких преступников невозможно обнаружить и разыскать. Стоит согласиться с тем, что Интернет-преступники действительно могут находиться даже в нашей стране, но правоохранительные органы «идут в ногу со временем», разрабатываются различные способы раскрытия данного рода преступлений. Но все же уровень раскрытия таких преступлений и большое количество регистрируемых преступлений показывает реальную «картину».

Среди преступлений против собственности, Интернет-хищения продолжают оставаться наиболее часто совершаемым преступлением. Стоит отметить, что согласно правовой статистике за 2020 и 2021 гг. регистрация Интернет-хищений выглядит следующим образом: в 2020 году количество зарегистрированных преступлений составляет 33759, в 2021 году количество данных преступлений растет и составляет 41083[6] (см. Приложение 1).

Одной из причин роста хищений в сфере Интернета стала регистрация корыстных преступлений под видом мошенничеств. При этом динамика преступлений в сфере Интернета стабильно увеличивается.

В настоящей работе автор рассмотрит уголовно-правовые и криминологические аспекты Интернет-хищений, в частности, совершение Интернет-хищений, среди которых распространенным видом является Интернет-мошенничество.

Оценка современного состояния научной проблемы исследования.

Исследованием проблемных аспектов, возникающих в связи с совершением хищений в сети Интернет, в юридической науке занимались такие ученые, как Р.М. Асайнова, А.В. Геллер, Р.М.Букалерова, Б.В. Вехова, А.И. Малярова и др.

Отечественные, зарубежные ученые и юристы внесли свой значительный и весомый вклад в совершенствование уголовного права и законодательства. Однако до настоящего периода не было проведено комплексных исследований, связанных с проблемными вопросами, складывающимися в связи с совершением Интернет-хищений, что свидетельствует о необходимости проведения данного диссертационного исследования.

Вместе с тем указанные труды не были специально посвящены комплексному анализу уголовно-правовых и криминологических аспектов Интернет-хищений чужого имущества в Республике Казахстан.

Кроме того, они не учитывали достаточно длительную практику применения Уголовного кодекса Республики Казахстан 2014 года и криминологическую ситуацию, сложившуюся в Казахстане в начале третьего тысячелетия с ее новыми политическими, духовно-нравственными и социально-экономическими детерминантами, оказывающими мощное влияние на криминогенную обстановку в целом и на сферу борьбы с хищениями в частности.

Нормативной и эмпирической базой исследования являются Конституция Республики Казахстан, Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V, Нормативное постановление Верховного Суда Республики Казахстан от 11 июля 2003 года № 8 «О судебной практике по делам о хищениях». Использовано в написании настоящей диссертации отечественное и зарубежное законодательство, данные правовой статистики, обобщенные отчеты и иные документы Верховного Суда Республики Казахстан,

размещенные в справочных правовых системах, а также результаты анализа изученных 40 уголовных дел по рассматриваемой тематике. Проведено анкетирование 33 респондентов, ответы которых отражены в таблице (см. Приложение 2).

Полученный в ходе исследования эмпирический материал позволил обоснованно и достоверно сделать выводы и внести предложения.

Изложенные выше обстоятельства обусловили выбор темы исследования, ее практическую и научную актуальность.

Таким образом, не преуменьшая труд отечественных учёных-правоведов, мы считаем целесообразным исследование вышеуказанной проблематики в области уголовного права.

Целью исследования является анализ теоретических и практических аспектов в процессе совершения Интернет-хищений, на основе которых выработать предложения по совершенствованию уголовного законодательства, а также практики его применения.

Задачи исследования. Необходимость достижения указанной цели обусловила постановку и решение следующих задач:

1. Исследовать понятие Интернет-хищений, их место в системе преступлений. Проанализировать отечественный и зарубежный опыт развития уголовно-правовых и криминологических аспектов по уголовному законодательству Республики Казахстан.

2. Подробно рассмотреть уголовно-правовую характеристику хищений в сети Интернет.

3. Раскрыть детерминанты Интернет-хищений и меры борьбы с такого рода преступлениями.

Объектом исследования является совокупность правоотношений, возникающих в процессе совершения хищений чужого имущества в сети Интернет.

Предметом исследования выступают совокупность норм уголовного законодательства, регулирующих вопросы совершения хищений чужого имущества в сети Интернет и возникающих в процессе совершения таких хищений проблемных моментов.

Методы и методологические основы исследования. Методологическую основу исследования составляют общенаучные методы познания: индуктивный, дедуктивный, метод синтеза, системного анализа, а также приёмы и способы, характерные для юридических наук: логико – правовой, историко - правовой, сравнительно - правовой, формально - юридический и статистический.

Обоснование научной новизны исследования. Автором исследованы актуальные вопросы по изучения вопросов первоначальной и последующей квалификации простого и квалифицированного составов Интернет-хищений. При этом автором затронуты вопросы и проблемы совершенствования применения законодательства в части совершения Интернет-хищений чужого имущества.

В работе излагаются предложения относительно изменений и дополнений в Уголовный закон Республики Казахстан и Нормативное постановление Верховного Суда Республики Казахстан «О судебной практике по делам о хищениях».

Данные предложения помогут устранить значительные противоречия в применении отдельных правовых норм как Уголовного кодекса нашей Республики Казахстан, так и в Нормативном постановлении.

Положения, выносимые на защиту. Диссертантом на защиту выносятся следующие теоретические положения:

1. На настоящий период времени в теории и практике нет однозначного понятия «Интернет-хищения», также не введены отдельные составы относительно «новых видов преступлений как Интернет-хищения».

С учетом сказанного, предлагается в Раздел 6 «Уголовные правонарушения против собственности» Уголовного кодекса Республики Казахстан 2014 года внести самостоятельный состав со следующей редакцией:

188-2. Интернет-хищение чужого имущества

1. Интернет-хищение, то есть кража, мошенничество, присвоение или растрата чужого имущества,

Наказывается...

2. Интернет-хищение, совершенное:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения,-

наказывается …

3. Интернет-хищение, совершенное:

1) в крупном размере;

2) неоднократно, -

Наказывается…

4. Интернет-хищение, совершенное:

1) преступной группой;

2) в особо крупном размере, -

Наказывается…

В связи с предложенными изменениями и дополнениями, из Уголовного кодекса Республики Казахстан исключить:«п. 4 ч. 2 из ст. 188» и «п. 4 ч. 2 из ст. 190», так как данные пункты будут предусмотрены в диспозиции ст. 188-2 Уголовного кодекса Республики Казахстан.

2. Внесение изменений и дополнений в Нормативное постановление Верховного суда от 11 июля 2003 года № 8 «О судебной практике по делам о хищениях», где в целях правильного и единообразного применения в судебной практике действующего законодательства при квалификации уголовных

правонарушений, связанных с посягательством на чужую собственность указать понятие «Интернет-хищение», способы и виды.

В связи с чем, в Нормативное постановление Верховного суда от 11 июля 2003 года № 8 «О судебной практике по делам о хищениях» добавить пункт 1-1 который изложить в следующей редакции: «Если хищение совершено в сети интернет, то его следует квалифицировать как Интернет-хищение».

3. В настоящее время наблюдается рост интернет хищений на всей территории страны, в этой связи, в областях происходит нехватка сотрудников подразделения «К» МВД РК. Поскольку имеющаяся штатная численность сотрудников данного подразделения не рассчитана на такое большое количество регистрируемых дел. В связи чем, возникает необходимость в выделении дополнительных штатных единиц сотрудников для более эффективной борьбы с интернет хищениями.

Также необходимо учитывать, что деятельность подразделения «К» МВД РК тесно связана с IT специалистами, нехватка которых остро сказывается на кибербезопасности граждан и государства, поскольку высококвалифицированные IT специалисты имеют возможность большего заработка в частном секторе, а также лучшие условия труда чем могут предоставить в правоохранительных органах. Что существенно влияет на привлечение в качестве сотрудников правоохранительных органов.

В целях решения данной проблемы предлагается выделить увеличенную сетку оплаты труда для данной категории лиц и предоставлением необходимых условий труда.

Данные предложения позволят разграничить ответственность за совершение преступлений в сфере Интернет.

Апробация и внедрение результатов исследования. Выводы и предложения, содержащиеся в диссертационном исследовании, могут быть использованы на законодательном уровне в процессе совершенствования

уголовного законодательства, также в правоприменительной практике следственных работников и в судебной практике.

Научные положения, сформулированные в диссертации, получили свою апробацию. Данное диссертационное исследование выполнено на кафедре специальных юридических дисциплин. Основные положения диссертации нашли свое отражение в опубликованных автором научных статьях:

«Актуальные проблемы уголовной ответственности за совершение Интернет-хищения чужого имущества» // международный научный журнал «Академик», г. Караганда, Республика Казахстан.

«Состав Интернет-хищений чужого имущества» // материалы международной научной конференции «Противодействие Интернет-мошенничествам и финансовым пирамидам, возврат криминальных активов: проблемы и пути решения», г. Караганда, Республики Казахстан.

1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ-ХИЩЕНИЙ ЧУЖОГО ИМУЩЕСТВА СОГЛАСНО ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ.

1.1. Интернет хищения чужого имущества: понятие и значение.

В отличие от традиционных видов преступлений, история которых уходит в прошлое, Интернет-преступность явление новое и молодое. Нельзя говорить об Интернет преступности в отрыве от сети Интернет. Именно такие свойства Глобальной сети, как быстрота и дешевизна трансакций, анонимность, трансграничность, создают уникальные условия для совершения новых видов преступлений и для качественного видоизменения традиционных [7].

Интернет-преступность — это противоправные общественно опасные деяния, совершенные с использованием сети Интернет. К Интернет-преступлениям могут быть отнесены некоторые составы преступлений, относящихся к киберпреступности, а также преступления, не относящиеся к киберпреступности, но совершаемые с помощью сети Интернет.

Большой рост Интернет-пространства среди нас, а также переход как юридических, так и экономических отношений в цифровое пространство «Интернета», таким образом, все правонарушения происходят в Интернете. Иными словами, происходит рост и зарождения новых видов деяний.

Необходимо отметить, что цифровизация – это положительное явление, однако, как и любое явление, цифровизация имеет как положительные, так и негативные моменты. Стоит ли говорить о том, что к негативным аспектам относится появление новых более универсальных видов правонарушений, характеризующиеся некоторыми особенностями, не свойственные другим видам правонарушений. Речь идёт о Интернет-мошенничестве и краже.

Согласно статистической отчетности за 12 месяцев 2020 года в Республике Казахстан было зарегистрировано всего 33 759 фактов

мошенничества, из которых 14 220 приходится на Интернет-мошенничества [6, с. 13] (см. Диаграмма).

Таким образом, 48,1 % всей совокупности зарегистрированных мошенничеств составляет Интернет-мошенничество. В статистической отчетности ведется регистрация только по Интернет-мошенничествам, других видов правонарушений в сети Интернет нет.

Интернет-хищения достаточно распространены на территории нашего государства, происходит большой процент регистрации данных правонарушений.

Интернет-мошенничество и Интернет-хищения указаны в Уголовном кодексе Республики Казахстан, но это не отдельные виды составов, а лишь указаны в частях статей (188 и 190) [8].

Законодатель на момент принятия Уголовного кодекса 2014 года предусмотрел указанные пункты, но опять же отдельных составов ныне действующий кодекс не содержит. Стоит отметить, что введение новой статьи, регламентирующей совершение именно Интернет-хищения позволит более четко и в соответствии с санкцией статьи назначать реальное наказание правонарушителям [8].

Интернет-хищения и Интернет-мошенничество являются схожими понятиями, но на наш взгляд, понятие «Интернет-хищения» шире, чем понятие «Интернет-мошенничество». Как правило, Интернет-мошенничество является одним из видов совершения «Интернет-хищения». Способом здесь будет являться именно злоупотребление доверием пользователя в сети Интернет, либо посредством данной сети.

Объектом указанных преступлений является имущество либо права на него, здесь необходимо отразить тот факт, что имущество может быть разным, но на наш взгляд, информация в сети Интернет не будет являться объектом преступлений против собственности [8].

Также важно отличать действительное имущество собственника от разного рода услуг, оказываемых собственнику в Интернет пространстве. Поэтому перед квалификацией деяния, следует выяснить действительно ли похищенное является имуществом. Например, некоторые пользовательские соглашения Интернет-ресурсов предусматривают, что регистрируемые пользователем аккаунты не являются имуществом последнего, а значит, не подпадают под объект Интернет-хищений.

Учитывая огромное множество Интернет сервисов, коими пользуются многие люди, напрашивается мысль о законодательном урегулировании оказываемых услуг, дабы иметь общий стандарт, который будет регулировать имущественные вопросы в данных сервисах.

Отсутствие общего стандарта создает потенциально серьезную проблему с правовым урегулированием имущества, находящегося в Интернете. Так, например, взлом электронной почты не будет квалифицироваться как покушение на кражу, так как сама электронная почта не является имуществом пользователя (согласно пользовательскому соглашению).

Данное деяние будет квалифицироваться по ст. 205 УК РК как неправомерный доступ к информации, охраняемое законом, и то, только в том случае, если данное деяние повлекло существенное нарушение прав и законных интересов пользователя. Информацию, охраняемая законом – это государственные секреты, личная, семейная, врачебная, банковская, коммерческая и иная охраняемая законом тайна [8, с. 45].

Подобное обстоятельство видится несправедливым, так как электронная почта, зачастую связана со многими другими электронными сервисами, Интернет-банками, кошельками и т.д. Доступ к электронной почте может привести к доступу к иным сервисам, где может храниться имущество пользователя. Поэтому сам факт неправомерного доступа к электронной почте

имеет куда более значительную общественную опасность, нежели это установлено статьей 205 УК РК.

В первые дни зарождения истории человечества были сформированы основные обязанности и принципы наказания за это нарушение, которые легли в основу формирования законов древности.

В различных периодах единственной и единой мерой наказания за данное преступление служил так-называемый «принцип возмездия», то есть предусматривал совершение иных преступлений, более тяжелых. Затем уже с появлением цивилизации и зарождения законодательной основы возникали иные меры наказания, соответствующие тому, что и как совершил «маргинал» [9, с. 12].

Тайное хищение чужого имущества выделяет много различных черт, среди них можно определить главные – это имущество. Составляющие объективной стороны данного рода преступления проявляется именно в непосредственном обращении ворованного имущества в свою преступную пользу. То есть возникает цель и мотив посягательства, а именно меркантильная цель.

Вышеуказанные черты содержатся в однородных преступлениях, направленных против собственности. Таким образом, можно сделать вывод, что кража имеет ряд свойственных именно данному конкретному виду черт, при этом данные признаки не стоит выделять как отдельные.

Как уже было сказано ранее, предметом хищения выступают вещи и предметы, в том числе движимость и недвижимость. Выступать объектом тайного хищения могут разного рода вещи, но при этом есть исключения. Это парк, лес, сельскохозяйственные и рыбные богатства и др. [9, с. 14].

В соответствии с нормами уголовного права под хищением понимается противозаконное безвозмездное приобретение чужого имущества, которому сопутствует последующее причинение ущерба и меркантильной цели. К числу

данных преступлений есть как кража, грабеж, разбой, так и мошенничество и др.

Стоит выделить обязательные элементы тайного хищения чужого имущества являются:

1) Ворованная вещь не должна принадлежать потенциальному преступнику, то есть потенциальный преступник не должен иметь законное право на краденную вещь.

2) Присутствует признак скрытности и тайности, то есть обращение происходит в отсутствии каких-либо лиц, либо присутствии лиц, но не соображавших о значении данного происходящего.

В статье 187 и 188 уголовного закона нашего государства кража закреплена в качестве тайного хищения, состав данного деяния включает в себя все четыре элемента, среди них можно отметить – субъект и объект, субъективная и объективные стороны [9, с. 65].

На сегодняшний день уголовное законодательство прошло определенные этапы, среди которых внесение изменений касательно введения новых составов уголовных правонарушений.

Интернет-хищения чужого имущества граждан являются в последнее время достаточно распространенным уголовным правонарушением, несет в себе большую общественную опасность.

В настоящей работе сделан акцент именно на освещение уголовно-правовых и криминологических аспектов Интернет-хищений чужого имущества, перечислены виды Интернет-хищений.

До последнего времени в теории и практике нет однозначного понятия «Интернет-хищения», также не введены отдельные составы относительно «новых видов преступлений как Интернет-хищения».

С учетом сказанного, предлагается внести поправки в Уголовный кодекс Республики Казахстан 2014 года в раздел 6. «Уголовные правонарушения против собственности», ввести ст. 188-2 со следующей редакцией:

188-2. Интернет-хищение чужого имущества

1. Интернет-хищение, то есть кража, мошенничество, присвоение или растрата чужого имущества,

Наказывается...

2. Интернет-хищение, совершенное:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения,-

наказывается …

3. Интернет-хищение, совершенное:

1) в крупном размере;

2) неоднократно, -

Наказывается…

4. Интернет-хищение, совершенное:

1) преступной группой;

2) в особо крупном размере, -

Наказывается…

В уголовном законе отсутствует квалифицирующие признаки, которые влияют на практику применения ст. 190 УК РК (мошенничество). В этой связи, с учетом опыта зарубежного законодателя предлагается дополнить часть вторую ст. 188-2 УК РК новыми отягчающими признаками и изложить их в следующей редакции:

Стоит отметить, что указанные нововведения в действующий Уголовный кодекс Республики Казахстан 2014 г. позволят достаточно точно квалифицировать действия каждого исполнителя и соучастника преступления.

При этом сеть Интернет является неотъемлемым инструментов в жизни каждого человека.

1.2. Интернет хищения чужого имущества, совершенные путем обмана и злоупотребления доверием.

Мошенничество – это вид хищения, регламентированный уголовным законом РК, совершается посредством злоупотребления доверием или обмана – предоставления заведомо недостоверных сведений, сокрытия правдивой информации, направленных на введение субъекта в заблуждение.

Злоупотребление доверием – использование в корыстных целях доверительных отношений, установившихся между виновным и потерпевшим. Они могут обуславливаться служебным положением, дружеской или родственной связью. Злоупотребление доверием имеет место и в случаях, когда виновный получает предоплату за услуги/работы, которые не собирается предоставлять (осуществлять), или за товар, который не планировал передавать потерпевшему [9].

Обман – предоставление, предъявление заведомо ложных сведений (т.е. сведений, не соответствующих действительности), вводящих потерпевшего в заблуждение.

Мошенничество считается оконченным с момента завладения виновным имуществом или правом на имущество и возникновением фактической возможности распоряжаться похищенным имуществом (т.е. определять судьбу имущества)[8].

Общественная опасность мошенничества состоит в том, что оно нарушает общественные отношения собственности независимо от ее форм, связанные с порядком распределения материальных благ, установленным в государстве, по поводу не только имущества, но еще и прав на имущество. Вследствие

совершения мошенничества, с одной стороны, собственник или иной владелец имущества или права на имущество утрачивают это имущество или право на имущество, что влечет причинение им имущественного ущерба, и, с другой - лицо, овладевая этим имуществом или правом на имущество способом обмана или злоупотребления доверием незаконно, т.е. помимо и вопреки установленному в государстве порядку распределения материальных благ, обогащается на сумму, равную стоимости имущества, либо получает возможность обогащения за счет права на имущество на соответствующую сумму [9, с. 101].

Объектом «злодеяния» является право (отношение) собственности. Предметом анализируемого преступления, как и в предыдущих уголовных правонарушениях, выступает чужое имущество, имеющее признаки, описанные выше [9, с. 103].Вместе с тем, предметом мошенничества может быть не только имущество, но и право на имущество. Документы, дающие право на получение имущества, в том числе и денег, могут быть предметом мошенничества в случаях, когда они являются эквивалентом имущества, носителями определенной стоимости. К ним относятся предъявительские ценные бумаги, в том числе денежные и платежные документы, т.е. документы, в которых содержатся определенные имущественные права, причем реализовать это право можно только при условии предъявления такой бумаги [9, с. 103].

К ним также относятся, например, облигации государственного займа, сертификаты, денежные и вещевые лотереи и т.д. Завладение такими бумагами равнозначно завладению самими материальными ценностями. Они выступают знаменателями материальных ценностей, их утрата означает прямой ущерб потерпевшему, уменьшение его материальных благ, потому что вместе с документами в таких случаях утрачиваются и воплощенные в нем имущественные блага. Что же касается правовой природы имущества, то предметом мошенничества может быть имущество либо право на имущество,

не принадлежащее виновному на праве собственности. Причем последний не имеет ни действительного, ни даже предполагаемого права на распоряжение этим имуществом как своим собственным, т.к. это имущество принадлежит на праве собственности другому лицу, т.е. оно должно быть чужим для виновного [9, с. 105].

С объективной стороны закон определяет мошенничество как хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием. Таким образом, можно выделить четыре способа совершения мошенничества:

- хищение чужого имущества путем обмана;

-хищение чужого имущества путем злоупотребления доверием;

- приобретение права на чужое имущество путем обмана; - приобретение права на чужое имущество путем злоупотребления доверием. Обман при мошенничестве может выражаться в умышленном ложном утверждении о заведомо не существующих фактах либо в сокрытии фактов, которые по обстоятельствам дела должны были быть сообщены собственнику либо владельцу имущества [9, с. 110].

Объективная сторона Интернет-хищений предусматривает конкретно определенный способ совершения преступления, а именно, использование Интернет-пространства. Использование Интернет-пространства в хищении предусматривает махинации с информационной системой, это может быть блокировка, удаление, добавление, изменение информации, находящиеся в сети. Однако, данное обстоятельство не регламентировано на законодательном уровне для Интернет-мошенничества.

Так, пп.4 п.2 ст.190 УК РК устанавливает квалифицированный состав мошенничества, совершенного путём обмана или злоупотребления доверием пользователя информационной системы. Такая формулировка не указывает на особенную объективную сторону данного состава, которая проявляется в

махинациях с информационной системой. Что примечательно, так это, что Интернет-кражи наоборот предусматривают особую объективную сторону. Так, пп.4 п.2 ст.188 устанавливает квалифицированный состав кражи, совершенной путём незаконного доступа в информационную систему либо изменения информации [9, с. 113].

Верным, на наш взгляд, будет изменить формулировку Интернет-хищений, в которой необходимо будет подчеркнуть способы совершения данных уголовных правонарушений.

В остальном же объективная сторона соответствует основным составам хищений. В случае кражи это: тайное хищение чужого имущества. В случае мошенничества: хищение чужого имущества, посредством обмана и злоупотребления доверия жертв.

Но, следует отметить, что интересным видится взгляд Т.Л. Тропиной, которая подмечает, что Интернет-мошенничество не имеет в своем составе той объективной стороны, которая характерна для основного состава мошенничества – обмана или злоупотребления доверия, так как в случае Интернет-мошенничества обманывается не человек, а компьютерная система.

В качестве примера Т.Л. Тропина приводит случаи Интернет-мошенничества, когда человек, совершая определенные действия, не знает, что в этот момент передает свое имущество другому человеку [10].

Однако, с данным мнением нельзя согласиться, так как приведенные в качестве примера случаи с легкостью квалифицируются как кража, совершенная посредством Интернет пространства.

Но, можно вспомнить, что некоторые способы Интернет-хищения действительно предполагают хищение чужого имущества с ведома собственника, но без его добровольного согласия. К таким способам можно отнести так называемые программы «ransomware», которые блокируют доступ

к компьютеру до тех пор, пока пользователь не переведет определенную сумму преступникам.

Программы-вымогатели «ransomware» подразделяются на два вида, которые квалифицируются разными составами: 1) программа, требующая платы за доступ к компьютеру; 2) программа, требующая выплатить «штраф» за якобы допущенные нарушения пользователем в Интернете (просмотр запрещенного материала и тому подобное) [11].

Соответственно, первый вид программ квалифицируются как вымогательство по п.1 ст.194 УК РК [8], так как в данном случае преступники вымогают имущество собственника под угрозой блокирования доступа к компьютеру. Стоит отметить, что ст.194 не имеет квалифицированного состава для Интернет-вымогательства, что, по-нашему мнению, является явным упущением законодателя.

Второй вид программ квалифицируются как мошенничество, так как в данном случае пользователь верит в то, что блокировка установлена правоохранительными органами, ввиду допущенных им нарушений. Поэтому здесь имеется факт добровольной передачи денежной суммы мошенникам.

Однако, как мы наглядно видим, все эти виды Интернет-хищений могут квалифицироваться по имеющимся составам уголовных правонарушений, поэтому мнение Т.Л. Тропиной, несмотря на интересный подход, всё же является ошибочным мнением [10, с. 23].

Ещё более интересным, на наш взгляд, является вопрос: «Можно ли квалифицировать незаконное использование чужого компьютера с целью похитить оттуда имущество как Интернет-кражу?». Очевидно, кража здесь есть, но, не столь очевидно, что из этого случая можно наглядно увидеть, как нынешнее законодательное регулирование не совсем верно оценивает общественную опасность Интернет-хищений.

В описанном случае мы видим, что кража была совершена в информационной системе, значит, здесь будет применяться квалифицированный состав пп.4 п.2 ст.188. Однако, если мы возьмем иной случай, в котором кража осуществляется дистанционно, то всё равно деяние будет квалифицированно по пп.4 п.2 ст.188 [8, с. 68].

Здесь возникает непосредственный вопрос, как абсолютно разные деяния квалифицируются как одно, хотя общественная опасность у деяний также различна. Законодатель специально предусматривает квалифицированный состав для краж, совершенных с проникновением в чужое жилье, так как подобные деяния покушаются на несколько объектов сразу (право собственности и право неприкосновенности жилища). Так почему же Интернет-кража не имеет подобного регламентирования, ведь очевидно, что кража дистанционная и кража физическая – это два разных деяния, которые должны квалифицироваться по-разному [8, с. 69].

С учетом сказанного, предлагается внести поправки в Уголовный кодекс Республики Казахстан 2014 года в раздел 6. «Уголовные правонарушения против собственности», ввести ст. 188-2 со следующей редакцией:

Статья 188-2. Интернет-хищения чужого имущества

1. Интернет-хищения чужого имущества, совершенные в сфере кредитования, с использованием электронных платежных средств, в сфере страхования, а равно путем кражи, мошенничества, присвоения или растраты чужого имущества в сети Интернет - наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до одной тысячи двухсот часов, либо ограничением свободы на срок до пяти лет, либо лишением свободы на тот же срок, с конфискацией имущества.

Субъект Интернет-хищений является аналогично традиционному субъекту, то есть дееспособное «лицо, достигшее возраста уголовной

ответственности», на момент совершения преступления, достигший возраста уголовной ответственности 16 лет [8, с. 1]. Стоит отметить, что данный вид уголовных правонарушений характерен особой сложностью выявления субъектов правонарушения, ввиду их дистанционной деятельности и анонимности.

Субъективная сторона Интернет-хищений выражается в форме прямого умысла. Однако, на деле лицо, осуществляющее досудебное расследование, должно точно выявлять цели и мотивы совершенного деяния. Так, учитывая особенности Интернет пространства, те или иные действия Интернет пользователя могут привести к неопределенным последствиям.

Например, незаконный доступ к электронной почте (взлом) может быть произведен как с целью похищения имущества, путем использования информации, хранящийся на электронной почте, либо же с целью доступа к какой-либо семейной или личной тайны пользователя Интернет сети. Поэтому крайне важно уметь правильно выявить основные мотивы и цели правонарушителя, дабы правильно квалифицировать совершенное им правонарушение [9, с. 123].

Переходя к зарубежному опыту, можно отметить, что в Российской Федерации Интернет-кражи не регламентированы на законодательном уровне вовсе, но, Интернет-мошенничество имеет свою отдельную статью - 159.6 УК РФ [11].

«Интересным выглядит подход российского законодателя, который выделил в отдельные составы мошенничества, совершенные в тех или иных сферах деятельности – непосредственно в сфере предоставления кредита, непосредственно при получении отчислений, с внедрением электронных средств платежа, непосредственно в сфере страхования [11, с. 124]. По этой же логике выделено и Интернет-мошенничество, как мошенничество, совершенное в сфере компьютерной информации» [11, с. 124].

Однако, подобный подход вызвал споры в среде юристов. Так, например, некоторые юристы подчеркивали необоснованность подобного выделения, так как подобная логика говорит о том, что в скором времени будут выделены и остальные сферы, в которых могут быть проведены мошеннические махинации, а значит, уголовный кодекс наполнится ещё многими статьями подобного рода.

И действительно, подобное выделение выглядит как лишнее усложнение уголовного права, что в данном случае совершенно неоправданно. Очевидно, что не всякое мошенничество, совершенное в той или иной сфере, являет из себя уникальный состав. Большая часть совершенных мошенничеств подпадают под основной состав, а значит, не требуют какой-либо специальной квалификации. Но, нельзя согласиться с тем, что Интернет-мошенничество не должно выделяться в отдельную статью, так как совокупность особенностей способов совершения, обнаружения, расследования и т.д. говорит о том, что здесь необходимо квалифицировать деяние по отдельному составу уголовных правонарушений [12].

На основании изложенного, делаем вывод о том, что отечественное законодательство должно отражать реалии современного мира, предусматривать соответствующее наказание за появление новых и распространенных преступлений, а также отражать развитие цифровых технологий, так как действительность ведет к тому, что Интернет-хищения и другие уголовные правонарушения в Интернет пространстве будут количественно и качественно расти, что требует соответствующей реакции со стороны законодателя и правоохранительных органов. Поэтому можно ещё раз подчеркнуть важность отдельного урегулирования Интернет-хищений, так как правильное и удобное законодательное регламентирование позволит точнее и эффективнее бороться с нарастающей угрозой «хищений» [13].

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Мошенничество путем обмана или злоупотребления доверием пользователя информационной системы – это те же действия, но совершенные с помощью Интернета [8].

Данный вид мошенничества является относительно новым и в то же время распространенным и опасным видом преступления. Это связано, в первую очередь, с возможностью глобального (использования компьютерных технологий, позволяющих скрыть действительный источник распространяемой информации и лица, получающего денежные средства потерпевших (например, путем использования Интернет-кошелька) [9, с. 145].

В первую очередь, следует установить, какое событие произошло. Видов и схем мошенничества в сети Интернет разнообразное количество.

«Непосредственные признаки мошенничества в Интернете –требование отправки SMS (которые в действительности являются платными), например, за скачивание необходимой литературы; (письма счастья) и т.д.» [9, с. 1].

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

Наиболее известными способами совершения данного вида преступления являются фишинг, киберсквоттинг, тайпсквоттинг, мошенничество с помощью платежных систем (программного обеспечения), иные способы Интернет-мошенничества. Способов совершения Интернет-мошенничеств большое количество. Это связано в первую очередь, с существенным расширением спектра услуг, предоставляемых в сфере информационных технологий [12].

«Посредством данных сведений возможно выяснить, не совершены ли другие жульничества подобным методом, и кто их мог совершить. Кроме, указание метода Интернет-мошенничества разрешает выставить версии о лицах

его совершивших, предназначить вероятные места выискивания результатов правонарушения» [9, с. 1].

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.

Что же такое обман? Под ним подразумевается недействительное «коверкание» правдивой информации и/или есть иной способ «обмана», такой как непосредственная недоговорка той же информации либо в частичной недосказанности [9, с. 1].

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 [9, с. 1].

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 жульничества.

В большинстве случаев, акцентируют двух группы злоумышленников:

- мошенники, лишенные работы и долговременного места жительства и работы, многократно судимые после жульничества и остальные правонарушения насупротив собственности;

- мошенники-рецидивисты, совершающие в генеральном незначительные мошенничества, плотнее только их жертвами останавливаются собственные лица [9, с. 1].

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 [11].

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. [12].

Стандартные необыкновенности Интернет-мошенника по исследуемой группы задевал разрешают правоохранительным органам в ходу выполнения следствия предназначить участок обвиняемых в совершении преступления, подготовить вероятные модификации их поведения, просечь последующие воздействия и выработать гамма-алгоритм усилий расследования в ходе обнаружения правонарушения и сбора подтверждений ради их предъявления в суде.

Одной из отличительных особенностей, неотъемлемых Интернет-мошенничеству, представляется превосходство законопреступников непосредственно определенного пола [9, с. 37].

Обман может касаться как действительного намерения виновного, так и количества и качества товара, субъекта преступления и других обстоятельств, которые могут ввести в заблуждение потерпевшего.

При мошенничестве обман может быть как устным, так и письменным. Использование при хищении поддельных документов, изготовленных другими лицами, является одной из форм обмана, и эти действия дополнительной квалификации по ч. 3 ст. 385 УК РК не требуют.

Подделка, изготовление или сбыт поддельных документов, штампов, печатей, бланков, государственных знаков почтовой оплаты, государственных наград, а затем их использование при хищении тем же лицом, подлежит квалификации по совокупности преступлений по соответствующим частям ст. 190 и 385 УК РК.

При мошенничестве путем злоупотребления доверием виновный, используя доверительные отношения между ним и собственником или иным законным владельцем имущества, совершает его обман либо вводит в заблуждение [8].

Необходимо раскрыть понятие факт, под которым трактуются те непосредственно действительные ситуации, которые возникают в реальном времени» [13].

…под обманом следует понимать как неправду, не верную информацию, не полное и не достоверная передача информации другому носителю [13, с. 1].

Обман как способ совершения мошенничества может выражаться не только в искажении фактов, существовавших в прошлом или существующих в настоящем, но и в утверждениях об обстоятельствах, которые по уверению мошенника, должны произойти в будущем [9, с. 111].

Дополнительно выделим: полным составом мошенничества будет считаться в тех ситуациях, когда используется применение недостоверной информации очно либо заочно для извлечения выгоды, как установлено, чаще всего непосредственно материальной.

Впервые термин «мошенничество» был упомянут в Судебнике Ивана Грозного, в статье 58 которого указывалось: «А мошеннику таже казнь, что и татю. А кто на мошеннике взыщет, (и) доведёт на него; будет (ино) у ищеи иск пропал, а обманщика как (ни) приведут, ино его бити кнутьём». Помимо мошенничества здесь также употреблялся термин «обман», однако очевидно, что законодатель того времени в большинстве случаев использовал их для обозначения одного и того же понятия.

Мошенничество того времени носило исключительно имущественный характер. Фойницкий И.Я. указывал, что «имущественный характер проводился в мошенничестве гораздо строже, чем в татьбе, состав которой находился под чрезвычайно сильным влиянием способа действия; так, обманы, направленные к обращению свободного человека в рабство, отнесены к головной татьбе, а не к мошенничеству».

Предметом мошенничества по Судебнику могло быть лишь чужое движимое имущество, и то с некоторыми исключениями (например, гонные собаки). К тому же следует отметить, что некоторые деяния, по сути, являвшиеся мошенничеством, влекли за собой последствия гражданско-правового характера. Преступления, предметом которых было недвижимое имущество, составляли отдельную группу деяний, ответственность за которые могла быть как уголовной, так и гражданской в зависимости от самого деяния.

Главным в способе совершения мошенничества был обман, поскольку, как отмечалось выше, Судебник Ивана Грозного использовал термины «мошенник» и «обманщик» («оманщик»), не проводя между ними чётких границ. Описания обмана в законе не содержалось, поэтому можно точно

говорить лишь то, что закон к мошенническому обману относил не все имущественные обманы. К таким исключениям можно отнести, например, составление поддельных актов, торговые обманы в количестве и качестве продаваемых товаров, разрезание монеты и выдача её частей за полноценные отдельные монеты и т.д.

Подобное понимание мошенничества оставалось доминирующим вплоть до вступления в силу Уголовного кодекса РСФСР 1922 года.

В УК РСФСР 1922 года под мошенничеством понималось «получение с корыстной целью имущества или права на имущество посредством злоупотребления доверием или обмана».

Впервые термин «обман» с юридической точки зрения также был раскрыт в том же УК РСФСР в примечании к статье 187. В частности, в нём указывалось, что «обманом считается как сообщение ложных сведений, так и заведомое сокрытие обстоятельств, сообщение о которых было обязательно».

В УК РСФСР 1960 года под мошенничеством понималось завладение личным имуществом граждан или приобретение права на имущество путём обмана или злоупотребления доверием.

Распространённым способом мошенничества следует считать различные обманы относительно предмета сделки, заключающиеся в фальсификации внешнего вида, свойств, качества, количества и других характеристик различных предметов, предлагаемых для покупки или обмена. Причем использование виновным подложных документов охватывается мошенничеством, предусмотренным ст. 190 УК РК [9, с. 115].

Например, в «традиционном» мошенничестве предмет «подменяется», к примеру, при продаже одного предмета передают потенциальной жертве иной предмет: вместо настойки продают подкрашенную воду (обман в предмете сделки), вместо денег пострадавшему вручается «искусственные» купюры. Здесь следует отразить, что предмет внешне по определенным параметрам и

признакам схож, но другой вопрос – цена, стоимость, как правило, ниже. Здесь требуется внимательно изучать обстоятельства и верно давать предварительную квалификацию.

Любой обман должен считаться мошенническим, если он направлен на возбуждение у потерпевшего желания или согласия передать мошеннику имущество или право на имущество [9, с. 123].

Непременно квалифицировав преступление по «мошенничеству» следует обозначить в материалах уголовного дела все признаки «злодеяния» и не забывать о том, что полным составом уголовного преступления является все непременные составляющие, среди которых и мотив, и цель.

Вторым способом мошенничества закон называет злоупотребление доверием, при котором виновный в целях незаконного завладения имуществом или правом на имущество использует специальные полномочия виновного или его личные доверительные отношения, сложившиеся между ним и собственником или иным владельцем этого имущества, совершает его обман либо вводит в заблуждение.

В основе доверительных отношений между мошенником и потерпевшим могут лежать не только правовые основания, но и иные обстоятельства, обуславливающие такие отношения: личное знакомство, рекомендация родственников, создавшаяся конкретная обстановка и тд. Важно, чтобы по своему содержанию эти отношения обеспечивали по следующее злоупотребление ими, т.е. совершение обманных действий [9, с. 123].

Теперь остановимся на следующем понятии, как «злоупотребление доверием. В чем разница обман и злоупотребление доверием. На наш взгляд, эти два понятия схожи в своих окончательных целях, но все-же отразим одну деталь. Здесь идет в ход психологический и человеческий подход, ведь доверием нужно заслужить. А когда происходит нарушение доверия, именно

направленное на такое состояние человека, когда он думает, что делает все правильно. Но здесь происходит преступление.

Отличительной особенностью объективной стороны мошенничества является то, что потерпевший, находясь в состоянии добросовестного заблуждения, добровольно передает имущество или предоставляет преступнику право на имущество.

Со стороны нападавшего потенциальной жертве наносится урон, который выражается в материальном и моральном вреде. Под приобретением права на имущество следует понимать такие действия, когда потерпевший передает виновному различного рода документы, подтверждающие юридическую возможность приобретения того или иного имущества, путем их представления (предъявления). Таковыми являются различные лотерейные билеты, квитанции, доверенности и т.п. [8, с. 1].

Жульничество следует считать оконченным, когда имущество изъято, и виновный имеет реальную возможность пользоваться или распоряжаться им по своему усмотрению [9, с. 1].

В толковых словарях и философской литературе доверие определяется как уверенность в чьей-нибудь добросовестности, искренности, в правильности чего-нибудь. Следовательно, злоупотребление доверием, с точки зрения русского языка, заключается в незаконном или недобросовестном использовании лицом уверенности других лиц в его добросовестности, искренности.

В основе доверительных отношений между мошенником и потерпевшим могут лежать не только правовые основания, но и иные обстоятельства, обуславливающие такие отношения: личное знакомство, рекомендация родственников, создавшаяся конкретная обстановка и тд. Важно, чтобы по своему содержанию эти отношения обеспечивали по следующее злоупотребление ими, т.е. совершение обманных действий [9, с. 123].

Злоупотребление доверием - это специфический вид обмана (обман доверия). Обман - это единственный способ совершения мошенничества, ведь в случае отсутствия доказательств об использовании виновным обмана для завладения чужим имуществом состав мошенничества исключается. Второй способ мошенничества - злоупотребление доверием - в «единственном числе», то есть без обмана, не встречается [9, с. 1].

Отличительной особенностью объективной стороны мошенничества является то, что потерпевший, находясь в состоянии добросовестного заблуждения, добровольно передает имущество или предоставляет преступнику право на имущество. Вследствие этого переход имущества обычно выглядит внешне как соглашение сторон, сделка. Однако такая сделка юридически незаконна, т.к. совершена в ущерб воле потерпевшего [9, с. 1].

Имущественный ущерб потерпевшему может быть причинен, как сказано в уголовном законе, не только путем завладения его имуществом, состоящим в деньгах или материальных ценностях, но и в результате противоправного приобретения права на его имущество. Под приобретением права на имущество следует понимать такие действия, когда потерпевший передает виновному различного рода документы, подтверждающие юридическую возможность приобретения того или иного имущества, путем их представления (предъявления). Таковыми являются различные лотерейные билеты, квитанции, доверенности и т.п. [9, с. 1].

Необходимо выделить три вида приобретения права на чужое имущество путем обмана или злоупотребления доверием:

1) с целью дальнейшего завладения им, например, получения путем обмана либо злоупотребления доверием доверенности от юридического или физического лица на получение денежных средств в банке с целью их хищения;

2) для создания видимости правомерного владения им, уже находившимся у виновного, например, получение виновным путем обмана или

злоупотребления доверием правоустанавливающего документа на имущество, которым он незаконно пользуется;

3) в виде осуществления отдельного правомочия по управлению чужим имуществом без его хищения, например, получение доверенности на распоряжение данным участком.

Мошенничество, представляющее собой приобретение права на чужое имущество, является оконченным преступлением в момент, когда виновный получает реальную возможность распоряжаться этим правом по своему усмотрению или пользоваться им.

С субъективной стороны мошенничество выражается в прямом умысле. Виновный осознает, что он путем обмана или злоупотребления доверием незаконно завладевает чужим имуществом или приобретает право на него, предвидит возможность или неизбежность причинения реального ущерба и желает [9, с. 1].

У виновного лица не водилось объективного ожидания когда-нибудь воротить такое имущество. Совместно с тем, аппараты заблаговременного следствия и суды порой предусматривают предоставленное обстоятельство, что приводит к погрешностям около квалификации [9, с. 1].

Ж. приобрел у А. трактор стоимостью 6 тыс. долларов США. С целью хищения чужого имущества путем обмана и злоупотребления доверием он выплатил только 4 тыс. долларов США. Постановлением коллегии Костанайского областного суда приговор нижестоящего суда оставлен без изменения [9, с. 110].

Коллегия Верховного Суда РК, рассмотрев дело в порядке надзора, все состоявшиеся судебные постановления в отношении Ж. отменила, а дело производством прекратила за отсутствием состава преступления по следующим основаниям [9, с. 112].

Материалами дела установлено, что Ж. после заключения договора купли-продажи трактора с А. в качестве частичной оплаты его стоимости передал ему 3 тыс. 600 долларов США, а позже еще 400 долларов, а остальную сумму обещал отдать до конца года, однако не выплатил, поскольку между ними возник спор по поводу технического состояния трактора, т.е. пока А. не произведет его ремонт.

Вместе с тем по данному делу из установленных судом обстоятельств не усматривается, что Ж. уже в момент получения трактора преследовал цель обмануть А. и не выплатить часть обусловленной договором суммы. Вывод суда о направленности умысла Ж. на мошенничество построен только на предположениях.

При данных обстоятельствах речь должна идти о гражданско-правовых отношениях.

В п. 2) ст. 190 УК РК предусмотрены следующие признаки: 1) группой лиц по предварительному сговору; 2) неоднократно; 3) лицом с использованием своего служебного положения; 4) путем обмана или злоупотребления доверием пользователя информационной системы; 5) в сфере государственных закупок (ч. 2 ст. 190 УК РК).

Субъектом мошенничества является физическое вменяемое лицо, достигшее 16-летнего возраста.

Пунктом 4 ч. 2 комментируемой статьи предусмотрено совершение мошенничества путем обмана или злоупотребления доверием пользователя информационной системы.

При этом под информационной системой понимается система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса.

Пунктом 5 ч. 2 комментируемой статьи предусмотрен квалифицирующий признак «мошенничество в сфере государственных закупок» [8, с. 43].

«О государственных закупках» от 21 июля 2007 г., - это приобретение заказчиками на платной основе товаров, работ, услуг, необходимых для обеспечения функционирования, а также выполнения государственных функций либо уставной деятельности заказчика, осуществляемое в порядке, установленном настоящим Законом, а также гражданским законодательством Республики Казахстан, за исключением:

услуг, приобретаемых у физических лиц по трудовым договорам;

услуг, приобретаемых у физических лиц, не являющихся субъектами предпринимательской деятельности, по договорам возмездного оказания услуг;

государственного задания и товаров, работ, услуг, приобретаемых в рамках его выполнения в соответствии с бюджетным законодательством Республики Казахстан;

внесения взносов (вкладов), в том числе в уставный капитал юридических лиц.

В уголовном законе выделяются следующие признаки:

1) в крупном размере;

2) лицом, уполномоченным на выполнение государственных функций, либо приравненным к нему лицом, либо должностным лицом, либо лицом, занимающим ответственную государственную должность, если оно сопряжено с использованием им своего служебного положения;

3) в отношении двух или более лиц.

Если мошенничество совершено в отношении двух и более лиц, действия виновного следует квалифицировать по п. 3) ч. 3 ст. 190 УК РК.

При хищении виновный преследует корыстную цель противоправного, безвозмездного изъятия имущества (денежных средств) в свою пользу или в пользу третьих лиц.

Мошенничество необходимо отличать от нарушения эмитентом порядка выпуска эмиссионных ценных бумаг (ст. 224 УК РК), характеризующееся внесением заведомо недостоверных сведений в проспект выпуска эмиссионных ценных бумаг, а равно составлением заведомо недостоверного отчета об итогах размещения эмиссионных ценных бумаг [9, с. 15].

Присутствует интразональность совершения жульничества с неправомерным употреблением товарных кредитов.

К признакам, свидетельствующим о подготовке мошеннических действий с использованием товарного кредита, можно отнести; 1) создание организации по подложным документам на вымышленных лиц, нередко регистрируемой по нескольким юридическим адресам; 2) малый размер уставного капитала; 3) крайне неблагополучное финансовое положение учредителя к моменту заключения договора, В данном случае речь идат не о мошенничестве, ответственность за которое предусмотрена ст. 190 УК РК, а о преступном деянии в сфере экономической деятельности, квалифицируемом как лжепредпринимательство, которое по ряду признаков нельзя отнести к формам хищения [9, с. 26].

Кое-какие эксперты полагают, что лжепредпринимательство и жульничество - независимые преступления, спрашивающие раздельной квалификации. Создание вымышленной бизнесменской организации, иногда жульническое исключение принадлежности не причинило большущего ущерба, подобает анализировать как мошенничество либо будто заготовление сиречь посягательство для него, ежели исключение не закончено. Лжепредпринимательство, в итоге какого еще не причастен дородный подрыв правоохранительным интересам, препровождает собой посягательство на него.

Мошенничество необходимо отличать от изготовления, хранения, перемещения или сбыта поддельных денег или ценных бумаг (ст. 231 УК РК) [9, с. 17].

По существу рассматриваемого вопроса Верховный Суд Республики Казахстан в п. 13 нормативного постановления «О некоторых вопросах квалификации преступлений в сфере экономической деятельности» от 18 июня 2004 г. разъясняет, что если сбыт заведомо поддельных денег или ценных бумаг совершен с целью их использования как средства обмана при незаконном завладении чужим имуществом, такие деяния следует квалифицировать по совокупности [9, с. 19].

С учетом сказанного, предлагается внести поправки в Уголовный кодекс Республики Казахстан 2014 года в раздел 6. «Уголовные правонарушения против собственности», ввести ст. 188-2 со следующей редакцией:

188-2. Интернет-хищение чужого имущества

1. Интернет-хищение, то есть кража, мошенничество, присвоение или растрата чужого имущества,

Наказывается...

2. Интернет-хищение, совершенное:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения, -

Наказывается …

3. Интернет-хищение, совершенное:

1) в крупном размере;

2) неоднократно, -

Наказывается…

4. Интернет-хищение, совершенное:

1) преступной группой;

2) в особо крупном размере, -

Наказывается…

В связи с предложенными изменениями и дополнениями, из Уголовного кодекса Республики Казахстан исключить: «п. 4 ч. 2 из ст. 188» и «п. 4 ч. 2 из

ст. 190», так как данные пункты будут предусмотрены в диспозиции ст. 188-2 Уголовного кодекса Республики Казахстан.

1.3 Интернет-хищения, совершенные путем тайного хищения имущества

Противоправные общественно опасные деяния, совершенные с использованием сети Интернет именуются Интернет-преступностью. К Интернет-преступлениям могут быть отнесены некоторые составы преступлений, относящихся к киберпреступности, а также преступления, не относящиеся к киберпреступности, но совершаемые с помощью сети Интернет.

Большой рост Интернет-пространства среди нас, а также переход как юридических, так и экономических отношений в цифровое пространство «Интернета», таким образом, все правонарушения происходят в Интернете. Иными словами, происходит рост и зарождения новых видов деяний.

Необходимо отметить, что цифровизация – это положительное явление, однако, как и любое явление, цифровизация имеет как положительные, так и негативные моменты. Стоит ли говорить о том, что к негативным аспектам относится появление новых более универсальных видов правонарушений, характеризующиеся некоторыми особенностями, не свойственные другим видам правонарушений. Речь идёт о Интернет-мошенничестве и краже.

Посягательство в виде кражи всегда являлось наиболее распространенным деянием, направленным на интересы против собственности, которое существенно разрушает как материальное благополучие граждан, так и государственные интересы. Государство в таких случаях несет материальные убытки, в тоже время население теряет свою собственность в виде различных предметов и вещей, как движимых, так соответственно недвижимых [14, с. 101].

Кража открывает раздел преступлений против собственности нашего уголовного законодательства, является данное преступление одним из самых древнейших и традиционных деяний, также является менее опасным среди всей системы однородных преступлений [14, с. 103].

Хищение данного рода выделяется по степени общественной опасности, и в тоже время часто встречаемое преступление. Вопросы борьбы с данным видом преступлений рассматриваются в нашей стране на постоянной основе [9, с. 64].

В первые дни зарождения истории человечества были сформированы основные обязанности и принципы наказания за это нарушение, которые легли в основу формирования законов древности.

В различных периодах единственной и единой мерой наказания за данное преступление служил так-называемый «принцип возмездия», то есть предусматривал совершение иных преступлений, более тяжелых. Затем уже с появлением цивилизации и зарождения законодательной основы возникали иные меры наказания, соответствующие тому, что и как совершил «маргинал» [9, с. 12].

Тайное хищение чужого имущества выделяет много различных черт, среди них можно определить главные – это имущество. Составляющие объективной стороны данного рода преступления проявляется именно в непосредственном обращении ворованного имущества в свою преступную пользу. То есть возникает цель и мотив посягательства, а именно меркантильная цель.

Вышеуказанные черты содержатся в однородных преступлениях, направленных против собственности. Таким образом, можно сделать вывод, что кража имеет ряд свойственных именно данному конкретному виду черт, при этом данные признаки не стоит выделять как отдельные.

Стоит выделить обязательные элементы тайного хищения чужого имущества являются:

3) Ворованная вещь не должна принадлежать потенциальному преступнику, то есть потенциальный преступник не должен иметь законное право на краденную вещь.

4) Присутствует признак скрытности и тайности, то есть обращение происходит в отсутствии каких-либо лиц, либо присутствии лиц, но не соображавших о значении данного происходящего.

В статье 187 и 188 уголовного закона нашего государства кража закреплена в качестве тайного хищения, состав данного деяния включает в себя все четыре элемента, среди них можно отметить – субъект и объект, субъективная и объективные стороны [9, с. 65].

На сегодняшний день уголовное законодательство прошло определенные этапы, среди которых внесение изменений касательно введения новых составов уголовных правонарушений.

Интернет-хищения чужого имущества граждан являются в последнее время достаточно распространенным уголовным правонарушением, несет в себе большую общественную опасность.

Как уже было сказано ранее, предметом хищения выступают вещи и предметы, в том числе движимость и недвижимость. Выступать объектом тайного хищения могут разного рода вещи, но при этом есть исключения. Это парк, лес, сельскохозяйственные и рыбные богатства и др. [9, с. 14].

В соответствии с нормами уголовного права под хищением понимается противозаконное безвозмездное приобретение чужого имущества, которому сопутствует последующее причинение ущерба и меркантильной цели. К числу данных преступлений есть как кража, грабеж, разбой, так и мошенничество и др.

Стоит выделить обязательные элементы тайного хищения чужого имущества являются:

5) Ворованная вещь не должна принадлежать потенциальному преступнику, то есть потенциальный преступник не должен иметь законное право на краденную вещь.

6) Присутствует признак скрытности и тайности, то есть обращение происходит в отсутствии каких-либо лиц, либо присутствии лиц, но не соображавших о значении данного происходящего.

В статье 187 и 188 уголовного закона нашего государства кража закреплена в качестве тайного хищения, состав данного деяния включает в себя все четыре элемента, среди них можно отметить – субъект и объект, субъективная и объективные стороны [9, с. 65].

Кто такой субъект. Субъект – это человек, дошедший возраста уголовной ответственности. Для совершения простой кражи достаточно достичь возраста 16 лет. Исключение – возраст 14 лет для человека, совершившего квалифицирующую и особо квалифицирующую кражи. Человек должен обладать соответствующим психическим здоровьем [9, с. 66].

Объект – это то, на что нацелен совершить подозреваемый, субъективная сторона выявляется в меркантильной цели и направленном умысле, как правило, в умышленных действиях. И соответственно объективная сторона выражается в совершении противоправных действий скрытно [9, с. 64].

Основной признак кражи - латентность действий подозреваемых. Для образования состава кражи нельзя применять силу и оружие, Основная черта совершения тайного хищения – украсть предмет и исчезнуть [9, с. 34].

Следующая основополагающая черта – это изъятие и обращение. К примеру, у преступника не было корыстного умысла, его деяние может квалифицироваться как хулиганство.

Третий признак - минимальная сумма похищенного имущества. Если она составляет менее 10 или 2 МРП, например, когда похищают товар в продуктовом магазине стоимостью менее 10 МРП, деяние квалифицируется как мелкое хищение и не влечет наступления уголовной ответственности [9, с. 67].

Кража – это тайное хищение чужого имущества, которое в зависимости от квалифицирующих признаков наказывается: штрафом, исправительными работами, либо привлечением к общественным работам, либо ограничением свободы, либо лишением свободы, с конфискацией имущества или без таковой [9, с. 64].

Кража подразделяется на непосредственно рядовую, квалифицированную и особо квалифицированную кражу. Сделано это с целью разграничения ответственности за совершение деяния [9, с. 44].

Объективной стороной кражи является совершение действий, отличительной приметой следует выделить тайность изъятия краденного [9, с. 45].

Отечественное законодательство отводит особое внимание уголовной ответственности и соответствующему наказанию за кражу. В санкциях УК РК виды наказания начинаются от мягкого к более строгому, что отвечает ст. 40 УК РК. Перечень наказаний носит исчерпывающий характер. При этом, строгий вид наказания применяется в той ситуации, когда мягкий вид не позволил исправить и достичь цели самого наказания [2, с. 14].

В действующем Уголовном кодексе Республики Казахстан уголовные правонарушения состоят из преступлений и проступков [8, с. 10].

В борьбе с преступностью государство использует разнообразные способы и меры. В качестве действенного метода выступает применение наказания, которое имеет свои особенности. Большинство населения страны ошибочно заблуждаются и считают, что уголовное наказание — это исключительно лишение свободы.

Каждый случай применения наказания должен соответствовать принципам уголовного права и общим основам назначения наказания. В частности, наказание должно быть справедливым, назначаться в соответствии с действующим законодательством, отражать все отягчающие и смягчающие обстоятельства и др. [9, с. 16].

Необходимо отметить, что действующее законодательство содержит ряд норм, указанных в международных ратифицированных договорах. К примеру, в ст. 5 Всеобщей декларации прав человека оговаривается: «Никто не должен подвергнуться пыткам или жестким, обеспеченным или унижающим его достоинство обращению и наказанию» [15].

В соответствии с п. 1 ст. 39 Конституции РК «права и свободы человека и гражданина могут быть ограничены только законами и лишь непосредственно в той мере, в какой это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения» [16].

Основным проблемным аспектом назначения наказания за кражу по законодательству Республики Казахстан остается вопрос правильного и законного вынесения решения по таким делам [9, с. 34].

Как известно, суд является органом правосудия, который наделен полномочиями назначения наказания по всем категориям дел [9, с. 34].

Анализируя следственную и судебную практику, отметим, что вопросы назначения наказания за кражу остаются открытыми. Прежде всего, при назначении наказания необходимо соблюдать общие нормы закона и действовать только в данных рамках. Правильное применение норм действующего законодательства является залогом правильного и справедливого вынесения наказания.

Анализируя санкцию ст. 188 УК РК (Кража) суду необходимо учитывать ряд моментов, а именно личность, совершившего преступление, когда и в какие

сроки было совершено деяние, количество раз, были ли следствием установлены квалифицирующие признаки, было ли лицо судимо, привлекалось к ответственности и т.д. При этом не стоит забывать о том, что назначение наказание происходит от мягкого к строгому [9, с. 55].

Наказание является реализацией уголовной ответственности, при этом преступник наделяется правами и свободами, ограничить которые может только суд.

Судья при вынесении наказания лицу за совершение кражи не должен выходить за рамки уголовного дела и оценивать только те обстоятельства, которые входят в круг досудебного производства.

Стоит остановиться на фигуре самого судьи. Судья является беспристрастным, справедливым, компетентным, знающим законодательство, умеющим применять нормы и соответствующие правила.

Анализ правоприменительной практики показывает, что следователи на стадии досудебного расследования не совсем верно трактуют нормы уголовного и уголовно-процессуального законодательства и «могут ошибочно квалифицировать действия лица (лиц) по таким деяниям как кража, так как хищения против собственности могут быть и других форм» [9, с. 56].

Это в свою очередь влечет ряд последствий, среди которых есть реализация целей назначения наказания. Наказание должно быть таким, чтобы виновник данного деяния не смог повторить в будущем свои преступные цели, смог встать на путь исправления и не нарушать закон.

Если же при расследовании уголовных дел, связанных с тайным хищением чужого имущества, следователь не укажет какое-либо событие или обстоятельство, то в будущем судья не сможет вынести правомерное и правильное наказание, так как изначально само назначение наказание теряет смысл.

К примеру, гражданин А., находясь в ресторане с гражданкой Б., распивал с ней спиртные напитки. Затем они вышли из ресторана, где воспользовавшись тем, что Б. находилась в сильном алкогольном опьянении, снял с ее пальца золотое кольцо и пытался скрыться, но был задержан на месте сотрудниками полиции [9, с. 78].

Суд первой инстанции пустил уроженца Н. виноватым согласно ст. 191 УК РК (Грабительство). Суд счел, как влияния виноватого квалифицированы никак неправильно. Н. во пора воровства считалась в спиртном охмелении и никак не вспоминала договора случившегося. Н. счел, то как пострадавшая никак не понимает обстоятельство кражи ее имущества. Его действия невольно заметили невзначай проходившие рядом свидетели. Как-нибудь зная о данном, то есть как Н. встретил пострадавшую и забрал кольцо, понимая, то как его внебрачные влияния открыты чужими лицами, во использованные тканях преступного процесса нет. Наличие сходных обстоятельствах влияния, однако обязаны представлять собой квалифицированы одинаково как-нибудь кража [9, с. 66].

Сходным способом, наличие изыскании абсолютно полных факторов преступного процесса, судебный процесс должен держаться главными основами, такими одинаково как-нибудь правомерность, гуманность, достоверность.

Судебный процесс должен учитывать требования уголовного законодательства:

1) картина совершенного преступления - криминальное действие или преступный преступление. То есть разграничить, реализовано воровство или маленькое воровство.

2) присутствие исключающих общественную угрозу поступка также караемость факторов;

3) отсутствие оснований освобождения с преступной ответственности;

4) ввести изъян оснований, наличие наличии которых тип, свершившее преступное правонарушение, обязано появляться выпущено с разрешения;

5) уровень незаконного планы также предпосылки;

6) уровень также пейзаж роли лиц во совершении преступного правонарушения;

7) следование строя употребления разнообразных разновидностей разрешения [15, с. 101].

Назначение наказание за кражу несет в себе не только исправление виновного лица, но получение данным лицом заслуженного наказания в установленных пределах.

Таким образом, судам необходимо неукоснительно соблюдать вышеуказанные нормы и формировать положительный опыт применения установленной системы наказания со строгим соблюдением норм законов.

2. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОФИЛАКТИКА ИНТЕРНЕТ-ХИЩЕНИЙ ЧУЖОГО ИМУЩЕСТВА.

2.1. Детерминанты Интернет-хищений чужого имущества.

Причины преступности являются наиболее специфичной и актуальной проблемой, как в теории, так и в практической деятельности. Такое выделение «причин преступности» на наш взгляд, служит последующим раскрытием такого рода преступлений, как Интернет-хищения.

Правоприменитель изучив причин Интернет-преступности сможет с одной стороны «вскрывает» природу этого негативного асоциального явления, в тоже время может «растолковывать» возникновение такой преступности, как Интернет-хищения. Здесь же может сделать вывод, что способствует возникновению такому негативному явлению.

Различными учеными, дается «определение детерминизм, то есть причинность или взаимосвязь, иными словами, понимается как одна из форм детерминации, отражающих существенную особенность бытия - всеобщую связь, взаимозависимость и взаимообусловленность явлений и процессов» [17].

При изучении и описании детерминантов преступности часто встречаемым понятием является «фактор». В ходе изучению литературы по криминологии, нами сделан вывод, что данная дефиниция применяется для первостепенного обозначения такого явления, а также изучения взаимосвязанных между собой явлений и процессов [17, с. 1].

По мере углубления познания задача исследователя состоит в определении степени и интенсивности взаимодействия, взаимовлияния выявленных факторов, установлении между ними функциональных и причинных зависимостей. В результате отдельные факторы, обладающие причинной связью с преступностью, рассматриваются в качестве ее причин, другие выступают условиями, ей способствующими.

Изучив и уяснив природу возникновения и зарождения причин и условий криминального поведения «маргиналов», правоприменитель может в дальнейшем предусмотреть такой момент, как разрозненные между собой явления и процессы связаны [17, с. 3].

На наш взгляд, уяснив предпосылки отрицательного явления можно понять в какую сторону действовать должностным лицам и как предупреждать создание угрозы в сети Интернет.

Раскрывая понятие «детерминант преступности» и на основе полученных знаний о нем, тем самым законодатель обеспечивает действенную борьбу с преступностью и может в последующем определить перечень необходимых мер по предупреждению возникновения такого негативного явления, как Интернет-хищения [17, с. 1].

Задача правоприменителя заключается в выявлении специфических черт преступного поведения, определения места Интернет-хищений в общей массе регистрируемых преступлений против собственности. Здесь отметим, как говорилось ранее, регистрация в правовой статистике отражает лишь регистрацию именно Интернет-мошенничеств, но никак не Интернет-хищений.

Тем самым мы не видим реальную «картину» совершения хищений в сети Интернет, какие виды и способы превалируют, какие имеют место быть и т.д., иными словами, проявляется определенная «скрытая латентность» хищений в сети Интернет.

Проблемный насущный вопрос относительно причин возникновении Интернет-преступности является наиболее актуальным и достаточно открытым. В настоящее время с учетом роста преступлений в цифровой среде нашей страны и роста числа пользователей Глобальной сети отражает настоящую действительность «роста злодеяний» [17, с. 1].

Этого недостаточно, ведь совершение определенного преступления, например, в общественном месте еще не означает, что причина - плохая охрана

порядка в общественных местах. Поэтому, прежде чем приступить к освещению одного из наиболее сложных и по своей сути действительно центральных вопросов криминологической науки о причинах преступности, следует заметить, что система данного криминологического знания охватывает не только собственно причины в их философском понимании, переведенном на криминологический язык [17, с. 1].

Раскрывая понятие «детерминант преступности» и на основе полученных знаний о нем, тем самым законодатель обеспечивает действенную борьбу с преступностью и может в последующем определить перечень необходимых мер по предупреждению возникновения такого негативного явления, как Интернет-хищения.

Задача правоприменителя заключается в выявлении специфических черт преступного поведения, определения места Интернет-хищений в общей массе регистрируемых преступлений против собственности. Здесь отметим, как говорилось ранее, регистрация в правовой статистике отражает лишь регистрацию именно Интернет-мошенничеств, но никак не Интернет-хищений.

Изучение преступности, ее изменений, региональных различий - это начальный пункт криминологического исследования. Само по себе выявление фактической картины преступности и ее развития еще не дает ответ на вопрос, что же делать.

Этого недостаточно, ведь совершение определенного преступления, например, в общественном месте еще не означает, что причина - плохая охрана порядка в общественных местах. Поэтому, прежде чем приступить к освещению одного из наиболее сложных и по своей сути действительно центральных вопросов криминологической науки о причинах преступности, следует заметить, что система данного криминологического знания охватывает не только собственно причины в их философском понимании, переведенном на криминологический язык.

Для создания систематизированного учения о причинах преступности необходимо учитывать, что они прямо связаны с действием весьма широкого спектра предопределяющих, стимулирующих либо сопутствующих причинам преступности условий, факторов, обстоятельств, ситуаций и др. Более того, для криминологии важно оценить значение самих этих терминов: причины, условия, обстоятельства, факторы, причем применительно как к преступности в целом (и отдельным ее видам), так и к конкретным преступлениям [16].

Тем самым мы не видим реальную «картину» совершения хищений в сети Интернет, какие виды и способы превалируют, какие имеют место быть и т.д., иными словами, проявляется определенная «скрытая латентность» хищений в сети Интернет.

Проблемный насущный вопрос относительно причин возникновении Интернет-преступности является наиболее актуальным и достаточно открытым. В настоящее время с учетом роста преступлений в цифровой среде нашей страны и роста числа пользователей Глобальной сети отражает необходимость изучения новых предпосылок и впредь недопущения совершения новых преступлений [17, с. 89].

Надо иметь в виду, что изучение возникновение отрицательного явления «злодеяния» в сфере Интернет, то можно разработать различные методики по предупреждению преступности, и в будущем исключить распространение угрозы, как со стороны внутренних нарушителей, так и внешних [17, с. 1].

Детерминация – это введенное непосредственное обозначение «маргинального поведения» людей, которое в общем дает непосредственное представление об изучаемом аспекте, в разрезе определения наиболее важных и ценных факторов [17, с. 1].

Общее определение причин преступности, оцениваемое как исходная научная позиция, сводится к тому, что под причиной понимается явление (или совокупность взаимосвязанных явлений), которое порождает, производит

другое явление (явления), рассматриваемое в этих случаях как следствие (или действие). Имея в виду причины преступности (совокупность взаимосвязанных явлений), их следствием выступает преступность (преступность как явление). Но причина создает возможность определенного следствия, для наступления которого необходимы еще и условия. Сами по себе условия не могут породить, произвести следствие, но в соответствующей ситуации (обстановке, обстоятельствах) способствуют реализации действия причины [17, с. 1].

Это относится и к причинам преступности и к ее условиям тоже. Однако при решении проблемы причин преступности надо учитывать различные типы связей: связи строения, связи функционирования, социально-генетические связи, причинно-следственные, многие друге связи и взаимозависимости. Некоторые из них имеют общие черты, но, безусловно, обладают самостоятельными особенностями [17, с. 1].

Изучая причины преступности, ученые обычно акцентируют внимание на причинно-следственных связях. Но абсолютизация их недопустима. Это может привести к изоляции отдельных явлений, к отчленению их от взаимосвязей с другими явлениями. Поэтому при изучении преступности нельзя видеть только одну связь - связь между причиной и следствием. Причина и следствие в таких случаях выступают в единстве, взаимно заменяют друг друга, порой даже не различаются. Стало быть, изучая причины преступности, надо иметь в виду и их следствия - саму преступность [17, с. 1].

Непосредственно ради криминологической науки расследование располагает величественное значение. Собственно, они и характеризуют преступность. Впрочем, существенно обозначить вновь одно обстоятельство. Для более совершенного исследования первопричин преступности, с учетом сориентированных связей, должно обследовать не столько первопричины взлета (роста) предоставленного явления, однако и причины его спада (снижения). Надобно сопоставлять доброжелатель с приятелем и те, и

остальные причины. Это дает вероятность довольно всесторонне проверить корпоративные связи преступности, положительно сориентироваться в причинности (причина, условие, следствие, результат) [17, с. 1].

В антагонистическом случае около исследованье преступности как явления не представляется вероятным увидеть, во-первых, корешки данного явления, во-вторых, своеобразные необыкновенности его причин. Это будет сползание после плоскости явлений. В целом первопричины преступности как явления очутятся описательными, не разъясняющими сущности обстоятельства и вопроса про то, оттого уровень преступности опускается или, напротив, увеличивается» [18].

Приступая к познанию криминологической теории причинности, представляется необходимым, прежде всего, рассмотреть соотношение понятий причины и условия. Как уже отмечалось ранее, причина рассматривается в системе необходимой связи явлений, из которых одно (причина) обусловливает, порождает другое (следствие или действие). Здесь можно говорить не только о причинах преступности, но и о причинах конкретного преступления: в одном случае причина (причины) порождает следствие (преступность как явление); в другом - причина (причины) порождает действие (преступление, конкретное деяние) [17, с. 1].

Поступок всегда индивидуален, как индивидуальны сама личность и та ситуация, которая обусловила данное поведение. Однако понятие «ситуация», как мне представляется, более широкое и менее конкретизированное, чем понятие «обстоятельства.

Обстоятельства напрямую связаны с конкретным человеком и его действиями. Это тот внешний фактор, который можно назвать объективным содержанием конкретного окружения человека в данный момент.

Именно в этом смысле решение вопроса связано с человеком, конкретной личностью и ее окружением. Не случайно ученые, ведя речь о причинах

преступлений, относящихся к самой личности, говорят о «внешних обстоятельствах», о том, что преступление может быть совершено в силу неблагоприятного стечения обстоятельств, что совершению конкретного преступления иногда способствуют случайные обстоятельства и т.д.

Конечно, человек не властен над обстоятельствами, иногда они сильнее его и потому могут помешать принять правильное решение. Но в принципе человек может подняться выше сложившихся обстоятельств, при этом для данной личности исчезнут причины и условия преступления, и оно не совершится».

В общественной жизни нет однозначных факторов, имеющих только положительную либо отрицательную направленность. Обычно все факторы в криминологии делятся на две основные группы: криминогенные и антикриминогенные. Совокупность факторов является своеобразным фоном общественного развития, на котором происходят (под воздействием криминогенных и антикриминогенных факторов) изменения преступности. Это как бы исходное измерение, являющееся основой криминологических исследований, обеспечивающих познание преступности на фоне происходящих изменений общественной жизни, общественного развития.

Конечно, механизм воздействия факторов на преступность весьма сложен. Поэтому часто о влиянии того или иного фактора можно говорить лишь условно, ибо положительное или отрицательное влияние той или иной стороны общественной жизни (явления, процесса) зависит от конкретной комбинации факторов.

Криминогенные моменты сами не порождают преступность. Противодействие таковых факторов, а временами и воздействие следствий их развития, высказывается в том, что они объективно споспешествуют преступности, упрощают ее существование. Это происходит вместе с воздействием антикриминогенных факторов, беспристрастно через причины,

условия и факторов представление обстоятельства. Оно обычно применяется тогда, иногда должно сформулировать то, что именно возникло, сформировалось на данный пункт кругом такого сиречь некоторого человека. Оттого предоставленное представление в некоторого ступени отождествляется с соображением ситуация, какое обозначает положение, обстановку, сумму обстоятельств. Всякий ход человека, потреблять в конечном счете счет реагирования сплетни на соответствующую обстановку» [19].

Надо, безусловно, признать верным и то, что такие выводы служат основанием для исследования связей преступности с другими массовыми явлениями на уровне обобщения. Они (эти выводы) служат реальной научной базой для разработки мер предупреждения преступности как социально-правового явления и профилактики антиобщественного поведения [20].

Рекомендуется обращать внимание на три основных фактора, позволяющих изобличить (выявить) попытку совершения мошенничества в сети Интернет:

Рекомендации Интернет-пользователям могут состоять в следующем:

Необходимо внимательно следить за обложкой ресурса, на который непосредственно переходите по набранной ссылке, стоит внимательно отнестись к передаче данных, так как введенная единожды информация на ресурсе, оставляет следы в виде фамилии, имени, отчестве, а также указания номера банковской карты.

В качестве рекомендации стоит отразить о должном и внимательном обращении на Интернет-площадке, так как Глобальная сеть несет в себе различные риски, у многих людей вся информация хранится на носителях, в том числе мобильных телефонах, цифровых источниках и тд. [21].

Рекомендации Интернет-пользователям могут состоять в следующем:

нужно осознавать – ценовая политика остается одинаковой, не стоит сразу же реагировать и оплачивать за тот товар, который имеет стоимость ниже рыночной.

также потенциальными покупателями стоит задуматься относительно местоположения ресурса, то есть выходные данные о непосредственном расположении: адрес, название и тд.

Основные непосредственно запретные функции, которые не нужно использовать в сети Интернет:

– не приводить ввод своих данных, не переходить по различным интернет-источникам;

– нельзя вести переписку с различными людьми, в том числе и детям;

– не приобретать сомнительный товар через ресурсы;

– категорически запрещено производить оплату своим знакомым, которые «якобы просят деньги в долг и тд». Стоит убедиться в просьбе лично либо очно [22].

В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности требуют криминализации ряда общественно опасных деяний и самостоятельной охраны названных отношений в отдельной главе Особенной части Уголовного кодекса.

Таким образом, зная природу возникновения Интернет-хищений можно вести соответствующую правовую борьбу с такого рода хищениями, а также предотвратить распространение Интернет-преступности.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуется принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, разработка средств защиты информации, совершенствования нормативной правовой базы в данной сфере.

2.2. Меры предупреждения и борьбы с интернет хищениями чужого имущества.

Вопросы борьбы с хищениями чужого имущества по-прежнему актуальны во всем мире. Следует отметить, что Интернет-хищения являются достаточно новыми преступлениями и меры борьбы с ними пока разрабатываются.

Одной из обязательных атрибутов в правоохранительной деятельности стоит отразить предупреждение преступности, в том числе и киберпреступности.

Для чего служит предупреждение, здесь, конечно же в первую очередь предотвращение попыток совершения преступлений, уменьшение их роста как гласным, так и негласным способом.

В настоящее время существует большое количество различных способов хищений в сети Интернет. Однако с течением времени появляются все новые виды такого рода преступлений иными словами, к сожалению, преступность на один шаг впереди [23].

Основные мерами предупреждения уголовных правонарушений данного вида заключаются в обеспечении информированности граждан о существующих видах мошенничеств, которые с каждым годом видоизменяются, в частности в связи с развитием цифровых технологий.

В настоящее время все больше фактов мошенничества происходит с использованием сети Интернет, что вызывает определенные сложности в поимке причастных лиц.

Следует выделить следующие направления и наиболее важные аспекты профилактики мошенничества.

1. Совершенствование информационно-аналитической деятельности ОВД по противодействию мошенничествам.

2. Формирование ведомственной базы данных оперативно-значимой информации, информационно-аналитической базы специальных оперативных учетов о лицах, систематически совершающих мошенничество.

3. Приумножение взаимодействия органов со средствами массовой информации.

Использование средств массовой информации в системе противодействия «плутовству» должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями; проведение правовой пропаганды, направленной на формирование правосознания; информирование населения о средствах и методах защиты от аферистских посягательств, о новых формах [24].

К работе со СМИ необходимо привлекать и общественные организации, заинтересованные в противодействии мошенничества (в том числе популярных блогеров).

4. Организация волонтерского движения в сфере противодействия мошенничеству, Интернет-мошенничеству (с привлечением молодежи, блогеров, активистов).

5. Предупреждение мошенничеств требует дифференцированного (раздельного) подхода, в зависимости от способа совершения:

1) в сфере употребления телефонной связи: объяснение работниками пластиковых созданий при совершении акций для большущую сумму личиками престарелого года о прецедентах вероятного совершения мошенничества; ужесточение ответственности за разглашение работниками финансово-банковской сферы индивидуальных предоставленных граждан;

2) в сфере кредитования: уведомление правоохранительных органов пластиковыми учреждениями о прецедентах предоставления неправильных сведений при попытке извлечения кредита, скрупулезное расследование

сплетни вероятного заемщика, разбор пластиковой банковской летописи заемщика;

3) в сфере страхования: углубление внутреннего контроля в страховых организациях за работниками для того недопущения сговора на хищение; заказ оформления страхового варианта соучастниками происшествия помимо уполномоченного работника ОВД в сфере путевой безопасности;

4) в сфере недвижимости: создание ОВД реестра граждан – вероятных потерпевших (одинокие пенсионеры, узколобо работоспособные и недееспособные граждане; лица, злоупотребляющие алкогольными напитками и т. непременное дактилоскопирование граждан, помещающихся в группы риска, в мишенях удостоверения сплетни в случае подмены документы прочерчивание виктимологической профилактики.

Персональная профилактика жульничества соответственна подсоединять последующие меры:

1) предупредительный протокол лиц, завлеченных к управленческой ответственности за мелкое присвоение постороннего имущества, произведенное хорошенько мошенничества; лиц, закончивших жульнические действия, но не завлеченных к ответственности в связи с недостижением 16-летнего возраста;

2) компенсация воздействия фаворитов санкционированных жульнических компаний для прочих соучастников хорошенько их направления ради отбывания наказания в другие области; непременное указание эксплуатационного контроля о освободившихся изо мест обособленности лидеров мошеннических преступных групп.

7. Как было указано выше важным направлением профилактики мошенничеств является виктимологическая профилактика (т.е. профилактическая работа с потенциальными жертвами по недопущению и

устранению допущенных факторов, провоцирующих потенциальных правонарушителей на посягательство) [25].

Основной формой виктимологической профилактики является распространение через СМИ профилактических видеоматериалов, наглядных памяток, буклетов о наиболее распространенных ситуациях, видах и способах противоправных посягательств, связанных с мошенничеством [26].

Рекомендуется обращать внимание на три основных фактора, позволяющих изобличить (выявить) попытку совершения мошенничества в сети Интернет:

Рекомендации Интернет-пользователям могут состоять в следующем:

Необходимо внимательно следить за обложкой ресурса, на который непосредственно переходите по набранной ссылке, стоит внимательно отнестись к передаче данных, так как введенная единожды информация на ресурсе, оставляет следы в виде фамилии, имени, отчестве, а также указания номера банковской карты.

В качестве рекомендации стоит отразить о должном и внимательном обращении на Интернет-площадке, так как Глобальная сеть несет в себе различные риски, у многих людей вся информация хранится на носителях, в том числе мобильных телефонах, цифровых источниках и тд. [27].

Рекомендации Интернет-пользователям могут состоять в следующем:

нужно осознавать – ценовая политика остается одинаковой, не стоит сразу же реагировать и оплачивать за тот товар, который имеет стоимость ниже рыночной.

также потенциальными покупателями стоит задуматься относительно местоположения ресурса, то есть выходные данные о непосредственном расположении: адрес, название и тд.

Основные непосредственно запретные функции, которые не нужно использовать в сети Интернет:

– не приводить ввод своих данных, не переходить по различным интернет-источникам;

– нельзя вести переписку с различными людьми, в том числе и детям;

– не приобретать сомнительный товар через ресурсы;

– категорически запрещено производить оплату своим знакомым, которые «якобы просят деньги в долг и тд». Стоит убедиться в просьбе лично либо очно [28].

В рамках профилактических мероприятий нужно дозировано предоставлять информацию, так как весь массив информации может дать возможность потенциальным аферистам вскрыть все моменты как для себя лично так и для своих соратников. Люди должны владеть информацией точечно, очень осторожно использовать полученную информацию, на основе чего делать правильные выводы.

Предупреждение должно работать не только с одной стороны, но должна быть адекватная реакция [29].

Таким образом, виктимологическая профилактика мошенничеств – это:

1) организованная работа всех служб правоохранительных органов:
2) зависеть от «списка потенциальных жертв»
3) производить учет всех лиц, склонных к совершению «жульничества»
4) разрабатывать на постоянной основе перечень действенных мери конкретных программ»

Одним из насущных и актуальных вопросов является увеличение количества работников, отвечающих новейшим требованиям. Наверняка в наше время люди с техническим и компьютерным уклоном являются достаточно профессиональными, владеющими навыками и умениями для предупреждения и расследования досудебных производств [30].

Генеральными задачами государственного института вырабатывания в

сфере предоставления информативной безвредности являются: отношение в реализации общегосударственной политики, разработка документов после стандартизации, установление технологической деятельности, прочерчивание технологической экспертизы проектов, установление подготовки, переподготовки и увеличения квалификации в области информативной безвредности [31].

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с «злодеяниями» в сфере Интернет. Помимо этого, необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с уголовными правонарушениями в сфере информатизации и связи.

Требуется правовое обеспечение информационной сферы на государственном уровне, в связи, с чем следует обратить особое внимание на правовые механизмы, регулирующие:

1) информационные правоотношения, возникающие при поиске, получении, потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг;

2) процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг;

3) информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры [32].

Недостаточная согласованность используемых правовых механизмов, фрагментарность деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточная эффективность,

противоречивость правовых норм, характерная для нынешнего состояния правового обеспечения противодействия уголовным правонарушениям в сфере информатизации и связи, в совокупности создают серьезную угрозу информационной безопасности государства [33].

Анализ показывает, что национальное уголовное законодательство государств в сфере ответственности за уголовные правонарушения в сфере информатизации и связи характеризуется относительным разнообразием. Развитие и изменение национального законодательства по противодействию уголовным правонарушениям в сфере информатизации и связи в вышеназванных государствах обусловлены появлением и тенденциями развития уголовных правонарушений в сфере информатизации и связи, и при подробном анализе обнаруживаются лишь некоторые закономерности.

Отсутствие социального контроля порождает долгосрочные социально-негативные тенденции. Интернет представляет собой глобальную компьютерную сеть, основанную на принципе саморегуляции, автономности, самодостаточности. Являясь глобальной формой организации общественных отношений, Интернет обществом вовсе не контролируется. Неурегулированность правом информационных процессов, трудности правоприменения, незащищенность интересов сетевых пользователей приводят к возрастанию правового нигилизма. Это состояние является следствием деформации нравственного сознания. Сегодня в сознании людей идет активная переоценка нравственных приоритетов -особое значение придается материальному успеху и власти как способам занять достойное положение в обществе.

Имеющиеся недостатки в правовом регулировании электронной торговли привели к тому, что потребители вынуждены нести на себе все риски предпринимательства. Предприниматели, потерпевшие ущерб от экономических преступлений, перекладывают потери на покупателей. Не

урегулированы вопросы заключения сделок в электронной форме, что не позволяет говорить о полноценной реализации концепции электронного бизнеса . Правовые недостатки в сфере защиты прав потребителей привели к тому, что покупатели настороженно относятся к возможности покупок через Интернет. Главная проблема заключается не в содержании норм, которые соответствуют общемировым требования, а в том, что контролировать исполнение законодательства в Интернет некому.

Отличие Интернет-хищения совершенного путем обмана и злоупотребления доверием от других видов хищений заключается в том, что потерпевшая сторона, веденная преступником в заблуждение, добровольно и сознательно передает последнему имеющиеся денежные средства в надежде получить материальную выгоду или избежать нежелательных последствий. Мошенничество совершается всегда открыто для потерпевшего, но связано с введением его в заблуждение относительно тех или иных фактических обстоятельств. При этом обман обнаруживается, как правило, не сразу, а через период времени, позволяющий не только полностью завладеть имуществом, но и скрыть какие-то важные обстоятельства.

Совершенствование информационных технологий и проникновение их во все сферы человеческой жизнедеятельности ведет к возникновению новых форм преступных посягательств и криминализации новых деяний, а это, в свою очередь, к необходимости выработки эффективных мер борьбы с ними, внесению изменений в уже существующее уголовное законодательство и принятию новых норм [34].

Бесспорно, эффективное международное сотрудничество в борьбе с уголовными правонарушениями в сфере информатизации и связи невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой - уголовной ответственности не предусмотрено. Отсутствие единообразия в национальном уголовном законодательстве стран может

негативно отразиться на развитии методов эффективной борьбы с уголовными правонарушениями в сфере информатизации и связи - явлением, для которого не существует государственных границ.

Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются преступниками, орудующими в сфере информатизации и связи, независимо от юрисдикции государств, с помощью компьютера и доступа в Интернет [35].

Эффективное противостояние уголовным правонарушениям в сфере информатизации и связи, учитывая ее трансграничный характер, невозможно, если расследование преступлений, выдача правонарушителей, их преследование в суде затруднены или вообще неосуществимы из - за нестыковок в национальном уголовном законодательстве отдельных стран.

Фактически, эти различия ограждают преступников в сфере информатизации и связи от преследования, являясь своеобразным «барьером», позволяют уйти от ответственности, оставляя безнаказанными их деяния.

Вследствие этого государства, прилагающие усилия для защиты своих граждан от преступников совершающих уголовные правонарушения в сфере информатизации и связи, тратят их впустую. С другой стороны, из-за различий уголовно-правового регулирования отношений в сфере информационных технологий лица, соблюдающие законы своего государства, могут подвергнуться уголовному преследованию в другом. Такая ситуация диктует потребность выработки международной стратегии борьбы с уголовными правонарушениями в сфере информатизации и связи и унификации национальных законодательств в области уголовно-правового регулирования отношений в сфере информационных технологий [36].

Приходится констатировать, что законодательное регулирование анализируемых отношений в уголовно-правовой сфере отстает от

стремительного развития компьютерных технологий. В настоящее время ответственность за уголовные правонарушения в сфере информатизации и связи в уголовном законодательстве не отражает глобальных перемен в непрерывном, стремительном процессе информационного развития человечества. Уголовное законодательство недостаточно эффективно регулирует отношения, складывающиеся при совершении уголовных правонарушений в сфере информатизации и связи, вследствие чего не реализуются его охранительные и предупредительные функции.

Уголовная ответственность в законодательстве Казахстана, как и в законодательстве некоторых государств СНГ, предусмотрена за компьютерные преступления, т. е. за преступления, которые совершаются в отношении компьютеров и компьютерной информации, при этом деяния, которые совершаются с их использованием и посягают на другие объекты уголовно-правовой охраны, остаются вне сферы уголовной ответственности [36, с. 87].

В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности требуют криминализации ряда общественно опасных деяний и самостоятельной охраны названных отношений в отдельной главе Особенной части Уголовного кодекса.

Таким образом, в целях борьбы с уголовными правонарушениями в сфере информатизации и связи, а также в сфере Интернет вводятся законодательные акты, которые будут заслоном от совершения подобных уголовных правонарушений.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуется принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, разработка средств защиты информации, совершенствования нормативной правовой базы в данной сфере.

Так, в новом Уголовном кодексе от 3 июля 2014 года имеется непосредственная глава 7 «Уголовные правонарушения в сфере информатизации и связи», в которой имеется в наличии несколько «злодеяний» в этой сфере.

А именно следующие статьи:

- 205 УК РК «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций»;

- 206 УК РК «Неправомерные уничтожение или модификация информации»;

- 207 УК РК «Нарушение работы информационной системы или сетей»;

- 208 УК РК «Неправомерное завладение информацией»;

- 209 УК РК «Принуждение к передаче информации»;

- 210 УК РК «Создание, использование или распространение вредоносных»;

- 211 УК РК «Неправомерное распространение электронных информационных ресурсов ограниченного доступа»;

- 212 УК РК «Предоставление услуг для размещения Интернет-ресурсов, преследующих противоправные цели»;

- 213 УК РК «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства» [8, с. 1].

Современный мир характеризуется динамичными глобальными процессами и трансформацией системы международных отношений. В условиях интеграции и укрепления экономических и политических позиций государств совершенствуются механизмы многостороннего управления, в которых все большую роль играют информационные факторы.

Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств.

Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества.

Вместе с тем технологическая эволюция одновременно с позитивом порождает новые проблемы и угрозы информационной безопасности государств, усугубляя существующие. В обстановке глобальной конкуренции информационное давление становится действенным и эффективным методом решения межгосударственных конфликтов. Все интенсивнее используются возможности глобальных информационно-коммуникационных сетей экстремистскими и террористическими организациями для пропаганды и популяризации своей идеологии, распространения радикальных идей, вовлечения все большего числа единомышленников и их обучения, поддержания контактов и финансирования.

Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности. Организованные транснациональные преступные группы все активнее используют современные информационно-коммуникационные технологии в криминальных целях. Меняется динамика уголовных правонарушений в сфере информатизации и связи - для нее характерна устойчивая тенденция роста.

При этом, несмотря на увеличение зарегистрированных преступлений с использованием современных информационно-коммуникационных технологий, официальная статистика не отражает объективную картину распространения

киберпреступлений, показывая лишь незначительную часть реально совершенных.

Особенность киберпреступлений заключается в их высокой латентности, появлении новых, изощренных способов совершения преступлений, доказательство которых сильно затруднено из-за отсутствия необходимых правовых, организационных и технических инструментов. Поэтому борьба с киберпреступностью обусловливает потребность соответствующего оперативного реагирования, совместных скоординированных действий спецслужб и правоохранительных органов государств.

В этой связи вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью, остро стоит на повестке дня не только в Казахстане, но ряде других государств.

Правовыми нормативно-правовыми актами нашей страны в области защиты информации выступает Конституция Республики Казахстан от 30 августа 1995 г., в которой в ст. 18 Конституции закреплена обязанность государственных органов, общественных объединений, должностных лиц и средств массовой информации обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации.

В п.2 ст. 20 Конституции Республики Казахстан указывается, что каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом [13, с. 3].

В 20 веке в нашей стране появилась достаточно новая корпорация, которая следит за безопасностью в пространстве. Смысловое значение данной организации в том, что «среди преступлений против собственности, Интернет-хищения продолжают оставаться наиболее часто совершаемым преступлением.

Стоит отметить, как говорилось выше, согласно отчетам по правовой статистике за 2020 и 2021 гг. регистрация Интернет-хищений выглядит следующим образом: в 2020 году количество зарегистрированных преступлений составляет 33759, в 2021 году количество данных преступлений растет и составляет 41083» [6, с. 1].

Данная служба производит различные законные действия, которые на постоянной основе производят непосредственный анализ причин и условий угрозы в сфере Интернет, на основе чего выводя все данные в обособленный анализ по изучаемой тематике. Проводя такие действия на постоянной основе могут законно получать различные данные для совершенствования действующего законодательства для предупреждения «распространенности угрозы.

Отметим, что данная служба является определенным способом быстрого реагирования именно на жалобы граждан, с оговоркой именно непосредственно возникающих в сети Интернет [37, с. 134].

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с уголовными правонарушениями в сфере информатизации и связи. Помимо этого, необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с уголовными правонарушениями в сфере информатизации и связи [37, с. 1].

Для этого необходимо активизировать потребность международного сотрудничества. Но ввиду того, что в современных условиях значительная

часть средств борьбы с уголовными правонарушениями в сфере информатизации и связи, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт [38].

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, а также разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере. Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [39, с. 16].

К мерам предупреждения компьютерных преступлений также относится защита информации (данных). Защита информации (данных) представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Семь причин, которые указаны в юридической литературе:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи

данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) отсутствие контроля за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции, ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации, ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категоричности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации [40, с. 114].

Также к основным детерминантам киберпреступности следует отнести некачественные услуги и приложения, предоставляемые гражданам и частным организациям в рамках «электронного правительства», в том числе машиночитаемые открытые данные, могут привести к нарушению прав и законных интересов граждан.

Особое место в обеспечении информационной безопасности Республики Казахстан занимают различные программные документы и ряд концепций, в частности в информационной безопасности Республики Казахстан.

Концепция информационной безопасности Республики Казахстан» была принята указом Президента Республики Казахстан от 10 октября 2006 года № 199, вторая «Концепция информационной безопасности Республики Казахстан до 2016 года» была принята указом Президента Республики Казахстан от 14 ноября 2011 г. N 174, третья Концепция кибербезопасности «Киберщит Казахстана» утверждена постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407.

Концепции определяют государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности, и разработаны в соответствии с Конституцией Республики Казахстан и Законами Республики Казахстан.

В законодательстве об информационной безопасности можно выделить два векторных направления правовой защиты объектов в информационной сфере:

- защита чести, достоинства и деловой репутации

- защита информационной сферы».

Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества.

Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности.

ЗАКЛЮЧЕНИЕ

Противоправные общественно опасные деяния, совершенные с использованием сети Интернет именуются Интернет-преступностью. К Интернет-преступлениям могут быть отнесены некоторые составы преступлений, относящихся к киберпреступности, а также преступления, не относящиеся к киберпреступности, но совершаемые с помощью сети Интернет.

Большой рост Интернет-пространства среди нас, а также переход как юридических, так и экономических отношений в цифровое пространство «Интернета», таким образом, все правонарушения происходят в Интернете. Иными словами, происходит рост и зарождения новых видов деяний.

Необходимо отметить, что цифровизация – это положительное явление, однако, как и любое явление, цифровизация имеет как положительные, так и негативные моменты. Стоит ли говорить о том, что к негативным аспектам относится появление новых более универсальных видов правонарушений, характеризующиеся некоторыми особенностями, не свойственные другим видам правонарушений. Речь идёт о Интернет-мошенничестве и краже.

Большой рост Интернет-пространства среди нас, а также переход как юридических, так и экономических отношений в цифровое пространство «Интернета», таким образом, все правонарушения происходят в Интернете. Иными словами, происходит рост и зарождения новых видов деяний.

Необходимо отметить, что цифровизация – это положительное явление, однако, как и любое явление, цифровизация имеет как положительные, так и негативные моменты. Стоит ли говорить о том, что к негативным аспектам относится появление новых более универсальных видов правонарушений, характеризующиеся некоторыми особенностями, не свойственные другим видам правонарушений. Речь идёт о Интернет-мошенничестве и краже.

Согласно статистической отчетности за 12 месяцев 2020 года в Республике Казахстан было зарегистрировано всего 33 759 фактов мошенничества, из которых 14 220 приходится на Интернет-мошенничества [6, с. 13] (см. Диаграмма).

Таким образом, 48,1 % всей совокупности зарегистрированных мошенничеств составляет Интернет-мошенничество. В статистической отчетности ведется регистрация только по Интернет-мошенничествам, других видов правонарушений в сети Интернет нет.

Интернет-хищения достаточно распространены на территории нашего государства, происходит большой процент регистрации данных правонарушений.

Интернет-мошенничество и Интернет-хищения указаны в Уголовном кодексе Республики Казахстан, но это не отдельные виды составов, а лишь указаны в частях статей (188 и 190) [8].

Законодатель на момент принятия Уголовного кодекса 2014 года предусмотрел указанные пункты, но опять же отдельных составов ныне действующий кодекс не содержит. Стоит отметить, что введение новой статьи, регламентирующей совершение именно Интернет-хищения позволит более четко и в соответствии с санкцией статьи назначать реальное наказание правонарушителям [8].

Нынешнее время предполагает использование передовых технологий всеми гражданами нашей страны. Однако применение в жизни человека различных «ноу-хау» подразумевают как возникновение положительных и отрицательных аспектов. Положительной стороной является использование в жизни рядового гражданина различных средств связи, глобальной сети и т.д. В то же время такое использование может спровоцировать возникновение «плохих» мыслей у человека, переступивших черту закона. Здесь необходимо отдельно выделить тот факт, что, к сожалению «цифровая» жизнь человека

предполагает возникновение и распространение Интернет-преступности, здесь остановимся на хищениях в сети Интернет.

Интернет – это прежде всего, система связанных между собой компьютерных сетей, где главной целью является сохранение и трансляция информации. В литературе можно встретить такие понятия, как «Всемирная сеть», также «Глобальная сеть» или на так-называемом разговорном стиле «Всемирная паутина» [2].

О плюсах использования такой сети известно всем, однако о отрицательных сторонах использования такой сети мы подробно раскроем далее.

Использование цифровых технологий предоставляет ряд преимуществ, среди которых: форсирование обмена информацией, упрощение доступа населения к государственным и коммерческим услугам, появление новых возможностей и дальнейшее развитие и создание цифровых продуктов. Республика Казахстан выбрала активную позицию в вопросах использования электронно-информационных технологий, как в деятельности государственных органов, так и в иных сферах.

Интернет-хищения и Интернет-мошенничество являются схожими понятиями, но на наш взгляд, понятие «Интернет-хищения» шире, чем понятие «Интернет-мошенничество». Как правило, Интернет-мошенничество является одним из видов совершения «Интернет-хищения». Способом здесь будет являться именно злоупотребление доверием пользователя в сети Интернет, либо посредством данной сети.

Объектом указанных преступлений является имущество либо права на него, здесь необходимо отразить тот факт, что имущество может быть разным, но на наш взгляд, информация в сети Интернет не будет являться объектом преступлений против собственности [8].

Также важно отличать действительное имущество собственника от разного рода услуг, оказываемых собственнику в Интернет пространстве. Поэтому перед квалификацией деяния, следует выяснить действительно ли похищенное является имуществом. Например, некоторые пользовательские соглашения Интернет-ресурсов предусматривают, что регистрируемые пользователем аккаунты не являются имуществом последнего, а значит, не подпадают под объект Интернет-хищений.

Учитывая огромное множество Интернет сервисов, коими пользуются многие люди, напрашивается мысль о законодательном урегулировании оказываемых услуг, дабы иметь общий стандарт, который будет регулировать имущественные вопросы в данных сервисах.

Отсутствие общего стандарта создает потенциально серьезную проблему с правовым урегулированием имущества, находящегося в Интернете. Так, например, взлом электронной почты не будет квалифицироваться как покушение на кражу, так как сама электронная почта не является имуществом пользователя (согласно пользовательскому соглашению).

На основании изложенного, делаем вывод о том, что отечественное законодательство должно отражать реалии современного мира, предусматривать соответствующее наказание за появление новых и распространенных преступлений, а также отражать развитие цифровых технологий, так как действительность ведет к тому, что Интернет-хищения и другие уголовные правонарушения в Интернет пространстве будут количественно и качественно расти, что требует соответствующей реакции со стороны законодателя и правоохранительных органов. Поэтому можно ещё раз подчеркнуть важность отдельного урегулирования Интернет-хищений, так как правильное и удобное законодательное регламентирование позволит точнее и эффективнее бороться с нарастающей угрозой «хищений» [15].

Проведя диссертационное исследование, посвященное вопросам Интернет-хищения чужого имущества, автор пришел к следующим выводам:

На сегодняшний день уголовное законодательство прошло определенные этапы, среди которых внесение изменений касательно введения новых составов уголовных правонарушений.

Интернет-хищения чужого имущества граждан являются в последнее время достаточно распространенным уголовным правонарушением, несет в себе большую общественную опасность.

В настоящей работе сделан акцент именно на освещение уголовно-правовых и криминологических аспектов Интернет-хищений чужого имущества, перечислены виды Интернет-хищений.

До последнего времени в теории и практике нет однозначного понятия «Интернет-хищения», также не введены отдельные составы относительно «новых видов преступлений как Интернет-хищения».

С учетом сказанного, предлагается внести поправки в Уголовный кодекс Республики Казахстан 2014 года в раздел 6. «Уголовные правонарушения против собственности», ввести ст. 188-2 со следующей редакцией:

188-2. Интернет-хищение чужого имущества

1. Интернет-хищение, то есть кража, мошенничество, присвоение или растрата чужого имущества,

Наказывается...

2. Интернет-хищение, совершенное:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения, -

наказывается …

3. Интернет-хищение, совершенное:

1) в крупном размере;

2) неоднократно, -

Наказывается …

4. Интернет-хищение, совершенное:

1) преступной группой;

2) в особо крупном размере, -

Наказывается…

В связи с предложенными изменениями и дополнениями, из Уголовного кодекса Республики Казахстан исключить: «п. 4 ч. 2 из ст. 188» и «п. 4 ч. 2 из ст. 190», так как данные пункты будут предусмотрены в диспозиции ст. 188-2 Уголовного кодекса Республики Казахстан.

В настоящее время наблюдается рост интернет хищений на всей территории страны, в этой связи, в областях происходит нехватка сотрудников подразделения «К» МВД РК. Поскольку имеющаяся штатная численность сотрудников данного подразделения не рассчитана на такое большое количество регистрируемых дел. В связи чем, необходимо в выделить дополнительные штатные единицы сотрудников для более эффективной борьбы с интернет хищениями.

Также необходимо учитывать, что деятельность подразделения «К» МВД РК тесно связана с IT специалистами, нехватка которых остро сказывается на кибербезопасности граждан и государства, поскольку высококвалифицированные IT специалисты имеют возможность большего заработка в частном секторе, а также лучшие условия труда, чем могут предоставить в правоохранительных органах. Что существенно влияет на привлечение в качестве сотрудников правоохранительных органов.

В целях решения данной проблемы выделить увеличенную сетку оплаты труда для данной категории лиц и предоставлением необходимых условий труда.

Данные предложения позволят разграничить ответственность за совершение преступлений в сфере Интернет.

При этом сеть Интернет является неотъемлемым инструментов в жизни каждого человека. И с другой стороны, распространение сети Интернет позволяет людям с «маргинальным поведение» совершать преступления.

Тем самым автор сделал попытку законодательно урегулировать «новый вид преступления – Интернет-хищения чужого имущества». И соответственно наличие указанных выше составов позволит назначать соответствующее наказание с указанием всех квалифицирующих признаков.

Внести изменения и дополнения Нормативное постановление Верховного суда от 11 июля 2003 года № 8 «О судебной практике по делам о хищениях», где в целях правильного и единообразного применения в судебной практике действующего законодательства при квалификации уголовных правонарушений, связанных с посягательством на чужую собственность указать понятие «Интернет-хищение», способы и виды.

В связи с чем, в Нормативное постановление Верховного суда от 11 июля 2003 года № 8 «О судебной практике по делам о хищениях» добавить пункт 1-1 который изложить в следующей редакции: «Если хищение совершено в сети интернет, то его следует квалифицировать как Интернет-хищение».

Рекомендации Интернет-пользователям могут состоять в следующем:

«необходимо внимательно следить за обложкой ресурса, на который непосредственно переходите по набранной ссылке, стоит внимательно отнестись к передаче данных, так как введенная единожды информация на ресурсе, оставляет следы в виде фамилии, имени, отчестве, а также указания номера банковской карты».

В качестве рекомендации стоит отразить о должном и внимательном обращении на Интернет-площадке, так как Глобальная сеть несет в себе различные риски, у многих людей вся информация хранится на носителях, в том числе мобильных телефонах, цифровых источниках и тд. [27].

Рекомендации Интернет-пользователям могут состоять в следующем:

«нужно осознавать – ценовая политика остается одинаковой, не стоит сразу же реагировать и оплачивать за тот товар, который имеет стоимость ниже рыночной».

«также потенциальными покупателями стоит задуматься относительно местоположения ресурса, то есть выходные данные о непосредственном расположении: адрес, название и тд.

Основные непосредственно запретные функции, которые не нужно использовать в сети Интернет:

– не приводить ввод своих данных, не переходить по различным интернет-источникам;

– нельзя вести переписку с различными людьми, в том числе и детям;

– не приобретать сомнительный товар через ресурсы;

– категорически запрещено производить оплату своим знакомым, которые «якобы просят деньги в долг и тд». Стоит убедиться в просьбе лично либо очно [28].

Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества.

Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности.

Таким образом, в целях борьбы с уголовными правонарушениями в сфере информатизации и связи, а также в сфере Интернет вводятся законодательные акты, которые будут заслоном от совершения подобных уголовных правонарушений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. «Об утверждении Концепции развития государственного управления в Республике Казахстан до 2030 года», утверждена Указом Президента Республики Казахстан от 26 февраля 2021 года № 522 // режим доступа: https://adilet.zan.kz/rus/docs/U2100000522

2. Семь причин возникновения киберопасности в Казахстане // режим дсотупа: 1. https://mail.kz/ru/news/kz-news/sem-prichin-vozniknoveniya-kiberopasnosti-v-kazahstane

3. Средняя плотность населения стран мира: таблица и рейтинг 2020-2021 годов // 1. http://visar.by/viza/crednyaya-plotnost-naseleniya-stran-mira-tablitsa-i-rejting-2020-2021-godov.html

4. Рост преступности, причины, пути и способы снижения // https://cyberpedia.su/17x73fe.html

5. Латентность преступлений и ее виды // http://miassats.ru/782/

6. Информационный сервис Комитета правовой статистики и специальным учетам Генеральной прокуратуры Республики Казахстан «О состоянии преступности в Республике Казахстан за III квартал 2020 года» // 1. https://online.zakon.kz/Document/?doc_id=34881745

7. Дремлюга Г.И. Интернет-преступность: монография. // http://window.edu.ru/catalog/pdf2txt/015/63015/33158?p_page=2

8. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V (с изменениями и дополнениями на 01.01.2022 г.) // https: //online.zakon.kz/

9. Борчашвили И.Ш. Хищение чужого имущества // 1. https://library.tou.edu.kz/fulltext/transactions/3847_borchashvili_i._sh_hishenie_chujogo_imushestva.pdf

10.Формы и средства мошеннического обмана // https://vuzlit.com/1325590/formy_sredstva_moshennicheskogo_obmana

11. Программы-вымогатели «ransomware» // https://www.youtube.com/watch?v=isRgoOLI5QM

12. Мошенничество в современном мире 2022 // 1. https://gkh-expert.ru/trudovoe-pravo/moshennichestvo-v-sovremennom-mire-2019

13. Правовое регулирование мошенничества в уголовном законодательстве Российской Федерации //https://pravo.bobrodobro.ru/126753

14. Галактионов Е.А. «Уголовно - правовые средства борьбы с организованной преступностью». Издательство «Наука», г. Москва. 1993 г.

15. Казахстан и Всеобщая декларация прав человека // 1. https://rus.azattyq.org/a/kazakhstan-vypolnenie-deklaratsii-prav-cheloveka-v-kazakhstane/29646432.html

16. Конституция Республики Казахстан принята на республиканском референдуме 30 августа 1995 года (с изменениями и дополнениями по состоянию на 23.03.2019 г.) // https://online.zakon.kz/m/document/?doc_id=1005029

17. Детерминанты (причины и условия) преступности // режим доступа: http://knowledge.albest.ru

18. Криминологический журнал «Предупреждение преступности» Криминологической ассоциации РК. № 2 от 2001 г., г. Алматы. 2001 г.

19. Методические рекомендации по предупреждению, раскрытия Интернет-мошенничеств. Карагандинская академия МВД Республики Казахстан им. Б.Бейсенова. - Караганда. 2021. – 70 с.

20. Русаков И. М. Актуальные вопросы допроса свидетеля по делам о мошенничестве в сфере предоставления услуг Интернет.: IV Международной научно-практической конференции. Краснодарский университет МВД России. 2016. С. 372-376.

21. Кучуков К.М. // Расследование мошеннических действий // Учебно-практическое пособие.- Алматы, 1999.
22. Борчашвили И.Ш., Мукашев А.К. // Преступление против собственности // Монография. – Астана: Институт законодательства, 2009. – 568с.
23. Петрухин И.Л. Уголовный процесс зарубежных государств. М. 1996;
24. Божьев В.П. Уголовно-процессуальное законодательство и его развитие. М., 1993.
25. Зуйнов Г. Поиск преступника по признакам способом совершения преступления. МВД СССР, М.-1970 г.
26. Жаклин Ф. // Органы юстиции завалены делами о преступлениях в Интернете // http: // www. inosmi. ru / 2019/02/20. - С. 1.
27. Безверхов А.Г. Имущественные преступления. - Самара: Изд-во «Самарский университет», 2002. - С. 106
28. Горшков А.Ф. Девиков Е.И. Опыт разработки информационно-логической поисковой системы по способу совершения преступления. Экспертиза при расследовании преступлений.
29. Галактионов Е.А. «Уголовно - правовые средства борьбы с организованной преступностью». Издательство «Наука», г.Москва. 1993г.
30. Кудрявцев В.Н. «Объективная сторона преступления». Издательство «Пресса», г. Москва. 1986 г.
31. Божьев В.П. Уголовно-процессуальное законодательство и его развитие. М., 1993;
32. Каиржанов Е. Криминология. Общая часть. — Алматы: Республиканский издательский кабинет, 1995. — С. 108.
33. Волохова О.В.// Современные способы совершения мошенничества: особенности выявления и расследования. – М.: Юрист, 2008.
34. Уголовное право РК. Под редакцией Поленова. А., 1998
35. Фойницкий И.Я. Курс уголовного судопроизводства. СПб.,1996. с. 51;

36. Васнецов А. Квалифицирующее значение объекта преступлений против собственности. РЮ, 1994 г.
37. Уголовное право Республики Казахстан. Особенная часть. Учебное пособие. В 2-х т. под ред. Борчашвили И.Ш. и Оразалиева М.М. Караганда: КарЮИ МВД РК им. Б. Бейсенова.
38. Уголовное право России. Особенная часть // 1. https://books.google.kz/books?id=ifC4AAAAQBAJ&pg=PT154&lpg=PT154&dq=
39. Зайцев О.А., Мишина И.М.–Расследование мошенничества, совершенного с использованием банковских карт (криминалистические и уголовно-процессуальные аспекты): Монография.–М.:» Московская академия экономики и права», 2009.– 188 с.
40. Комментарий к уголовному кодексу Республики Казахстан. Учебное пособие. Борчашвили И.Ш. - Алматы «Жеті Жарғы», 2015.

Приложение 1

Акт внедрения

Приложение 2

Сравнительная таблица

Приложение 2

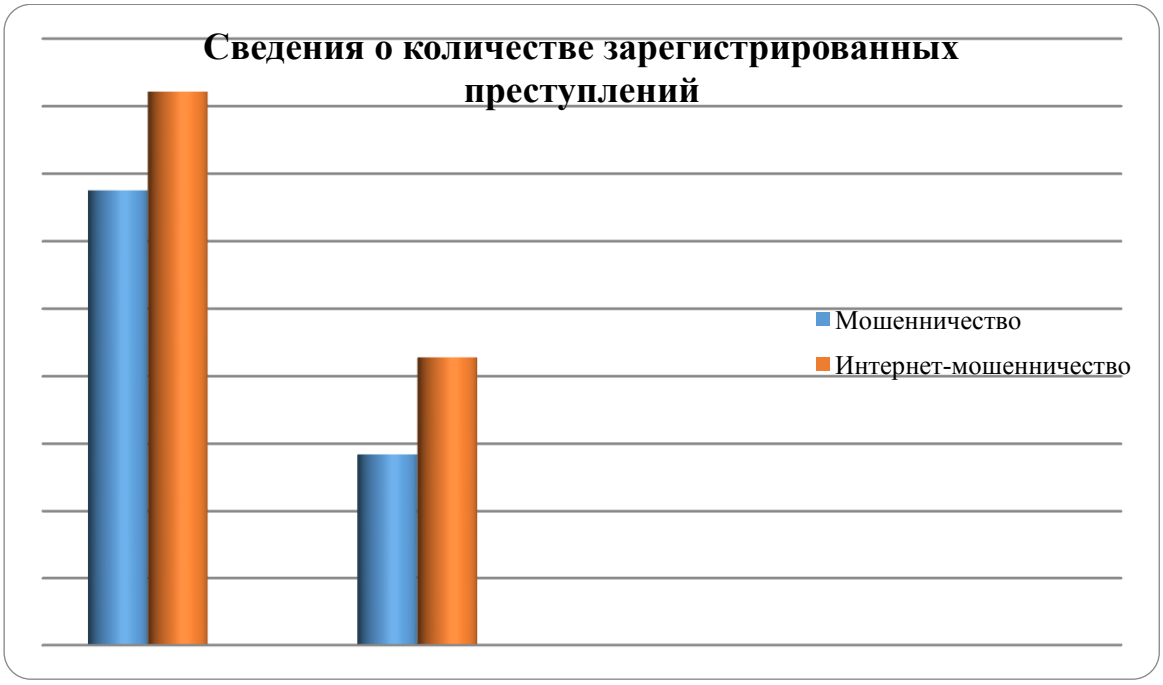
Сравнительная таблица 2 стр.

Приложение 3

Таблица. Количество зарегистрированных преступлений за 2020 и 2021 гг.

Количество зарегистрированных преступлений	Годы	
	2020	2021
Мошенничество	33759	41083
Интернет-мошенничество	14220	21405

Диаграмма. Количество зарегистрированных преступлений за 2020 и 2021 гг.



Приложение 4

ОПРОСНЫЙ ЛИСТ

Уважаемый коллега!

Настоящее анкетирование проводится в рамках диссертационного исследования «Интернет-хищения чужого имущества: уголовно-правовые и криминологические аспекты». Полученная информация будет использоваться исключительно в научных целях.

Просим Вас выделить (подчеркнуть, округлить и т.п.) те ответы, с которыми согласны, и указать персональное мнение в определенных местах. Заранее благодарим Вас за сотрудничество!

1. Какие виды Интернет-преступлений чаще всего находятся в Вашем производстве?

а) мошенничество в сети Интернет

б) неправомерный доступ к информации

в) иные виды

2. Кто чаще всего становится жертвой Интернет-хищений?

а) мужчина

б) женщина

в) несовершеннолетние

3. Каким способом чаще всего происходит хищение в сети Интернет?

а) путем кражи

б) путем мошенничества

в) другое

4. Как Вы считаете, есть ли необходимость введения новой статьи в действующий Уголовный кодекс РК 2014 г. относительно Интернет-хищений

а) да, я считаю,это будет правильным и верным решением

б) да, в таком случае ответственность за данные виды преступлений будет разграничена

в) нет

г) другое

5. Какими способами чаще всего происходят хищения в Интернете?

а) путем списания денежных средств

б) путем звонка с неизвестного номера

в) путем предоставления личной информации преступнику

г) другое

6. Как сразу жертвы обнаруживают, что произошло преступление?

а) практически сразу

б) в течение суток

в) другое

7. По Вашему мнению, число жертв такого рода преступлений увеличивается?

а) да

б) нет

в) другое

8. Каким образом, по Вашему мнению, можно предотвратить Интернет-преступления?

а) путем профилактических методов

б) путем реализации различных программ

в) другое

9. Какова раскрываемость Интернет-хищений в РК?

а) низкая раскрываемость

б) раскрывается небольшой процент от общего числа преступлений

в) раскрываются на должном уровне

Приложение 5

РАСПРЕДЕЛЕНИЕ ОТВЕТОВ РЕСПОНДЕНТОВ НА ВОПРОСЫ АНКЕТЫ

Вопрос анкеты	Количество респондентов
1	2
Какие виды Интернет-преступлений чаще всего находятся в Вавшем производстве?	33 (100%)
мошенничество в сети Интернет	25 (75,8%
неправомерный доступ к информации	2 (6%)
иные виды	6 (18,2%)
Кто чаще всего становится жертвой Интернет-хищений?	33 (100%)
Мужчина	5 (15,2%)
Женщина	25 (75,8%)
несовершеннолетние	3 (9,1%)
Каким способом чаще всего происходит хищение в сети Интернет?	33 (100%)
а) путем кражи	2 (6,1%)

б) путем мошенничества	29 (87,9%)
в) другое	2 (6,1%)
Как Вы считаете, есть ли необходимость введения новой статьи в действующий Уголовный кодекс РК 2014 г. относительно Интернет-хищений?	33 (100%)
да, я считаю это будет правильным и верным решением	14 (42,4%)
да, в таком случае ответственность за данные виды преступлений будет разграничена	10 (30,3%)
Нет	8 (24,2%)
Другое	1 (3,1%)
Какими способами чаще всего происходят хищения в Интернете?	33 (100%)
путем списания денежных средств	7 (21,2%)
путем звонка с неизвестного номера	7 (21,2%)
путем предоставления личной информации преступнику	19 (57,6%)
Как сразу жертвы обнаруживают, что произошло преступление?	33 (100%)

практически сразу	12 (36,4%)
в течении суток	20(60,6%)
Другое	1 (3%)
По Вашему мнению, число жертв такого рода преступлений увеличивается?	33 (100%)
Да	32 (97%)
Нет	1 (3%)
Другое	0 (0%)
Каким образом, по Вашему мнению, можно предотвратить Интернет-преступления?	33 (100%)
путем профилактических методов	17 (51,5%)
путем реализации различных программ	16 (48,5%)
Другое	0 (0%)
Какова раскрываемость Интернет-хищений в РК?	33 (100%)
низкая раскрываемость	23 (69,7%)
раскрывается небольшой процент от общего числа преступлений	10 (30,3%)
раскрываются на должном уровне	0 (0%)