Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра оперативно–разыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «Тактика ОРД по раскрытию мошенничеств, связанных с использованием компьютерных и информационных технологий»

Выполнил: СеребренниковНиколай Петрович
(фамилия, имя, отчество)
Правоохранительная деятельность,
2015 года набора, 051 учебная группа
(специальность,год набора, №группы)

Руководитель:
к.ю.н., доцент,доцент кафедры ОРД КЮИ МВД России
(ученая степень,ученое звание, должность)
Музеев Айдар Иршатович
(фамилия, имя, отчество)

Рецензент:
НачальникОУР УМВДРоссиипо г.Ижевску, майор полиции
(должность, специальное звание)
Брыляков Вячеслав Николаевич
(фамилия, имя, отчество)

Дата защиты: «___» _____2020г. Оценка _____

Казань 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время важным фактором общественного устройства определились как, отношения собственности, которые в связи с этим требуют повышенной охраны, поскольку продолжается рост преступных посягательств на этот объект. Среди способов хищений по размерам причиненного ущерба личности, обществу и государству во всем мире, мошенничество заняло лидирующие позиции.

Уровень преступлений данного вида возрастает с каждым годом, защита собственности, по критерию возмещения причиненного ущерба, не улучшается. Более того, наметилась тенденция к профессионализации данного вида преступности с образованием преступных организации, в том числе международных и вовлечением в их деятельность все большего числа лиц.

Актуальность темы исследования. Как известно, мошенничество возникло с момента основания российского государства. Мошенничество зародилось в отношениях товарообмена, где злоумышленник мог рассчитывать на максимальное извлечение выгоды для себя. Технический прогресс, революции, научные открытия, изобретения, которые мы используем в повседневной жизни, все это вывело нас в век высоких технологий. В работе отражаются новые, технически и организационно сложные преступления – хищение денежных средств, совершенные с использованием платежных карт, а также с помощью специализированных вредоносных компьютерных программ, массово распространяемых в сети Интернет. Конечно же законодатель старался реагировать на новые явления и предпринимать меры, направленные на борьбу с подобными деяниями. В настоящее время такие преступления квалифицируются как мошенничество в сфере компьютерной информации, предусмотренное в сфере компьютерной информации, предусмотренное ст.

159.6 УК РФ, введенной в действие Федеральным законом от 29 ноября 2012 г. № 207 – ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

На сегодняшний день актуальность противодействия настоящему деянию нисколько не уменьшалась, а наоборот, только увеличилась. Это преступление в настоящее время отличается исключительным многообразием, адаптивностью, динамизмом и способностью к модернизации в зависимости от сферы проникновения. Быстрые темпы развития экономики государства, развитие института собственности, увеличение количества договорных отношений, конечно же, не оставили мошенников равнодушными. Широкое распространение настоящее деяние получило ввиду подверженности нашей жизни технизации. Человеческое общение приобретает новые формы, которые все больше внедряют в свою деятельность компьютеры, компьютерные технологии, а так же обогащаются в интеллектуальном отношении, значительную роль играют информационные технологии, особенно в сфере бизнеса и финансов. Если раньше злоумышленнику необходимо было осуществлять все свои мошеннические замыслы «вручную», что требовало значительного времени, то в настоящее время для достижения аналогичного результата достаточно потратить лишь несколько часов благодаря информационным технологиям.

По официальным данным ГИАЦ МВД России за 2019[1] г. было зарегистрировано 294409 преступлений из них раскрыто 65238 преступлений, совершенных с использованием информационно – телекоммуникационных технологий, это на 68,5% больше, чем за 2018 г. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8% в январе – декабре 2019 года до 14,5%.

[1] ФКУ «Главный информационно – аналитический центр» Состояние преступности в России за январь-декабрь 2019г.

В результате совершения мошеннических действий ущерб претерпевают не только частные лица, но также и экономика Российской Федерации в целом. При этом, несмотря на официальные данные ГИАЦ МВД России, присутствует высокий уровень латентности данного деяния. Подобный уровень латентности обусловлен скрытым характером самого деяния. Субъект мошеннических действий – это не бродяга, не алкоголик, не безработный, все чаще это жизненно подкованный, образованный человек, нередко к тому же обладающий должностными или властными полномочиями. Изменение социального положения субъекта мошенничества предопределяет тот факт, что на данном этапе это деяние совершается с куда большим размахом, чем это было, например, в прошлых веках.

Изложенные обстоятельства вызывают необходимость в более качественном конструировании норм, предусматривающих ответственность за мошенничество. Вместе с тем, обстоятельства действительности диктуют необходимость развития уголовного законодательства в части противодействия мошенничеству. Диспозиция ст. 159 Уголовного Кодекса Российской Федерации[2] (далее УК РФ) предусматривает определение мошенничества, которое сформировалось еще с советских времен, однако изменение социально– экономической обстановки в стране требует переосмысления данного деяния, чтобы учитывались отношения, которые ранее не существовали.

Таким образом, очевидно, что государство постепенно уступает инициативу в пользу криминальных сообществ и индивидуально действующих лиц, не признающих каких – либо ограничений в сфере компьютерной информации. Так как, сеть Интернет, компьютерные и высокие технологии выходят на первое место в управлении государством и обществом.

---

[2] Уголовный кодекс Российской Федерации: федеральный закон РФ от 13 июня 1996 г. № 63-ФЗ (в ред. федерального закона от 1 апреля 2020 г. №73-ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL: http://www.consultant.ru

Объект и предмет исследования. Объектом исследования – являются общественные отношения, возникающие в связи с совершением преступлений в сфере высоких технологий.

Предметом исследования – выступают нормы уголовного законодательства Российской Федерации об ответственности за мошенничество, материалы статистики, следственно – судебной практики, а также специальная литература, отражающая вопросы обеспечения безопасности компьютерной информации.

Цели и задачи исследования. Цель изучения состоит в комплексном исследовании особенностей раскрытия преступлений в сфере использования компьютерных и информационных технологий.

Обозначенная цель предопределила формулировку и необходимость решения следующих **задач:**

1. Изучить уголовно– правовую характеристику мошенничеству в сфере компьютерной информации.
2. Изучить уголовно– правовую характеристику специальных видов мошенничества связанных с использованием компьютерных и информационных систем.
3. Раскрыть понятие компьютерной информации как объекта исследования.
4. Изучить механизм раскрытия преступлений, совершаемых в сфере высоких технологий.
5. Рассмотреть особенности взаимодействия сотрудников правоохранительных органов по проведению оперативно – технических мероприятий.

Методологическая основа исследования. Для достижения обозначенной цели и решения указанных задач в исследовании использовались положения всеобщего метода материалистической диалектики, диалектического и исторического методов познания. Достоверность и всесторонность исследования основывалась как на общенаучных, так и на частно – научных методах познания. Среди общенаучных методов наиболее

часто использовались сравнение, обобщение, формализация, анализ, дедукция, индукция, синтез. Из числа частно – научных методов познания применялись формально – юридические, лингвистические, логические, сравнительно – правовые, статистические и эмпирические методы познания.

Практическая значимость исследования состоит в возможности использования результатов при совершенствовании Уголовного кодекса РФ в части регламентации ответственности за мошенничество в сфере компьютерной информации; отдельные выводы могут быть использованы в разъяснениях постановлений Пленума Верховного Суда РФ; выводы о правилах квалификации отдельных видов мошенничества могут быть использованы в судебно – следственной практике по данным преступлениям. Что в свою очередь, поможет способствовать раскрытию такого рода преступлений.

Теоретическую основу исследования составляют труды отечественных ученых в области общей теории права, гражданского права, уголовного права, криминологии, экономики. Основными источниками информации являются монографии, диссертации, научные статьи и другие опубликованные материалы, отражающие те или иные стороны объекта исследования.

Нормативную базу исследования составляют Конституция РФ, уголовное законодательство РФ; нормативные правовые акты иных отраслей права, касающиеся рассматриваемой проблематики.

Структура ВКР. Выпускная квалификационная работа состоит из введения, двух глав, заключения и списка использованных источников.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА СВЯЗАННОГО С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

§1. Современная оперативная обстановка по линии преступлений, связанных с использованием компьютерных и информационных технологий

В современном российском обществе сеть Интернет является важнейшим фактором в сфере коммуникаций. С их помощью каждый день осуществляются различные операции с денежными средствами (с использованием компьютеров, банкоматов, иных платежных систем), осуществляются покупки различных товаров и услуг. Все вышеперечисленные действия напрямую зависят от различных информационных технологий, в результате чего ряд пользователей ежедневно подвергаются атакам со стороны злоумышленников.

В Главе 28 Уголовного кодекса Российской Федерации (далее УК РФ) предусматривает ответственность за преступления в сфере компьютерной информации. Киберпреступность является самым распространенным видом преступления, потому что действия преступников осуществляются через сеть Интернет, а он в свою очередь помогает анонимно, эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, порождать новые, неизвестные мировому сообществу виды общественно опасных преступлений[3].

Под киберпреступностью следует понимать, совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных

[3]Хохлова О.М. Общественное согласие в социально-политической сфере современного общества: монография. – Красноярск: Сиб. федер. ун-т, 2016. – 5с.

систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных.

Основными преступными деяниями, образующими рынок киберпреступности, являются:

1) Мошенничество в системах интернет – банкинга;
2) Фишинг;
3) Хищение электронных денег;
4) Услуги обналичивания иных нелегальных доходов;
5) Спам (информация о медикаментах и различной контрафактной продукции, поддельном программном обеспечении, сфере услуг, образования, туризма, страхования, кредитования);
6) Продажа трафика;
7) Продажа эксплойтов;
8) Продажа загрузок;
9) Анонимизация;
10) DDoS – атаки.

По официальным данным МВД РФ в 2019 г. преступлений, совершенных с использованием информационно – телекоммуникационных технологий, где присутствует прирост раскрываемости в таких субъектах:

Таблица №1.

Раскрываемость преступлений, совершенных с использованием информационно – телекоммуникационных технологий.

Субъект РФ	Раскрываемость,%
Республика Дагестан	57,4
Чукотский АО	48,2
Республика Ингушетия	47,5
Оренбургская область	44,2
Карачаево – Черкесская Республика	42,5

Чеченская Республика	42,1
Республика Саха (Якутия)	40,6
Московская область	39,5
Псковская область	38,6
Астраханская область	37,3

Также присутствует и отрицательная тенденция, т.к. уменьшается количество расследованных преступлений в таких регионах:

Таблица №2.

Регионы с наименьшей раскрываемостью.

Субъект РФ	Раскрываемость,%
Республика Башкортостан	17,0
Воронежская область	16,9
Калужская область	16,6
Ярославская область	15,8
Орловская область	15,2
Тверская область	15,0
Ставропольский край	14,8
Краснодарский край	14,6
г.Москва	13,8
Ленинградская область	12,8

Борьба государства с киберпреступностью, отражена в нормативно – правовых актах, где четко отражено взаимодействие правоохранительных органов с преступлениями связанными с компьютерными технологиями.

Например, нормативные акты МВД России отражают тенденцию отождествления преступлений, совершаемых в сфере высоких технологий, с преступлениями, совершенными с использованием информационно–телекоммуникационных сетей, включая сеть Интернет и компьютеров. «Инструкция по организации информационного обеспечения сотрудничества

по линии Интерпола» в разделе «Информационное обеспечение борьбы с преступлениями в области высоких технологий» (приказ МВД России № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 06.10.2006 г. (ред. от 22.09.2009 г.) предусмотрено, что взаимодействующие правоохранительные органы в процессе расследования преступлений направляют запросы о преступлениях в области высоких технологий, имеющих международный характер, связанных с: неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных программ, нарушением правил эксплуатации компьютерной техники , систем компьютера и их сети.

Так, исходя из статистических данных, в соответствии с рисунком 1., представленных из ГИАЦ МВД России за 2019 год, структура российской компьютерной преступности выглядит следующим образом:

1. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием платежных карт (ст. 159.3 УК РФ),

2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ),

3. Нарушение авторских прав и смежных прав, совершенное с использованием компьютерной и телекоммуникационных технологий (ст. 146 УК РФ),

4. Создание, использование и распространение вредоносных компьютерных программ (ст.273 УК РФ),

5. Кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ),

6. Незаконное изготовление и оборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ),

7. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с

использование компьютерных и телекоммуникационных технологий (242.1 УК РФ),

8. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершенные с использованием компьютерных и телекоммуникационных технологий (ст.183 УК РФ),

9. Незаконный оборот специальных технических средств, предназначенный для негласного получения информации (ст.138.1 УК РФ),

10. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов, совершенное посредством компьютерных и телекоммуникационных технологий (ст.242.2 УК РФ),

11. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч.1 ст.138 УК РФ),

12. Причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 165УК РФ),

13. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно – телекоммуникационных сетей (ст.274 УК РФ)

14. Незаконное организация и проведение азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 171.2 УК РФ).

Что касается источников киберпреступлений, то специалисты подразделяют лиц, осуществляющих атаки, на несколько категорий[4]:

1. Хакеры – лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций.

---

[4]Яблоков Н. П. Криминалистика: учебник. – М.: ЛексЭст, 2006; Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы.

Лица, имеющие высокий уровень знаний в области компьютерных технологий, которые проводят много времени за компьютером в поисках уязвимости компьютерных систем.

2. Хактивисты. Термин «хактивизм» введен впервые специалистом по компьютерной преступность Д. Деннинг. Он возник из соединения двух слов «hack» и «activism» и используется для обозначения явления социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего – либо, и хакерства (использования Интернет – технологий с целью причинения ущерба компьютерным сетям и их пользователям).

3. Киберпреступники, «корыстные преступники» – лица, вторгающиеся в информационные системы для получения личных имущественных или не имущественных выгод.

4. Лица, занимающиеся шпионажем, «шпионы» – лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях.

5. Террористы – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия.

6. Вандалы – лица, взламывающие информационные системы для их разрушения.

7. Психически больные лица, страдающие новым видом психичеких заболеваний – информационными болезнями или компьютерными фобиями.

По проведенным исследованиям, выделяют характерные черты киберпреступников: большая часть преступников – мужчины в возрасте от 16 до 48 лет. Цели имеют различия в зависимости от возраста и социального положения. Если среди молодежи распространены преступления, связанные с нарушением лицензионных соглашений, различных онлайн – проектов (в частности, игр) и мелкие мошенничества, то среди более взрослого поколения такие преступления, как вмешательства в данные, незаконный перехват и т.д. В

настоящее время достижения, полученные в изучении психологии киберпреступников, уже активно применяются в других странах при расследовании преступлений, в основном, при определении типа преступников.

Таким образом, необходимоучитывать, такой фактор как низкий уровень защиты информации в сети Интернет, незащищенные базы данных с персональными данными пользователей, с которыми может ознакомиться большое количество преступников в свою пользу для совершения преступления. При расследовании преступлений в сфере высоких технологий присутствует такой фактор, как недостаточный уровень квалификации правоохранительных органов, это в значительной степени влияет на низкую раскрываемость преступлений, а также безнаказанность злоумышленников. Данную тенденцию необходимо учитывать в крупных, развивающихся городах для эффективного повышения предупреждения и расследования такого рода преступлений. Так, предупредительные меры способны обеспечить необходимый эффект на практике лишь в тех случаях, когда осуществляется взаимодействие государственных органов с институтами гражданского общества, включая общественные объединения, органы местного самоуправления, средства массовой коммуникации, образовательные и научные организации на основе осуществления планирования, программирования своей совместной деятельности, учитывая специфику деятельности каждого заинтересованного субъекта профилактики преступной деятельности.

§2. Виды мошенничества, совершаемых с использованием компьютерных и информационных технологий и их уголовно– правовая характеристика

Важное значение в деятельности по раскрытию преступлений оперативными подразделениями органов внутренних дел имеет сыскная квалификация преступления, проводимая еще до принятия процессуального решения о возбуждении уголовного дела. Обладая начальными признаками отклоняющего поведения в глобальной сети, оперативный сотрудник должен иметь четкое представление о квалифицирующих признаках, образующих состав преступления.

Законодательная формулировка мошенничества, закрепленная в диспозиции ст. 159 УК РФ гласит, что под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Разъяснение дается в постановлении Пленума Верховного Суда от 27.12.2007 № 51, которое позволяет выделить следующие характерные черты объективной стороны мошенничества:

1) в соответствии с диспозицией ст. 159 УК РФ мошенничество является одной из форм хищения, следовательно, характеристика признаков объективной стороны этих деяний совпадает.

2) мошенничество может быть совершено путем приобретения права на чужое имущество, что является самостоятельной формой преступления;

3) ненасильственные способы исполнения объективной стороны, результатом которых становится добровольная передача имущества или права на него виновному или же потерпевший не препятствует изъятию имущества или приобретению права на него.

Анализ примечания к ст. 159 УК РФ позволяет заключить, что состав хищения сконструирован как материальный и предполагает совершение

определенных общественно– опасных действий, запрещенных УК РФ, выраженных в противоправном безвозмездном изъятии, обращении чужого имущества, в результате которых наступают негативные последствия, связанные с нанесением ущерба собственнику или иному владельцу этого имущества. Конечно же требуется наличие причинно– следственной связи между этими действиями и последствиями.

Характеристика противоправности хищения лишний раз подчеркивает общественную опасность данного деяния. Виновный стремится приобрести правомочия собственника или иного законного владельца в нарушение установленного порядка положений гл. 14 – 15 ГК РФ[5]. Законодателем в очередной раз акцентируется, что в результате таких действий виновный не становится собственником. Поэтому используется формулировка «в пользу виновного или иных лиц».

Таким образом, в Уголовном Кодексе выделяют мошенничества в сфере высоких технологий как отдельный состав преступления против собственности и квалифицированного вида мошенничества в экономической сфере, а также уголовно– правовой анализ состава данного преступления.

В ст. 159.3. УК РФ основания наступления уголовной ответственности за мошенничество при использовании электронных средств платежа. В соответствии с положениями статьи 8 Общей части УК РФ, основанием для наступления уголовной ответственности за мошенничество с использованием платежных карт является совершение виновным лицом деяния, содержащего все признаки состава преступления, предусмотренного статьей 159.3 Уголовного кодекса.

Объект в ст. 159. 3 УК РФ полностью совпадает с родовым объектом хищения – это общественные отношения, сложившиеся в сфере социального обеспечения населения. Как и мошенничество вообще, квалифицированное

[5]Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (в ред. от 27.12.2019 г. №489-ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

мошенничество с использованием платежных карт – всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Объективная сторона в ст. 159.3 –хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем обмана уполномоченного работника кредитной, торговой или иной организации. Также объективная сторона предполагает хищение чужого имущества, которое предопределено или обусловлено использованием платежной карты, которая подпадает под признаки состава. Перед использованием банковской карты виновное лицо может осуществлять ряд первоначальных действий, к которым относятся изготовление, приобретение, хранение, транспортировка поддельных платежных карт. Если при наличии этих действий преступный умысел, направленный на совершение мошеннических действий с использованием платежных карт не был доведен до конца, по независящим от лица обстоятельствам, то содеянное необходимо квалифицировать по совокупности преступлений, предусмотренных ст. 187 УК РФ и ч. 3 ст. 30 соответствующей части ст. 159.3 УК РФ.

Для наглядности рассматриваемых действий приведем пример из судебной практики.

Так, приговором И– ого районного суда г. П от 07.02.2018 по делу 1–35/2018, в котором гражданку Ч., признали виновной в совершении преступлений предусмотренных, ч. 1 ст. 158, ч. 1 ст. 159.3 УК РФ. Гражданка Ч., похитила у своего знакомого банковскую карту, которую в дальнейшем использовала по своему усмотрению. Так гражданка Ч., попросила сотрудника кафе оплатить с данной карты сумму заказа, при этом осужденная не указала на то, кому принадлежит данная карта. Работник торговой организации, то есть кафе, будучи введенным в заблуждение, произвел с предъявленной карты оплату.

Субъектом преступления, предусмотренного ст. 159. 3 УК РФ – любое дееспособное лицо, достигшее 16 – летнего возраста.

Субъективная сторона статьи 159. 3 УК РФ – прямой умысел. О наличии умысла, направленного на совершение такого мошенничества, свидетельствует факт использование поддельной карты или чужой платежной карты без согласия на то ее владельца.

Преступление, предусмотренное ст. 159.3 УК РФ считается оконченным с момента получения лицом товаров или суммы денег, а равно приобретения им юридического права на распоряжение данными товарами или деньгами. Деяние, предусмотренное ст. 159. 3 Уголовного кодекса будет иметь место в случаях, когда платежная карта использована в банкомате, либо ином устройстве, приспособленном для выполнения операций с использованием платежных карт. Действия лица, расплатившегося поддельной или чужой платежной картой в сети Интернет, также подлежат квалификации по соответствующей части статьи 159. 3 УК РФ «Мошенничество с использованием платежных карт».

Мошенничество, совершенное виновным с использованием подделанной им платежной карты, предоставляющей право получения товаров, денег и услуг, квалифицируется по совокупности преступлений, предусмотренных частью 1 статьи 327 УК РФ и соответствующей частью статьи 159.3.

Мошенничество, совершенное с использованием изготовленной другим лицом поддельной платежной карты, полностью охватывается составом преступления, предусмотренным комментируемой статьей, и не требует дополнительной квалификации по ст. 327 УК РФ.

Как квалифицированные составы мошенничества с использованием платежных карт законом предусмотрены, как совершенное группой лиц по предварительному сговору, с причинением значительного ущерба гражданину (часть 2 ст. 159. 3 УК РФ), так и особо квалифицированные составы данного преступления: во– первых, деяния, совершенные с использованием виновными своего служебного положения, а равно в крупном размере (часть 3 ст. 159. 3

УК); во– вторых, деяния, совершенные организованной группой либо в особо крупном размере (ч. 4 ст. 159.3). Сфера противоправного использования платежных карт – область специальных познаний, следовательно, предъявлению обвинения по статье 159. 3 УК РФ должно предшествовать проведение соответствующей технической экспертизы.

Согласно примечаниям к статье 159.3 Уголовного кодекса мошенничество с использованием платежных карт признается совершенным в крупном размере, если стоимость похищенного имущества, превышает сумму 1 500 000 (Один миллион пятьсот тысяч) рублей, мошенничество с использованием платежных карт признается совершенным в особо крупном размере, если стоимость похищенного имущества, превышает сумму 6 000 000 (шесть миллионов) рублей.

В соответствии с Постановлением Пленума Верховного Суда РФ, понимается, что мошенничество РФ не образует состава преступления, предусмотренного ст. 159.3 УК РФ, если хищение денежных средств происходит без участия работника кредитной организации, то оно должно квалифицироваться как кража, на это четко указывает Пленум Верховного Суда в п. 17 Постановления от 30.11.2017 «По делам о мошенничестве, присвоении и растрате».

Согласно Положению об эмиссии платежных карт и об операциях, совершаемых с их использованием, утвержденным Банком России 24.12.2004 №266– П, платежные карты идентичны понятию банковских карт, в свою очередь, банковские карты. При этом согласно п. 1.5 названного положения, банковские карты могут быть кредитными, дебетовыми и предоплаченными, т.е. подделка именно этих трех видов карт либо использование таких карт, принадлежащих другим лицам, подпадает под рассматриваемый состав преступления.

Банковская платежная карта – пластиковаякарта, привязанная к одному или нескольким расчетным счетам в банке, используется для оплаты товаров и услуг, в том числе через сеть Интернет, а также снятия наличных.

Так, согласно ст. 159.6 УК РФ под мошенничеством в сфере компьютерной информации, понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно – телекоммуникационных сетей. Ее появление связано с принятием Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» № 207 – ФЗ от 29 ноября 2012 года, которым в Уголовный закон был введен ряд экономических преступлений, предусматривающих ответственность за совершение, так называемых, квалифицированных видов мошенничества, в том числе и статья 159.6 УК РФ.

Основным объектом рассматриваемого преступления выступают общественные отношения в сфере охраны собственности.

Предметом рассматриваемого преступления выступают чужое имущество или право на чужое имущество. Следует отметить, что при мошенничестве в сфере компьютерной информации предметом, как правило, выступает чужое имущество в виде безналичных денежных средств, изъятых у собственника или доверенных им лиц.

С субъективной стороны мошенничество в сфере компьютерной информации характеризуется наличием у виновного прямого умысла, направленного на хищение чужого имущества или на приобретение права на чужое имущество. При совершении этого преступления виновный не только сознает общественно опасный характер своих действий и предвидит причинение общественно опасных последствий в виде реального имущественного ущерба собственнику (владельцу) имущества, но и желает путем совершения таких действий обратить внимание в свою собственность похищенное имущество (право на него) за счет причинения ущерба законному собственнику (владельцу) имущества.

Субъектом мошеннического посягательства, как и любого преступления, может быть только физическое вменяемое лицо, достигшее 16 лет. Мошенники в сфере компьютерной информации, как правило, обладают определенными профессиональными знаниями в банковском деле, бухгалтерии, в области компьютерных технологий и т.п.

В ч.1 ст. 159.6 УК РФ, мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно – телекоммуникационных сетей, наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

К квалифицированному виду мошеннического посягательства, предусмотренного ч.2 ст.159.6 УК РФ, относится мошенничество совершенное, группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

Часть 3 ст.159.6 УК РФ говорит о более опасных для общества квалифицированных видах мошенничества, совершенные лицом с

использованием своего служебного положения, а равно в крупном размере, наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срокдо пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

Часть 4 ст.159.6 УК РФ говорит о еще более опасных для общества квалифицированных видах мошенничества, совершенные организованной группой либо в особо крупном размере, наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Мошенничество, предусмотренное ст. 159 УК РФ, как «базовый состав», охватывает ряд общественно опасных деяний, выраженных в хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Именно обман и (или) злоупотребление доверием является той границей, которая отделяет мошенничество от иных преступных хищений чужого имущества. Выбор места новых норм о мошенничестве в структуре УК РФ указывает на то, что статьи 159.1 – 159.6 УК РФ являются частными случаями ст. 159 УК РФ и производны от общего «базового» мошенничества – по узкой сфере уголовно – правовой охраны; конкретным предмету посягательства, пострадавшему, уточненным составляющим обманного способа совершения деяния.

С развитием высоких технологий, законодатель выделяет несколько видов мошеннический действий в сфере компьютерной информации. Необходимо учитывать, что мошенничество в сфере высоких технологий

носит более повышенную общественную опасность, чем простое мошенничество. Стремительное развитие цифровых технологий, переход бумажного документооборота на электронный, а также виртуализация в жизни общества и государства, заставляют злоумышленников разрабатывать новые виды преступлений с уникальными способами хищения. Следовательно, необходимо продолжить научные исследования проблем криминализации общественно опасных деяний в сфере высоких технологий для создания и совершенствования теоретической базы противодействия компьютерной преступности.

Из вышеуказанного параграфа, можно сделать вывод, что отсутствие прямо подтвержденных «ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно –телекоммуникационных сетей» (либо «неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации») вызывает затруднение при квалификации преступления по ст.159.6 УК РФ или возможно альтернативным ст. 272 и 273 УК РФ. В отдельных случаях следствием могут быть усмотрены признаки кражи (ст.158 УК РФ) или простого мошенничества (ст.159 УК РФ).

§3. Способы совершения мошенничества связанного с использованием компьютерных и информационных технологий.

Как известно, критерием классификации выступает способ совершения преступления. Согласно диспозиции ч. 1 ст. 159.6 УК РФ и комментариям Верховного Суда РФ к данной норме мошенничество в сфере компьютерной информации выполняется посредством «ввода», «удаления», «блокирования», «модификации» либо «иного вмешательства» в функционирование средств хранения, обработки или передачи компьютерной информации или информационно – телекоммуникационных сетей. Таким образом, мошенничество в сфере компьютерной информации осуществляется не путем «обмана» или «злоупотребления доверием», а посредством разнообразных манипуляций с использованием компьютерной информации (которая выступает средством совершения преступления), и, стало быть, законодатель предусмотрел новую форму хищения. В примечании к ст. 272 УК РФ термин «компьютерная информация» обозначается как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В соответствии с ФЗ от 27 июля 2006 г. N 149[6] «Об информации, информационных технологиях и о защите информации» информация – сведения (сообщения, данные) независимо от формы их представления. Таким образом, согласно УК РФ компьютерная информация представляет собой: а) любые данные; б) в определенной форме – электрических сигналов; в) находящиеся в средствах их хранения, обработки или передачи.

[6]Об информации, информационных технологиях и о защите информации: федеральный закон РФ от 27.07.2006 № 149-ФЗ (в ред. федерального закона от 3 апреля 2020 г. № 105-ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

Однако указание на форму представления информации в примечании к ст. 272 УК РФ диссонирует с положениями ФЗ N 149[7] и не учитывает направления развития информационных технологий. В английских и американских научных журналах уже появились сообщения о способах передачи информации с помощью света, т.е. в основу распространения информации могут быть положены световые, а не электрические сигналы.

Представляется, что определение, используемое в судебной практике, должно базироваться на основополагающих признаках компьютерной информации с учетом перспектив развития информационных технологий. Во–первых, это данные любого содержания. Во – вторых, это данные, которые уже находятся в компьютерах, разновидность которых представлена в виде планшетов, смартфонов, гаджетов, коммуникаторов и т.п. изделий, в основу которых положены принципы действия, присущие любому компьютеру, информационно – телекоммуникационных сетях, серверах, любых материальных (например, флеш – карты) и нематериальных (облака) хранилищах информации. В то же время информация, которая вводится в машину с материальных носителей, становится компьютерной после ее ввода, когда произошло ее преобразование и определено место в памяти компьютера.

Деяние рассматриваемого преступления выражается в действиях в форме хищения чужого имущества или приобретение права на имущество осуществляемого в комбинации или одним из следующих способов:

а) Под вводом такой информации при буквальном толковании ст. 159.6 УК РФ понимается привнесение новых последовательностей электрических сигналов в систему хранения информации с помощью средств ввода: клавиатуры, мыши, сенсорного экрана, соединения между двумя носителями информации для передачи данных, камеры портативного гаджета или лазера и соответствующих программ считывания графической информации (например,

[7]Об информации, информационных технологиях и о защите информации: федеральный закон РФ от 27.07.2006 № 149-ФЗ (в ред. федерального закона от 3 апреля 2020 г. № 105-ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

QR – codereader) и т.д. Ввод информации может выражаться в наборе пароля или номера банковской карты на web – сайте, создании сайта, считывании штрих – кода или QR – кода с пластиковой карточки на КПП охраняемого объекта.

Из этого следует, что вводимые данные могут быть как ложными, так и соответствовать действительности. Получить эти данные лицо может как случайно, так и путем использования высокотехнологичных методов. Один из наиболее сложных способов получения данных – технология фишинга (fishing), не предусматривающая контакта злоумышленника и жертвы, в основе которой находятся рассылка спама, использование вредоносных программ, поддельных сайтов, создание компьютерных сетей (ботнетов), объединяющих без ведома их владельцев тысячи компьютеров, зараженных программами – роботами, выполняющими в интересах владельца ботнета определенные действия.

Этот способ завладения идентифицирующей информацией может выполняться с помощью электронной почты или sms – рассылок сети Интернет, в комбинации этих способов. Так, отдельные вредоносные программы сканируют банковскую активность потерпевшего в сети Интернет, ничем не проявляя себя до тех пор, пока пользователь не посещает web – сайт одного из заложенных в программе банков. В период такого диалога программа активизируется, сканирует пароль входа в систему, сохраняет скриншоты проведенных сессий и отсылает их злоумышленнику. Особенностью программы является ее применение для получения информации при посещении абсолютно легальных, действительно принадлежащих банкам сайтов. Далее средства потерпевшего без его ведома перемещаются на счета злоумышленников, причем нередко производится коррекция страниц с историей переводов и доступного баланса с целью скрыть хищение.

б) удаление компьютерной информации – второй способ совершения преступления, предусмотренного ст. 159.6 УК РФ. Следует отметить, что в ст. 272 УК РФ содержится схожий термин – «уничтожение компьютерной

информации». В то же время удаление и уничтожение информации не синонимичные понятия. Под удалением понимается отведение, разлучение, отдаление с целью не предоставления чего – либо к чему(кому) – либо. Уничтожение означает обращение в небытие, полное истребление. Среди специалистов в области информационных технологий удаление информации рассматривается скорее как ее сокрытие от посторонних, при котором применение специальных методов позволяет эти данные восстановить. При уничтожении информация восстановлению не подлежит.

в) блокирование компьютерной информации – результат воздействия на компьютерную информацию или технику, последствием которого является ограничение или закрытие доступа к компьютерной информации связанное с невозможностью в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, но не связанных с ее удалением.

г) модификация компьютерной информации – внесение любых изменений сведений, сообщений, данных, представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

д) иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно – телекоммуникационных сетей – неправомерное действия, нарушающие установленный процесс обработки, хранения , использования, передачи и иного обращения с компьютерной информацией.

Проведенное обобщение судебной практики показывает, что по ст.159.6 УК РФ квалифицируются хищение чужого имущества, сочетающие в себе комбинацию вышеуказанных способов и, как правило, состоящие в использовании электронных платежных систем (мобильный банк, онлайн банкинг, банк клиент и т.д.), вредоносных программ.

Так например, О – ким районным судом г.Т– ка К. был осужден по ч.2 ст. 159.6 УК РФ, Судом установлено, что К. действуя в группе по предварительному сговору с неустановленным лицом посредством специальной компьютерной программы (приложения), позволяющей получать удаленный доступ к управлению мобильными телефонами (смартфонами) граждан РФ на базе операционный системы «Android»,запущенной в сеть «Интернет», и внедренной в устройства сотовой связи, используемые гражданами РФ, не подозревающими о скрытом размещении данной программы, осуществил незаконный доступ к счетам, на которых размещены безналичные денежные средства держателей банковских карт ПАО «Сбербанк России», реквизиты доступа к которым были определены банковским продуктом «Мобильный банк». Затем данная группа путем ввода, удаления, блокирования, модификации компьютерной информации совершила хищение безналичных денежных средств граждан РФ на общую сумму 46950 рублей без ведома последних, перечислив денежные средства на банковские карты ПАО «Сбербанк России», находящиеся в пользовании и управлении виновного лица.[8]

Также наиболее часто встречающиеся способы мошенничества в сфере компьютерной информации в следственно – судебной практике такие, как:

1. Хищение путем использования виновным лицом номера телефона потерпевшего, к которому подключена услуга «мобильный банк», является наиболее распространенным способом мошенничества в сфере компьютерной информации.

[8]Приговор по делу № 1-25/2017 // Архив Октябрьского районного суда г. Томска

а) потерпевшим в течение нескольких месяцев сим – карта с подключенной услугой «Мобильный банк» не используется, после чего продается компанией сотовой связи новому владельцу, который, получая смс – сообщения с номера «900», имеет возможность осуществлять операции с денежными средствами на счетах потерпевшего.

Например, С. приобрел сим – карту с абонентским номером и с подключенной бывшим владельцем данной сим – карты услугой «Мобильный банк», на которую приходили sms – уведомления о движении денежных средств со счета банковской карты, зарегистрированной на Д.. С., достоверно зная, что на счету указанной банковской карты находятся денежные средства в сумме 13 021 рублей, понимая, что имеет доступ к управлению счетом банковскойкарты, посредством мобильного телефона с использованием услуги « Мобильный банк» путем формирования и отправки sms – сообщения на специальный номер оператора мобильной связи «900» с текстом «5000», то есть ввода компьютерной информации, представленного в форме электронного сигнала, в компьютерную систему банка с последующей модификацией информации о состоянии счета, выраженной в изменении первоначальных данных по движению денежных средств по счету, зачислил со счета указанной банковской карты на счет своего абонентского номера денежные средства в сумме 5 000 рублей, принадлежащие Д. Данные действия квалифицированы судом по ч.2 ст.159.6 УК РФ как мошенничество в сфере компьютерной информации с причинением значительного ущерба гражданину.[9]

б) Телефон с подключенной услугой «Мобильный банк» выбывает из владения собственника по различным причинам (утрата телефонного аппарата, передача во временное пользование, либо его хищение) и преступник получает возможность производить манипуляции с денежными средствами, пользуюсь данной услугой.

[9]Приговор по делу № 1-64/9-2014г.// Архив Кировского районного суда г. Курска.

Так, Р., находясь возле торгового отдела, подошла к К. и под вымышленным предлогом, якобы позвонить, попросил у нее сотовый телефон. К., доверяя Р., добровольно передала ей свой сотовый телефон. Затем Р., незаконно внесла изменения в первоначальное состояние данных лицевого счета банковской карты на имя К., выполнив финансовую транзакцию по списанию денежных средств в сумме 5000 рублей с лицевого счета на имя К., и зачислению указанных денежных средств на лицевой счет на имя Р., тем самым похитила денежные средства, принадлежащие К. в сумме 5000 рублей.[10]

в) Получение путем использования служебного положения или подложный доверенности дубликата SIM– каты, с номером, которому подключена услуга, мобильный банк.

Например К., находясь на своем рабочем месте в офисе продаж и обслуживания ОАО «Вымпелком», используя свое служебное положение, под своей учетной записью осуществила вход в программу АВС « Ensemble» и используя функцию «Запрос данных» осуществила обращение к личной карточке действующего абонента с номером … принадлежащего Е., после чего с помощью функции замены SIM – карты, противоправно, в отсутствие соответствующего заявления клиента Е. произвела замену SIM– карты номера ICCID № на новую SIM– карту с номером ICCID № … Убедившись, что на лицевом счете, принадлежащем Е., находятся денежные средства, незаконно осуществило перевод принадлежащих Е., денежных средств с лицевого счета Е. на банковскую карту № получив реальную возможность распоряжаться поступившими на счет банковской карты денежными средствами.

2. Хищение путем получения виновным лицом данных, санкционирующих доступ к банковским счетам (логин и пароль электронных платежных систем). Доступ к защищенным ресурсам данных систем может быть осуществлен различными способами:

[10]Приговор по делу № 1-188/2015 // Архив Братского городского суда Иркутской области.

а) Получение путем использования вредоносных компьютерных программ и системы удаленного доступа к сети Интернет логина и пароля, вводимых потерпевшим «зараженный» компьютер, посредством которых виновное лицо получает несанкционированный допуск к банковским счетам потерпевшего и управляет движением денежных средств;

б) Получение логина и пароля для доступа к системам электронных платежей благодаря доверительным отношениям с потерпевшим или информации чеков, осуществляемых у банкоматов после активации услуги онлайн – банкинга.

Так, например, Г., в ночное время отыскивал мусорных корзинах стоящих рядом с банкоматами ПАО «Сбербанка России», чек – идентификатор и чек с одноразовыми паролями, используя которое путем удаленного доступа через сеть «Интернет» с помощью системы дистанционного банковского обслуживания «Сбербанк Онлайн» незаконно проникал в «личный кабинет» клиента ПАО «Сбербанк России», после чего с помощью электронных поручений осуществлял переводы с этого счета денежныхсредств на счет имеющиеся у него в распоряжении банковской карты.

3. Хищение путем имитации внесения денежных средств в банкоматы или терминалы самообслуживания. Это также может осуществляться различными способами:

а) Имитация внесения денежных средств, банкоматы или терминалы самообслуживания возможна с помощью вредоносной программы внедренной в банкоматы и терминалы самообслуживания.

Так, Ш. используя вредоносную программу, внедрял ее через зараженные компьютеры – посредники в терминалы самообслуживания. Программа эмулировала принятие купюроприемником терминала наличных денежных средств без фактического их внесения, создавая фонд безналичных денежных средств, которые впоследствии переводились виновным на банковские счета и обналичивались другими участниками преступной группы.

б) Имитация внесения денежных средств в банкоматы или терминалы самообслуживания с помощью поддельных денежных купюр.

Так, Б. с целью хищения чужого имущества, путем вмешательства функционирование средств хранения в информационно телекоммуникационных сетей, внеся платежный терминал № … 4 поддельных денежных банкнот ЦБ России номиналом 5000 рублей, каждая, выполнил функции по пополнению счета абонентского номера мобильного телефона, после чего перевел безналичные денежные средства на свой счет.

4. Хищение путем использования служебного положения, возможности электронного доступа к счетам организации, в которой работа – невиновные лицо или ее клиентов.

Например, Л., работавшая в должности старшего специалиста отдела по работе с корпоративными клиентами, используя автоматизированную систему расчетов «Marti», осуществила операции по переносу денежных средств с лицевых счетов ключевых клиентов на под контрольный ей лицевые счета на имя Б., Ж. на общую сумму 75 373 рублей. Затем Л. провела финансовой корректировки на счетах ключевых клиентов, мотивировавший это тем, что был применен неправильной тариф, при этом достоверно знаю, что тарификация была произведена конкретно.[11]

5. Хищение путем использования вредоносных компьютерных программ внедряемые в мобильные устройства или компьютерные системы, подключенные электронным банковским сервисам.

С помощью вредоносной программы происходит несанкционированная модификация компьютерной информации, формируются подложные электронные платежные поручения и удаляется файл платежного получения с заменой на подложный, содержащий реквизиты счета, подконтрольного виновному лицу.

---

[11] Приговор по делу №1-251/6/2013 // Архив Нижегородского районного суда г. Н.Новгорода.

Конечно, арсенал мошенников, совершающих хищение в сфере компьютерной информации, постоянно расширяется и не ограничивается только вышеуказанными способами. Выбор конкретного способа совершения преступления зависит от имеющихся познаний и навыков, технической оснащенности и изощренности преступников. Следовательно, правоохранительным органам необходимо, совместно с программистами служб безопасности во всех сферах жизни общества разрабатывать, совершенствовать меры по предупреждению посягательств на персональные данные, а также по их сохранению и нахождение их в конфиденциальном виде. Также взаимодействовать синженер – программистами, по созданию современных программных оболочек, а также периферийных устройств для компьютера, которые способствуют защите от атак и кибер – угроз злоумышленников.

Подводя итоги, следует сделать вывод, что в зависимости от конкретного вида мошенничества, ответственность за которые предусмотрена в специальных нормах, законодатель по – разному определил как способ совершения такого преступления, так и их последствия, что опять же приводит к разночтению определения мошенничества в его классическом уголовно-правовом понимании.

На законодательном уровне, необходимо внести изменения в ст.159.6 УК РФ, а именно ч.1 новую формулировку, как «Приобретение права на чужое имущество путем, ввода, уничтожения, блокирования, модификации компьютерной информации». Именно данный состава преступления не включает в себя как, нарушение правил эксплуатации средств хранения либо информационно – телекоммуникационных сетей. В связи с наличием высокой вариативностью мошеннических схем, целесообразнее сохранить указание на иные виды вмешательств и изменить название ст. 159.6 УК РФ на «Приобретение права на чужое имущество путем манипуляций с компьютерной информацией».

Так, в примечании к ст. 159 УК РФ прежде всего необходимо определить мошенничество как хищение чужого имущества, посягающее на права

собственника, независимо от сферы хозяйственной (экономической) деятельности, и причиняющее вред правам и законным интересам потерпевшего.

Кроме того, представляется правильным определение в примечании крупного и особо крупного размера, отличающихся по этим признакам от других преступлений против собственности, кражи, грабежа и т.д. Этим будет подчеркиваться особое внимание законодателя к совершенствованию данной нормы с учетом необходимости усиления уголовной ответственности за такие преступления.

ГЛАВА 2.ТАКТИКА РАСКРЫТИЯ МОШЕННИЧЕСТВ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕ КОМЬЮТЕРНЫХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Особенности раскрытия мошенничеств с использованием платежных карт

XXI век – век, развитых технологий. Технологий, которые кардинально изменили, облегчили нашу жизнь. Связанно это с различными инновациями, в сфере компьютерных технологий, а именно, я хотел затронуть банковскую карту. Во всем мире большое разнообразие различных карт, которые являются носителями денежных средств. Именно поэтому банковская карта, становится объектом преступного посягательства. Мошенники каждый день придумывают

новые способы хищения денежных средств с банковских карт. В законодательстве есть ответственность за совершение таких видов преступлений, как ст.159.3 УК РФ «Мошенничество с использованием платежных карт» .

Профессиональность мошенников повышается вместе с информатизацией населения, поэтому создаются новые способы и методы незаконного завладения чужими денежными средствами. Распространенными схемами преступников являются созданием так называемых «карт – клонов» или по другому «белых карт», «фишинг», «фарминг» и еще ряд других преступлений.

При создании подложных карт, мошенники используют секретную информацию путем считывания ее с магнитной полосы при помощи скимера. После чего мошенники создают копию карты из куска пластика с магнитной полосой на которую переносится вся информация.[12]В последствии мошенник, может свободно пользоваться и распоряжаться картой. Как часто это бывает, когда карта переходит третьим лицам, например при оплате в ресторане, карта переходит в руки официанта.

Также, известными способами являются такого вида преступления как «фишинг» и «фарминг». Рассмотрим их подробнее.

Под фишингом, понимается деятельность преступника по созданию поддельных сайтов товаров, услуг или онлайн – банков и это, как правило, с использованием зарубежных доменов.[13] Попадая на такой сайт, потерпевший вводит свой личные данные с банковской карты для совершения какой – либо покупки или оплаты услуги. Также очень часто бывает спам рассылка, в сообщениях содержатся данные фишингового сайта, на который необходимо перезвонить, где уже соответственно ждут злоумышленники. Как правило,

---

[12]Сенченко П.П. Основные способы хищений с использованием банковских платежных карт // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2014. № 2 (30). С. 30-33.

[13]Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами // Вестник НГИЭИ. 2015. № 3 (46). С. 49-53.

цены на товары и услуги существенно дешевле, тем самым потерпевший «клюет» на предложение преступника, передавая свои данные и внося предоплату за товар. Как правило, после получения суммы, сайт перестает работать. Также очень часто бывает, мошенники завладевают базами номеров абонентов, и затем звонят под видом службы безопасности банка или иными лицами, которые сообщают потерпевшему, что у него проблемы с родственниками или же с персональными данными в банке. В ходе беседы мошенники входят в доверие и под предлогом помощи совершают преступные действия, а именно осуществляют перевод через онлайн – сервисы или же преступник просит подойти к банкомату и выполнить ряд комбинаций, подключит мобильный банк и с помощью поступившего кода потерпевшему, происходит списание денежных средств.

Для хранения, использования и вывода похищенных денежных средств злоумышленники часто используют:

a. Банковские карты;

b. Расчетные счета;

c. Счета абонентских номеров;

d. Электронные кошельки;

e. Наличные переводы .

Также существуют сервисы по переводу наличных денежных средств – «Колибри», «Вестерн Юнион», «Золотая корона». Работа этих сервисов заключается в передаче денежных средств на имя получателя с указанием контрольной информации – кода или пароля. Таким образом, получить переведенные деньги сможет только лицо, предъявившее удостоверяющий личность документ, а также сообщившее кодовое слово или комбинацию. Мошенники не редко используют расчетные счета, открытые на подставных лиц, поэтому они не могут лично обратиться в банк с просьбой снять денежные средства или перевести на другой счет или банковскую карту – для этого они используют онлайн – ресурсы (ДБО – дистанционное банковское обслуживание) на сайте банка, тем самым оставляя свой след в виде IP – адреса.

В раскрытии данного вида преступления оперуполномоченному, необходимо произвести ряд действий таких как:

1. Подробный опрос (допрос) потерпевшего и свидетелей;

2. Попросить выписку с банковской карты потерпевшего, а также детализацию звонков;

3. Необходимо отправить запрос по абонентским номерам мошенника, запрос по банковской карте и электронному кошельку мошенника, запрос SIP – провайдеру (в случае наличия виртуального номер), с приложением судейского постановления;

4. Также направить запросы:

1) по установлению IP – адреса, с которого производился вызов;
2) запрос на дальнейшее движение денежных средств (если деньги переводили на номер);
3) запрос по банковской карте или электронному кошельку мошенника;
4) запрос на получение образца голоса при звонке на горячей линии;
5) изъять видео с банкомата (в случае снятия);

5. В случае установления лица на кого зарегистрирован абонентский номер, произвести допрос лица.

Еще один из не менее популярных, но одна из самых опасных способов хищения денежных средств является как «фарминг». Под фармингом следует, понимать установку на компьютер программного обеспечения, мешающего нормальной работе системе, при этом появляются различного рода сообщения, содержащие ложную информацию. А именно, направление по ложному адресу, т.е злоумышленники портят навигационную структуру, которая отвечает за функционирование браузера. Это может быть локальная версия или система доменных имен, которая используется вашим интернет провайдером, для наведения браузера на нужный объект. Механизм фарминга имеет много общего со стандартным вирусным заражением, т.е жертва открывает электронное письмо исполнительным файлом, который запускается тайно в

фоновом режиме. При этом пользователь даже не догадывается, что собственноручно его запустил, операция не занимает много времени, однако, вредоносное программное обеспечение может содержать URL многих банковских систем. Активируется в тот момент, когда пользователь вводит знакомый ему адрес соответствующий его банку, но при этом попадает на один из ложных сайтов.

Необходимо отметить, что согласно Постановлению Пленума Верховного Суда РФ от 30.11.2017г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если потерпевший сам переводит денежные средства путем обмана или же уговора, это действия необходимо квалифицировать как мошенничество.

При совершении такого рода преступлений, необходима быстрота проведения оперативных действий, а именно взаимодействие с оперативными службами, следственными органами, а также службами безопасности банков.

В первую очередь при раскрытии мошенничества с использованием платежных карт, необходимо подробно опросить потерпевшего совершал ли он покупки в интернет – магазинах, а также установить не производились ли звонки, от службы безопасности банка или же псевдо – родственников, которые просили сообщить данные о банковской карте и PIN – код. Если совершались покупки в интернет – магазине установить электронный адрес. Необходимо уточнить не предшествовали ли ранее сбои в онлайн – сервисах или же при оплате бесконтактным путем. Помимо этого нужно установить факт попадания банковской карты третьим лицам, которые недобросовестно работают в сфере услуг.

Затем потерпевшему необходимо добровольно предоставить, распечатку по банковскому счету, а также детализацию разговоров, что способствует скорейшему раскрытию и квалификации преступления.

Во вторых, необходимо судебное постановление на проведение оперативно – розыскных мероприятий, такого как наведение справок[14]. При наличии вышеуказанного постановления, направить запрос в банк на счет которого перевели денежные средства, с целью получение информации о владельце карты. Как правило, такого рода преступлений, злоумышленники находятся в других субъектах или же за пределами РФ. После установления лица, направляем поручение правоохранительным органам на установление и опрос лица.

Так например, В Казани был вынесен приговор жителю города Москвы, признанному виновным в телефонном мошенничестве. Советский районный суд города Казани рассмотрел уголовное дело в отношении 29 – летнего С– го. Он признан виновным в совершении преступлений, предусмотренных ч. 2, 3 ст. 159 УК РФ (мошенничество с причинением значительного ущерба гражданину в крупном размере), ч. 3 ст. 30, ч. 2 ст. 159 УК РФ (покушение на мошенничество с причинением значительного ущерба гражданину). В ходе следствия и судебного разбирательства было установлено, что с мая по декабрь 2016 г. подсудимый, находясь на территории г. Москвы, с целью хищения денежных средств звонил пожилым жителям Казани и заявлял, что у них обнаружены тяжелые заболевания. При этом злоумышленник представлялся главврачом Республиканской клинической больницы г. Казани. Затем подсудимый предлагал им пройти дорогостоящее лечение. Деньги злоумышленник просил перевести на его счет в банке. В разговорах с некоторыми потерпевшими подсудимый менял тембр своего голоса на женский, имитируя лаборантку. Суд, согласившись с мнением государственного обвинителя, приговорил подсудимого к 4 годам лишения свободы с отбыванием наказания в исправительной колонии общего режима.

---

[14] Об оперативно-розыскной деятельности: федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ (в ред. федерального закона от 2 августа 2019 г. № 311-ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL: http://www.consultant.ru.

В процессе раскрытия данного рода преступлений, а именно мошенничество с использованием платежных систем, есть существенные проблемы такие как:

1. Большое количество времени затрачивается, когда банковские организации и другие правоохранительные органы ответят на поручение.

2. Также как правило, мошенники часто используют незарегистрированные SIM – карты, принадлежность которой установить невозможно.

3. Похищенные денежные средства злоумышленники как правило, переводят на электронные кошельки (Qiwi, WEB – money, Яндекс.Деньги), которые не имеют регистрации.

4. С каждым днем изобретаются новые способы криминальных действий с использованием банковских карт.

5. Отсутствие методических рекомендаций по организации расследования преступных деяний, а также ряд проблем, которые представляют трудности из – за категории мошенничества, связанных с использованием банковских карт, которая в свою очередь, является самой не раскрываемой.

Несмотря, на вышеуказанные проблемы оперативным работникам удается раскрывать, некоторые факты преступлений, так как правоохранительные органы проводят информатизацию населения не только о фактах совершения такого рода преступлений, но и обо всех используемых методах завладения мошенническим путем денежными средствами, находящимися на банковских картах, а также о том, как защититься от мошенников.

Таким образом, подведем выводы по параграфу:

1. Законодателю необходимо, ограничить сроки исполнения постановлений операторами сотовой связи, интернет – провайдерами и банковскими учреждениями до 3 – х суток и установить ответственность за надлежащее исполнение.

2. Мошенничества, совершенные с использованием платежных карт, являются на первых местах из распространенных и при этом, довольно сложным при раскрытии, с которым ежедневно приходиться сталкиваться правоохранительным органам. И следовательно, для своевременного и эффективного раскрытия мошенничества, совершенных с использованием банковских карт, будут зависит от создания специализированных подразделений в составе уголовного розыска, что позволит более интенсивнее бороться с преступлениями в сфере высоких технологий.

§2.Особенности раскрытия мошенничеств в сфере компьютерной информации

Борьба с преступностью – этокомплекс мер, направленных на предупреждение, выявление, пресечение и раскрытие преступлений, установление причин и условий их порождающих, юридическое воздействие на лиц, совершающих преступления. Правоохранительная деятельность осуществляется специально уполномоченными государственными органами в строгом соответствии с законом. Основной задачей остается, борьба с хищениями денежных средств, совершаемых с использованием высоких технологий. Особенностью таких преступлений является новизна и высокая технологическая сложность.

За последнее время информационная среда выступает местом, где совершаются мошеннические действия. Предметом посягательства злоумышленников при совершении мошенничества в сфере компьютерной информации, выступает компьютерная информация, имущество, находящееся в собственности лица или материальные права.

В связи с таким видом преступлений, законодательство выделяет ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», в диспозиции статьи понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей. Также в Постановлении Пленума Верховного Суда от 30 ноября 2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания,

использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» или ст. 274.1 «Неправомерное воздействие на критическую информационную структуру РФ» УК РФ.

В целях раскрытия подобных видов преступлений необходимо определить признаки и место совершения мошенничества. Для определения которого необходимо определить контроль движения информации в сети. В сети Интернет есть система адресации называемая IP – протоколом, построена на основе присвоения каждому компьютеру, подключенному к сети Интернет. IP– адрес – это уникальный идентификационный номер, который присваивается каждому компьютеру при входе в сеть Интернет. Таким образом, числовые адреса заменяются символьными знаками с использованием доменной системы преобразования имен. Система доменов позволяет преобразовывать символьные имена в IP – адреса и обратно определять имя домена по числовому адресу. IP – адрес выдается компьютеру его интернет провайдером в момент начала сессии – открытия первой интернет – страницы, и заканчивается закрытием интернет – сессии, а именно закрытием последней интернет – страницы. Как правило, злоумышленники размещают на Интернет – сайтах, разрешающие файлы на которых установлено вредоносное программное обеспечение, в результате чего в фоновом режиме устанавливается на персональный компьютер потерпевшего.[15]

С помощью такого вируса и совершаются преступления связанные с компьютерной информацией, именно этот вирус может удалить, блокировать, модифицировать или иным образом, существенно навредить персональной информации и материальным правам пользователя. При этом пользователь не

[15]Селяков Н. А., Градицкая Н. С. Мошенничество в сфере компьютерной информации // Уголовная политика, уголовное законодательство: правоприменительная практика: сборник научных статей. Спб.: СпбГЭУ, 2016. 34 –37с.

осознает, что он подвергся такого рода преступления и с помощью флеш – накопителя распространяет вредоносное программное обеспечение, другим пользователям, тем самым открывая все больше доступ для злоумышленников.

В данном случае для раскрытия преступления необходимо, IP – адрес злоумышленника, что способствует установлению его нахождения персонального компьютера с которого он работал. В помощь оперативному работнику существует интернет – ресурс www.2ip.ru, который помогает установить город, страну провайдера злоумышленника, а также направить запрос в правоохранительные органы для точного определения преступника и дальнейшего его задержания и изъятия компьютерной информации. Конечно же, более продвинутые мошенники не останавливаются и совершают преступления с помощью виртуальной частной сети (VPN), которая усложняет установить получения IP – адреса путем ее анонимности в сети. Смысл виртуальной частной сети заключается в том, что пользователь интернета, перед тем как выйти на сайт, подключается к серверу третьего лица, как правило локализующего на территории иного государства. По сути запрос на интернет – сайт проходит аналогичным образом, какой был описан ранее, однако в истории соединений сайта остается не реальный IP – адрес пользователя, а IP – адрес использованного им VPN – сервера, который, как показывает практика, в большинстве случаев принадлежит иностранным интернет провайдерам, которым направить запрос в рамках Российского правового поля не представляется возможным. В раскрытии и установлении лица помогают Cookie– файлы, которые имеют множество интернет сайтов, но не все хранят информацию о своих пользователях.[16]

Cookie – файл – это фрагмент данных, который интернет сайт передает в интернет – браузер (GoogleChrome, MozillaFirefox, Яндекс и др.) своего нового пользователя, чтобы «запомнить» его. При следующем посещении данного

[16]Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4 – 9.

сайта, он уже будет «знать» о подключившемся пользователе ряд информации, которая будет расти с каждым последующим посещением:

1. сайт запоминает логин и пароли – именно благодаря Cookie – файлам не нужно каждый раз вводить пароли в социальных сетях и других сайтах;

2. сайт запоминает предпочитаемый язык;

3. сайт запоминает последние просматриваемые страницы;

4. сайт запоминает историю посещения.

Важной особенностью Cookie – файлов является их неизменность – мошенник может множество раз менять свой IP – адрес через VPN, сайт все равно «поймет», что подключается один и тот же пользователь.

Один из примеров мошеннической схемы через сайт «Авито»:

Иванов Иван Иванович регулярно размещает на вышеуказанном сайте мошеннические объявления о продаже автомобильных запчастей, при этом перед входом на сайт подключается к VPN, чтобы его реальный IP – адрес оставался неизвестным. По одному из таких объявлений ему звонит покупатель, вносит предоплату за товар на счет банковской карты или абонентского номера злоумышленника, тем самым становится жертвой мошеннических действий.

Сотрудники правоохранительных органов направляют запрос на сайт «Авито» о предоставлении информации о лице, разместившем данное мошенническое объявление, необходимо также запросить провести анализ Cookie – файлов мошенника с целью установления всех объявлений, которые размещались с браузера данного персонального компьютера, а также информацию о всех IP – адресах, использованных для посещения сайта.

В результате чего, при наличии информации хотя бы по одному объявлению злоумышленника, возможно получить сведения по всем объявлениям, размешенным раннее злоумышленником.

Таким образом, целесообразно провести анализ ранее размещенных объявлений, с целью определения всех созданных злоумышленником объявлений, определить с какого конкретно персонального компьютера

создавалось объявление, с указанием личных IP – адресов и личного абонентского номера злоумышленника. Так как, данные объявления мог разместить сам Иванов И.И. или же их мог создать один из членов его семьи, воспользовавшись его компьютером, тем самым раскрыв реальные персональные данные мошенника. Также необходимо учитывать человеческий фактор, Иванов И.И. при создании нового объявления мог забыть включить VPN, что позволит узнать конкретный адрес преступника.

Следует отметить, что рассмотренные выше особенности выявления мошенничества в сфере компьютерной информации оказывают огромное влияние на деятельность правоохранительных органов, расследующих преступления связанных с мошенничеством в сфере компьютерной информации[17].

Таким образом, способы совершения преступления в сфере компьютерной информации не исчерпывающий, как и «профессионализм», а также психофизические свойства мошенников. Именно поэтому при расследовании мошенничества не нужно прибегать только к одной тактике, следует всесторонне рассматривать данный вид преступления.

Подводя вывод, следует отметить, что необходимо законодательно выделить основные мероприятия:

1. Рассмотреть и разработать план взаимодействия правоохранительных органов на международном уровне, а также с обменом практики и информацией в борьбе с преступностью в сфере высоких технологий.
2. Повысить уровень практических работников по раскрытию и расследованию преступлений в сфере высоких технологий.
3. Необходимо разработать программу для подготовки молодых кадров специализирующихся конкретно для работы в сфере высоких технологий.

---

[17] Миронов С.Н., Музеев А.И. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных ст. 159.6 УК РФ: методические рекомендации/ Министерство внутренних дел РФ, Казанский юридический институт; – Казань: КЮИ МВД России, 2018.С. 6 – 8.

§3. Тактика выявления мошенничеств в сети Интернет.

В мировой глобальной сети Интернет содержится большое количество разнообразных услуг, предложений производителей и не всегда за этим стоит законопослушное лицо. Как правило, за красивым брендом может скрываться мошенник. Преступления в сети Интернет представляют собой разного рода, начиная от покупки продуктов питания, до совершения сделки с недвижимостью, в которых задействованы крупные денежные суммы. Злоумышленники создают красивые рекламы, небывалые скидки и приятные акции, которые конечно не пройдут мимо глаз покупателей и, как привило, они становятся потерпевшими в мошеннических действиях.

Выявить и установить мошенника представляется возможным, соблюдая некоторые предосторожности перед совершением покупки:

1. Низкая цена.

При обнаружении объявления или магазина, предлагающие товары по ценам существенно ниже рыночных, необходимо помнить, что злоумышленники используют данный прием для привлечения жертв. Необходимо сравнить стоимость аналогичных товаров в других Интернет–магазинах, она должна отличаться от объявлений мошенников. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить».

2. Требование предоплаты.

Мошенники предлагают перечислить некую предоплату за товар, особенно с использованием электронных кошельков, анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя совершенно иного лица, данные операции являются опасными.

3. Отсутствие возможности курьерской доставки и самовывоза товара.

Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату. Необходимо выбирать магазины, где есть возможность забрать товар самостоятельно. Преступники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствуют сведения о продавце, а также его контактов для связи.

На сайте Интернет– магазина отсутствуют сведения об организации или индивидуальном предпринимателе. Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Подробно изучить отзывы о магазине в Интернете. В случае совершения покупок необходимо посмотреть историю сделок продавца и ознакомиться с его рейтингом, большое количество торговых площадок предлагают подобную услугу.

5. Неточности или несоответствия в описании товаров.

В описании товара присутствуют несоответствия. Необходимо внимательно прочитать описание товара и сравнить его с описаниями на других Интернет– ресурсах.

6. Как правило, у мошенников присутствует излишняя настойчивость.

В процессе совершения покупки продавец магазина начинает торопить с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи. Злоумышленники часто используют временной фактор для того, чтобы покупатель не смог адекватно оценить все нюансы сделки.

7. Преступники для подтверждения личности отправляют изображение паспорта.

Чтобы войти в доверие продавцы в социальных сетях отправляют изображение паспорта, при этом ожидая перевода денежных средств. Не нужно

забывать, что в условиях развития современной техники изготовить изображение паспорта на компьютере не представляет никакой сложности.

Учитывая вышеперечисленные обстоятельства, мошенники все же достигают своих целей, но в случае установления справедливости и возврата денежных средств, у правоохранительных органах существует алгоритм раскрытия такого рода преступлений.

1. При поступлении заявления или сообщения о мошенничестве необходимо подробно опросить потерпевшего, выяснить:

- в какое время поступил звонок;
- с какого номера телефона ему звонили;
- кем представился преступник, о чём говорил, что предлагал сделать;
- какую сумму денежных средств и за какие услуги преступник просил передать ему;
- способ передачи денежных средств (блиц– перевод, нарочным, пополнение счёта определённого номера мобильного телефона и др.);
- звонил ли заявитель повторно преступнику;
- сможет ли описать голос преступника (хриплый, высокий или низкий, молодой или старый и т.п.) и опознать его;
- если денежные средства передавались нарочным посреднику, то необходимо описать внешность лица, которому переданы денежные средства, и в последующем рассмотреть вопрос о воссоздании его внешности с помощью составления субъективного портрета.

2. При поступлении сообщения о «телефонном» мошенничестве сотрудникам оперативных подразделений необходимо немедленно принять меры к установлению вида, марки сотового телефона, идентификационного («IMEI») и абонентского номера, по возможности установить место нахождения, установить в какой организации, оказывающей услуги населению по осуществлению мобильной связи, зарегистрирован указанный абонентский номер.

IMEI – уникальный номер сотового аппарата, данный номер состоит из 15 последовательных чисел, из которых первые 14 определяют происхождение, модель и серийные номера сотового устройства именно по ним осуществляется идентификация, а пятнадцатая –контрольная цифра.

3. При дальнейшей работе по материалу предварительной проверки либо по возбуждённому уголовному делу в кратчайший срок провести биллинг исходящих мобильных соединений с телефонного номера, по которому звонили потерпевшему, установить номера абонентов соединений, адреса, данные о личности (организации, предприятии и др.), проверить указанных абонентов на причастность к преступлению.

4. С целью получения дополнительных данных об абоненте, представляющих интерес по материалу проверки (ФИО, адреса, названия предприятия и т.д.), оперуполномоченный, выносит постановление о возбуждении перед судом ходатайства о проведении оперативно– розыскных мероприятий с целью получения информации об абоненте, либо, в случае необходимости, о самих телефонных переговорах, либо о производстве контроля и записи телефонных и иных переговоров. Анализ полученной информации от операторов мобильной связи позволит выявить не известных соучастниках, потерпевших и свидетелей преступления.

5. При установлении полных данных лиц, которым поступали входящие вызовы и СМС– сообщения с мобильных средств связи «телефонного» мошенника, опросить и допросить их в установленном уголовно– процессуальным законом порядке, проверить на причастность к преступлению.

6. Если денежные средства отправлены онлайн – переводом через приложение Сбербанка России, необходимо установить, когда и каким способом потерпевший сообщил ФИО и контрольный номер перевода, которые необходимы для получения отправленных денежных средств преступнику. Запросить в Сбербанке России информацию о денежных переводах, полученных злоумышленником, название и адрес филиала, где они были получены, а также изъять записи с камер видео – наблюдения; при

установлении получателя денежных средств запросить форму № 1 получателя денежных средств. По полученной информации необходимо установить лицо, а также изучить сведения о судимости. Допросить данного гражданина по обстоятельствам получения им денежных переводов, получить образцы голоса и предъявить их на опознание потерпевшему. При необходимости назначить и провести психофизиологическое исследование (ПФИ «Полиграф).

7. При получении результатов из компании мобильной связи: необходимо опросить (допросить) лицо, на которое зарегистрирован мобильный номер телефона (SIM– карта), с использованием которого звонили потерпевшему, получить образцы голоса и предъявить их на опознание потерпевшему. При необходимости назначить и провести психофизиологическое исследование. В случае, если гражданин, на которого оформлен мобильный номер телефона, говорит о том, что не оформлял его, то необходимо изъять документы из компании мобильной связи и назначить исследование по почерку или почерковедческую судебную экспертизу по ним, а также установить родственников данного гражданина и круг его общения с целью получения информации, нет ли среди них лиц, ранее судимых за аналогичные преступления, и лиц, отбывающих наказание в исправительных учреждениях. В случае положительного результата проверить их на причастность и провести проверку на причастность к ранее совершённым преступлениям.

8. Если денежные средства были зачислены на мобильный номер телефона или электронный кошелёк (Qiwi,WebMoney, Яндкс.Деньги и др.), направить запрос в организацию, которая осуществляет администрирование электронного кошелька с целью предоставления регистрационной информации владельца идентификатора, выписки из журнала входа его в систему и журнала транзакций с момента регистрации в системе, сведений об IP– адресе, с которого осуществлялось вхождение в систему.

Сведения по электронным кошелькам которые необходимо запрашивать :

– информацию о паспортных данных владельца электронного кошелька;

– информацию о способе и месте идентификации электронного кошелька;

– информацию об абонентском номере, с использованием которого был создан электронный кошелек;

– информацию об абонентских номерах, привязанных к электронному кошельку;

– информацию о виртуальных банковских картах, которые были выпущены по данному электронному кошельку;

– информацию о пластиковых картах, выпущенных по данному кошельку, способ их получения (адрес почтового отправления);

– информацию о входящих и исходящих платежах по электронному кошельку с момента его регистрации;

– информацию об IP – адресах, использованных для совершения денежных транзакций, а также администрирования электронного кошелька.

Необходимо опросить (допросить) лицо, на которое зарегистрирован электронный кошелёк, с использованием которого были похищены денежные средства, получить образцы голоса и предъявить на опознание потерпевшему. В случае положительного результата проверить на причастность и провести проверку на причастность к ранее совершённым преступлениям.

9. Если денежные средства переданы потерпевшим нарочному с участием заявителя, очевидцев составить субъективный портрет лица, которому переданы денежные средства. Затем установить, имелись ли в месте передачи денежных средств камеры наружного наблюдения, если да, то изъять видеозаписи, осмотреть их и приобщить к материалам проверки или уголовного дела в качестве вещественных доказательств;

10. Полученные в ходе проверочных действий документы (предметы) приобщить к материалам проверки.

Первоначальные оперативно– розыскные мероприятия и следственные действия, порядок их проведения зависят от того, удалось ли по «горячим

следам» задержать мошенника. В большинстве случаев на момент поступления заявления неизвестно, кто совершил мошенничество.

Выводы по параграфу:

1.Необходимо на законодательном уровне, правоохранительным органам и сотрудниками интернет – провайдеров сократить уровень анонимизации в сети Интернет, для дальнейшего выявления и идентификации лица, а также установить ответственность за уклонение от регистрации. Данные условия способствуют не только выявлению лиц совершающих мошенничества в сфере высоких технологий, но и с такими видами преступлений как: распространение ложных данных в сети Интернет, кибербуллинг, незаконный оборот наркотиков осуществляемый бесконтактным путем.

2. С целью повышения качества расследования данного вида преступлений необходимо совместное планирование процессуальных и оперативных мероприятий, которые изложены в методических рекомендациях: «О предупреждении, раскрытии и расследовании преступлений по отдельным видам мошенничеств». Необходимо, включить изучение преступлений в сфере высоких технологий в высших учебных заведениях системы МВД России, а также проводить научно – практические мероприятия с будущими сотрудниками правоохранительных органов. При этом расследование преступлений в сети Интернет, требует привлечение специалистов по конкретной области, на что затрачивается время раскрытия и обнаружение преступника, чтобы ускорить этот процесс. МВД России необходимо усовершенствовать материально – техническую базу сотрудников, начиная с территориальных отделов ОВД.

§4. Использование возможностей БСТМ при раскрытии мошенничества, совершенного с использованием компьютерных иинформационных технологий

В последнее время в связи с повышением компьютерной грамотности общего числа населения РФ возросло количество преступлений, совершенных в сфере высоких технологий.

Проведение мероприятий по преступлениям связанным с неправомерным доступом к компьютерной информации и использованием вредоносного программного обеспечения, требует специальных познаний в области компьютерной информации и должно осуществляться в тесном взаимодействии с отделом «К» БСТМ МВД РФ.

В пределах своей компетенции БСТМ МВД России осуществляет выявление, предупреждение, пресечение и раскрытие:

1. Преступлений в сфере компьютерной информации:

– неправомерный доступ к охраняемой законом компьютерной информации;

– создание, использование и распространение вредоносных компьютерных программ;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно – телекоммуникационных сетей;

– мошенничество в сфере компьютерной информации.

2. Преступлений, совершаемых с использованием информационно телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности:

– изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних;

– использование несовершеннолетнего в целях изготовления порнографических материалов или предметов.

3. Преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации.

4. Преступлений, связанных с незаконным использованием объектов авторского права или смежных прав.

На первоначальном этапе необходимо установить признаки совершения подобных преступлений, которые выражаются в следующем:

– потерпевшим самостоятельно не производились какие – либо сомнительные операции, связанные с переводом денежных средств с расчетных счетов;

– потерпевшему без его участия или участия владельца определенного Интернет – ресурса заблокирован доступ к собственной компьютерной информации, разрешенной на компьютерной технике, современном устройстве сотовой связи, электронном почтовом ящике, персональной странице в социальной сети и т.п.;

– информация, размещенная на перечисленных ресурсах, уничтожена, модифицирована или скопирована без участия потерпевшего.

В случае выявления перечисленных признаков необходимо провести следующие первоначальные мероприятия:

1. Произвести подробный опрос потерпевшего с целью выяснения следующих обстоятельств:

– когда и при каких обстоятельствах обнаружен факт хищения, или когда и при каких обстоятельствах произошло уничтожение, блокирование, модификация либо копирование компьютерной информации;

– какие электронные платежные средства использовались потерпевшим при совершении финансовых операций с использованием расчетного счета, с которого были похищены денежные средства;

– какая компьютерная техника использовалась потерпевшим при совершении законных финансовых операций, а также отклонения от обычной

работы данной техники (наличие сбоев, следов посторонних воздействий и т.п.);

– в случае уничтожения, блокирования, модификации либо копирования компьютерной информации, на какой компьютерной технике, современном устройстве сотовой связи или Интернет – ресурсе размещалась компьютерная информация;

– дата и время совершения противоправных платежных операций;

– осуществлялось ли дальнейшее использование компьютерной техники после обнаружения факта хищения, либо уничтожения, блокирования. Модификации либо копирования компьютерной информации;

– проводились ли ремонтные, профилактические работы.

2. В обязательном порядке разъяснить потерпевшему необходимость сохранения компьютерной техники в неизменном виде (исключить дальнейшее использование, самостоятельное удаление вредоносного программного обеспечения).

3. По возможности изъять для приобщения к материалу проверки компьютерную технику в комплексе (системный блок, смартфон) либо накопитель информации (жесткий диск, флэш – карту и т.п.).

4. По изъятой компьютерной технике необходимо назначить компьютерное – техническое исследование с целью получения ответа на следующие вопросы:

– наличие на компьютерной технике вредоносного программного обеспечения или его следов;

– каким способом произведена установка на компьютерную технику вредоносного программного обеспечения;

– наличие следов деятельности или образцов вредоносного программного обеспечения;

– наличие следов деятельности или образцов вредоносного программного обеспечения (присутствие файлов, созданных вредоносным программным обеспечением и т.п.);

– иные сведения, представляющие интерес.

При назначении компьютерного – технического исследования постановку вопросов необходимо согласовывать с экспертом. В самом отношении необходимо указывать, что вопросы поставлены в редакции эксперта.

5. Организовать работу с отделом «К» БСТМ МВД России по существу проведения дальнейших мероприятий.

Анализ оперативной обстановки и имеющиеся оперативные данные свидетельствует о том, что в настоящее время на территории России существует обширный рынок сбыта вредоносного программного обеспечения, широко развернута деятельность ряда глубоко законспирированных, либо с закрытым доступом, то есть требующих специального «инвайта», а также «открытых» и «полуоткрытых» Интернет – ресурсов, на которых происходит рекламирование, распространение, обмен и продажа вирусных программ, в том числе с участием несовершеннолетних. Также не стоит забывать и об Интернет – ресурсах бесплатных объявлений – излюбленное место распространителей вируса.

В по факту распространения гражданином вредоносных компьютерных программ за денежное вознаграждение, в рамках материала проверки возбужденно уголовное дело по ст. 273 УК РФ в СУ УМВД России Н – ской области.

Для наглядности используются материалы оперативных разработок, реализованных сотрудниками подразделения «К» БСТМ УМВД России по Н– ской области, а также материалы расследования уголовного дела (№2012– …) в отношении лица, обвиняемого в преступлении, предусмотренном ст.273 УК РФ.

Работу по выявлению и пресечению фактов преступной деятельности фигурантов по распространению вредоносных компьютерных программ условно можно разделить на три взаимосвязанных и последовательных этапа:

– получение и проверка информации в целях установления фактов незаконного распространения вредоносного программного обеспечения, и лиц к ним причастных;

– оперативная разработка и документирование преступной деятельности фигурантов (с использованием имеющихся оперативных возможностей), подготовка и предоставление в следственные органы материалов ОРД, достаточных для возбуждения уголовного дела;

– реализация материалов разработки и оперативное сопровождение расследования по уголовному делу, как правило, вплоть до рассмотрения дела в суде.

Например: В 2014 году в отдел «К» БСТМ УМВД России по Н– ской области поступила оперативная информация, о том, что гражданин, имеющий ник в сети Интернет в программе видео – звонков «Skype» «51» (предположительно Иванов Иван Иванович), в группе с неустановленными лицами занимается за денежное вознаграждение созданием и распространением вредоносных компьютерных программ, предназначенных для взлома и неправомерного доступа, а также обучает хакингу. Продажа вредоносных компьютерных программ «51» (Ф.И.О.) осуществляется с использованием возможности сети Интернет (в том числе через сайты объявлений), через форумы Интернет – ресурсов таких, как «Xaker.ru», «Forum.N– sk.ru», размещенные на ресурсах « Н– скета».

В целях конспирации «51» никаких контактных данных в сети не оставлял, кроме почты «51@gmail.ru» и ника «Skype» «51». Регистрацию и доступ к вышеуказанным ресурсам осуществляет с использованием анонимайзера.

В целях проверки достоверности полученной оперативной информации была разработана оперативная комбинация, целью которой являлась попытка войти в доверие и получить дополнительные контактные сведения о распространителе программных продуктов посредствам переписки.

В целях установления причастности фигуранта к распространению вредоноса в сети Интернет проведен мониторинг (наблюдение), поиск и анализ информации, размещенной на сайтах, расположенных на информационных ресурсах Н– ский провайдеров сети Интернет, на англо– русскоязычных сайтах России и иностранных государств. Получены образцы продукции для проведения сравнительного исследования.

Даны соответствующие задания (поручения) подсобному аппарату на установление фигуранта и его связей, причастных к распространению, написанию и распространению вредоносных компьютерных программ, а также конкретных фактов преступной деятельности.

Осуществлены необходимые проверки по оперативно– розыскным, справочно – вспомогательным и криминалистическим учетам УМВД России по Н– ской области и другим информационным база данных.

Проведен сбор и анализ дополнительно полученной оперативной информации, по результатам которой был назначен последующий план действий по документированию и разоблачению преступной деятельности фигурантов (сбор характерных следов и установления способов совершения данного вида преступлений).

В ходе ОРМ были получены сведения об IP – адресе, с которого фигурант размещал объявления, а также установлен круг лиц, способных освещать деятельность фигуранта.

Также в ходе переписки, оформленной актом наблюдения в присутствии представителей общественности, с фигурантом посредством компьютерной программы «Skype» установлены контактные номера телефонов, а также назначена встреча для проведения ОРМ «проверочная закупка».

В ходе реализации намеченного плана действий оперативной комбинации на подготовительном этапе перед встречей был составлен ряд вопросов, при ответе на которые фигурант давал бы конкретные ответы, указывающие на осведомленность о нарушении законодательства РФ и достаточность своих

знаний в технической части. В зависимости от складывающейся оперативно–розыскной ситуации определяется список необходимых вопросов:

1. Какое образование имеет фигурант?

2. Его уровень навыков владения компьютером?

3. Осведомленность об уголовной ответственности за распространение вредоносных программ?

4. Имело ли место создание им конкретно данной компьютерной программы? Если да, то при каких обстоятельствах.

5. Где, когда, при каких обстоятельствах имело место завладение данной компьютерной программой?

6. Сколько раз и кому реализовывал фигурант распространенную программу?

7. Какие функции выполняет интересуемая программа?

8. Осуществлял ли фигурант неправомерный доступ с использованием продаваемой программы? Если да, то в отношении кого именно.

9. Обучал ли кого – либо пользоваться данным программным продуктом?

После проведения исследования закупленной компьютерной программы 15 апреля 2014 года на основании постановления заместителя начальника УМВД России по Н – ской области произведена проверочная закупка образцов вредоносного компьютерной программы «SpyNet 2.7» распространяемой фигурантом.

По итогам проведенного исследования собранного материала, где следы совершения данного вида преступления были задокументированы, выяснены обстоятельства, указывающие на преступную деятельность фигуранта, появились достаточные основания полагать, что в действиях разрабатываемого лица (разрабатываемых лиц) имеются признаки преступления, указанные в ст. 273 УК РФ. Далее данный материал проверки был направлен в следственный орган для вопроса о возбуждении уголовного дела.

В ходе взаимодействия оперативных сотрудников уголовного розыска и сотрудников оперативного подразделения «К» БСТМ МВД России, существует

алгоритм действий по проведению оперативно – технических мероприятий, которые в свою очередь должны носить законную правовую основу в собирании доказательственной базы в рамках материала проверки, а также содержать в себе обоснованность, мотивированность , своевременность и реальность их исполнения.

Подводя итоги, можно сделать вывод, что сотрудникам отдела «К» совместно взаимодействовать с международными компаниями, специализирующихся на разработке систем защиты от компьютерных угроз по созданию единой базы программ по выявлению, а также по раскрытию лиц, которые непосредственно занимаются распространением вирусных программ, спама в сети Интернет.

В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистической значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве одноименного оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам.

Как бы ни складывалась оперативно – следственная ситуация, в любом случае сотрудники правоохранительных органов, должны всегда знать о нюансах и последовательности получения следов, которые в дальнейшем будут вещественными доказательствами в уголовном деле.

ЗАКЛЮЧЕНИЕ

Обобщая результаты проведенного исследования, мы приходим к выводу, что система работы оперативных подразделений правоохранительных органов, обеспечивающих своевременное реагирование и раскрытие на преступления в сфере высоких технологий с использованием вредоносных программ, не достаточно проработана, но приобретает особую значимость в связи с компьютеризацией и использованием глобальной сети Интернет.

С учетом сложившейся ситуации, по поводу правоприменительной практики форм хищения, ст.159.6 УК РФ, определено, что в случае, если хищение чужого имущества или приобретение частного права на чужое имущество путем ввода, удаления, блокирования, модификации либо иного вмешательства функционирование средств хранения, обработки или передачи компьютерной информации или сетей Интернет осуществляется с участие лица, который воспринимает искаженную информацию как истинную, то данное преступление необходимо квалифицировать как мошенничество в сфере компьютерной информации.

Развитие высоких технологий в настоящее время находится на этапе развития и требует пристального внимания и изучения, так как реализация правовой защиты затруднена наличием пробелов в законодательстве, которые вызывают огромное количество проблем на практике. В связи с этим работа может представлять интерес в качестве законотворческой инициативы и практической значимости для ОВД, уголовного розыска.

Основные выводы проведенного исследования, сделанные на основании анализа действующих нормативных правовых актов российского законодательства, теоретических положения, материалов оперативно–

розыскной и судебной и следственной практики, а также мнения практических сотрудников, нашли свое отражение в следующих положениях:

1. Очевидный факт повышения общественной опасности мошенничества в сфере высоких технологий по сравнению с простым мошенничеством. На данный момент общественно опасные деяния в сфере компьютерных технологий не отвечает реальному положению вещей. Именно, причиной данного проявления является изучение проблем компьютерной преступности и стремительное развитие самой сферы высоких технологий.

2. Выделение мошенничества в сфере высоких технологий как отдельного состава преступления против собственности и особо квалифицированного вида мошенничества. Необходимость введения вышеуказанной нормы у законодателя не должен вызывать никаких сомнений, так как недооценка борьбы с вышеуказанными действиями, носящими противоправный характер, приводит к печальным последствиям.

3. Любая информация хранящаяся на персональном компьютере пользователя, а также на периферийных устройствах , подлежит уголовно – правовой защите, так как неправомерное обращение с которой может нанести ущерб ее собственнику.

4. Способы хищения такие как: ввод, удаление, блокирование, модификация компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно – телекоммуникационных сетей, вызывают вопросы, при решении квалификации о совокупности преступлений со ст. 183, 187,272, 273 УК РФ, при этом необходимо установить, основания доступа к компьютерной информации, а также осуществлялся ли доступ незаконно.

5. Взаимодействие оперативных подразделений ОВД, такие как Управление «К» БСТМ МВД России, отделы «К» БСТМ МВД России, ГУМВД и УМВД субъектов РФ, специализированные отделы ГУЭБиПК МВД России и подразделений экономической безопасности МВД, ГУМВД и УМВД субъектов РФ, а также некоторых подразделений уголовного розыска, значительно

способствует работе по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации.

6. В представленной работе также приведен алгоритм действий, а также проведение ОРМ по раскрытию оперативными работниками преступлений в сфере высоких технологий.

7. В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистической значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве одноименного оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате чего, собранные оперативными сотрудниками сведения о переговорах и других, в широком понимании этого значения, задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного разрешения по уголовным делам.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативно – правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6– ФКЗ, от 30.12.2008 N 7– ФКЗ, от 05.02.2014 N 2– ФКЗ, от 21.07.2014 N 11– ФКЗ)// Собрание законодательства РФ. – 2014. – N 31. – Ст. 4398.

2. Уголовный кодекс Российской Федерации: федеральный закон РФ от 13 июня 1996 г. № 63– ФЗ (в ред. федерального закона от 1 апреля 2020 г. №73– ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL: http://www.consultant.ru.

3. Уголовно– процессуальный кодекс Российской Федерации: федеральный закон РФ от 18 декабря 2001 г. №174– ФЗ (в ред. федерального закона от 24 апреля 2020 г. №130– ФЗ)// Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL: http://www.consultant.ru.

4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51– ФЗ (в ред. от 27.12.2019 г. №489– ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

5. Об оперативно– розыскной деятельности: федеральный закон РФ от 12 августа 1995 г. № 144– ФЗ (в ред. федерального закона от 2 августа 2019 г. № 311– ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

6. О национальной платежной системе: федеральный закон РФ от 27.06.2011 № 161– ФЗ (в ред. федерального закона от 27.12.2019 г. № 490– ФЗ)

// Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

7. О банках и банковской деятельности : федеральный закон РФ от 02.12.1990 № 395– 1 (в ред. федерального закона от 27.12.2019 г. № 507– ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

8. Об информации, информационных технологиях и о защите информации: федеральный закон РФ от 27.07.2006 № 149– ФЗ (в ред. федерального закона от 3 апреля 2020 г. № 105– ФЗ) // Консультант Плюс: комп. справ.правовая система [Электронный ресурс] URL:http://www.consultant.ru.

9. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2012 г. № 51 // Рос.газета. – 2008. – № 4.

Книги, монографии, сборники научных трудов, учебные пособия

10. Андреев, Б.В., Пак, П.Н., Хорст, В.П. Расследование преступлений в сфере компьютерной информации: учебное пособие/Б.В. Андреев. П.Н. Пак, В.П. Хорс. – М.: Юрлитинформ, 2012. – 152 с.

11. Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. – 449с.

12. Атаманов, Р.С. Некоторые вопросы расследования мошенничества в сети Интернет/Р.С. Атаманов. – Актуальные проблемы российского права, 2010. – № 4 (17). – 496 с.

13. Бурлаков, В.Н., Горшенков, Г.Н, Максина, С.В.,. Шестаков, Д.А. Средства массовой информации и преступность (криминология СМИ)/В.Н. Бурлаков, Г.Н. Горшенков, С.В.Максина. – Правоведение, 2012. – № 5. – 584 с.

14. Вехов, В. Б., Попова, В. В., Илюшин, Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: учебное пособие/В.Б. Вехов, В.В Попова, Д.А.Илюшин., 2014. – 289 с.

15. Воробьев, В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. канд. юрид. наук. – Н. Новгород, 2010. – 200 с.

16. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных ст. 159.6 УК РФ: методические рекомендации/ С.Н. Миронов, А.И. Музеев, Н.М. Сафин, – Казань: КЮИ МВД России, 2018. – 51 с.

17. Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. №.23. С. 2– 5.

18. Гудзь, Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий/Е.Г. Гудзь. – Сб. докладов науч. практ. Семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств». – М., 2012. – 62 с.

19. Дворецкий, М.Ю. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ: учебное пособие/М.Ю. Дворецкий, А.Н. Копырюлин. – Уголовное право, 2012. – № 4. –34с.

20. Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – 200 с.

21. Завидов Б. Д., Ибрагимова, З. А. Мошенничество в сфере высоких технологий: учебное пособие/Б.Д. Завидов, З.А. Ибрагимова. – Современное право, 2011. – № 4. – 44 с.

22. Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами // Вестник НГИЭИ. 2015. – № 3 (46). – 150с.

23. Крылов В. В. Расследование преступлений в сфере компьютерной информации: учебное пособие/В.В.Крылов. – М., 2012. – 615 с.

24. Маляров А.И. Объект преступления в сфере электронно– цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт)/А.И. Маляров. – Общество и право, 2008. – № 2. – 25 с.

25. Никифоров И., Уголовные меры борьбы с компьютерной преступностью: учебное пособие/И. Никифоров. – Защита информации, 2010. – № 5. – 230с.

26. Номоконов В.А. Новые информационные технологии в борьбе с преступностью/В.А. Номоконов. – Российский криминологический взгляд, 2012. – № 1. – 94 с.

27. Селяков Н. А., Градицкая Н. С. Мошенничество в сфере компьютерной информации // Уголовная политика, уголовное законодательство: правоприменительная практика: сборник научных статей. Спб.: СпбГЭУ, 2016.– 215с.

28. Сенченко П.П. Основные способы хищений с использованием банковских платежных карт // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2014.– № 2 (30). – 499с.

29. Тищенко В.И. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. – 352 с.

30. Хохлова О.М. Общественное согласие в социально– политической сфере современного общества: монография. – Красноярск: СФУ, 2016. – 255с.

31. Шмонин А.В. Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания: // А.В. Шомин/ Информатизация и информационная безопасность правоохранительных органов». М., 2014.– 210 с.

32. Яблоков Н. П. Криминалистика: учебник. –М.: ЛексЭст, 2016; Киберпреступность: понятие, состояние, уголовно– правовые меры борьбы. – Москва, 2016. – 168с.

Диссертации и авторефераты

33. Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. канд. юрид. наук. – Н. Новгород, 2010. – 200 с.

34. Дикова Н.И. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем :автореф. дис. канд. юрид. наук. – С., 2011.– 18– 29 с.

35. Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. канд. юрид. наук: 12.00.08. – М., 2012. – 207 с

Судебная практика

36. Приговор по делу № 1– 25/2017 // Архив Октябрьского районного суда г. Томска

37. Приговор по делу № 1– 64/9– 2014г.// Архив Кировского районного суда г. Курска.

38. Приговор по делу № 1– 188/2015 // Архив Братского городского суда Иркутской области.

39. Приговор по делу №1– 251/6/2013 // Архив Нижегородского районного суда г. Н.Новгорода.

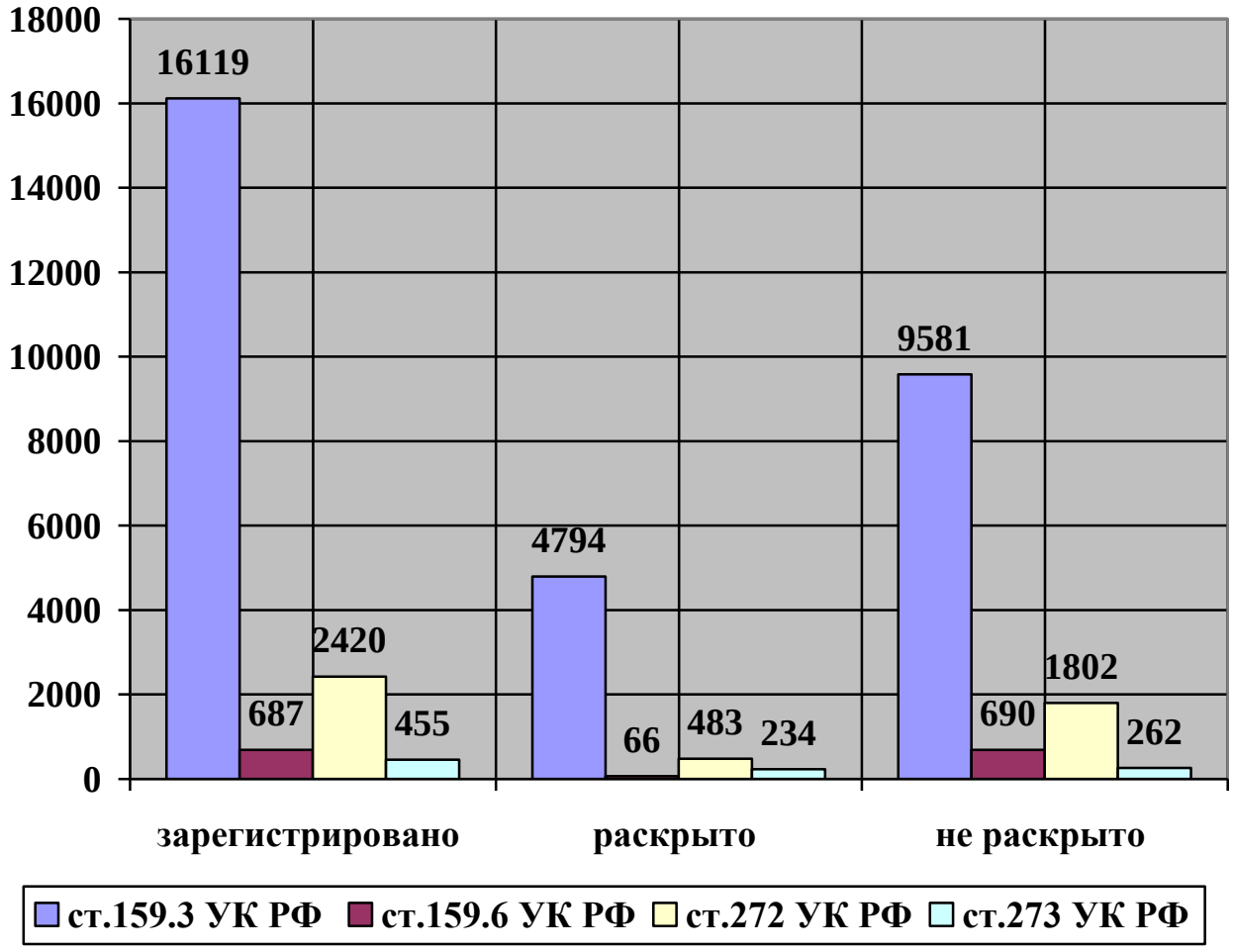
Информационные ресурсы:

40. http://www.mvd.ru/userfiles/file/2012/ban/mart/sb_1207.pdf
41. http://mvd.ru/presscenter/statistics/reports/item/804701/
42. http://mvd.tatarstan.ru/rus/index.htm/news/156697.htm
43. http://www.symantec.com/ru/ru/security
44. http://www.group– ib.ru/list/1008

ПРИЛОЖЕНИЯ

Приложение №1.

Состояние преступности за 2019 г.



АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

Казанский юридический институт МВД России

СПРАВКА

о результатах проверки текстового документа на наличие заимствований

Проверка выполнена в системе Антиплагиат.ВУЗ

Автор работы	**Серебренников Николай Петрович**
Подразделение	
Тип работы	Выпускная квалификационная работа
Название работы	ВКР-Н.Серебренников
Название файла	ВКР-Н.Серебренников.docx
Процент заимствования	**25.22 %**
Процент самоцитирования	**0.00 %**
Процент цитирования	**24.17 %**
Процент оригинальности	**50.61 %**
Дата проверки	**10:36:11 12 июня 2020г.**
Модули поиска	Модуль поиска ИПС "Адилет"; Модуль выделения библиографических записей; Сводная коллекция ЭБС; Коллекция РГБ; Цитирование; Модуль поиска переводных заимствований; Модуль поиска переводных заимствований по elibrary (EnRu); Модуль поиска переводных заимствований по интернет (EnRu); Коллекция eLIBRARY.RU; Коллекция ГАРАНТ; Модуль поиска Интернет; Коллекция Медицина; Сводная коллекция вузов МВД; Коллекция Патенты; Модуль поиска общеупотребительных выражений; Кольцо вузов
Работу проверил	Музеев Айдар Иршатович
	ФИО проверяющего
Дата подписи	
	Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

Отзыв
о ходе выполнения выпускной квалификационной работы слушателем 051 учебной группы Серебренниковым Николаем Петровичем на тему «Тактика ОРД по раскрытию мошенничеств, связанных с использованием компьютерных и информационных технологий»

Данная тема выбрана автором из списка тем, предложенных кафедрой. Серебренников Н.П. проявил заинтересованность к данной тематике, изучал данную проблему с различных позиций. Были подготовлены тезисы выступлений на научных форумах.

Автором обработано достаточно большое количество научного материала, на хорошем теоретическом и методологическом уровне проведено исследование особенностей тактики оперативно-розыскной деятельности ОВД по раскрытию мошенничества, совершаемого с использованием средств электронных расчетов и иными способами, связанными с применением высоких технологий. Материал в выпускной квалификационной работе изложен с соблюдением внутренней логики, между разделами прослеживается логическая взаимосвязь.

Правильно поставленные цель и задачи помогли автору работы четко выстроить логическую цепочку исследования и всесторонне изучить объект и предмет исследования, характер профессиональной деятельности субъектов оперативно-розыскной деятельности ОВД.

Автор активно использовал эмпирический материал по теме исследования, тем самым показав достаточные навыки работы с материалами оперативно-розыскной и следственно-судебной практики. Всегда прислушивался к рекомендациям и корректировкам руководителя, своевременно исправляла замечания.

В работе использованы последние данные статистики, которые еще раз делают акцент на актуальность темы.

Выводы и умозаключения, полученные в результате проведения автором собственного авторского исследования, логически обоснованы и опираются на правоохранительную практику.

Решение поставленных автором задач проходило на хорошем теоретическом уровне и сопровождалось творческим анализом литературы, научных и учебных статей правовой тематики, а также рядом других достоверных источников. Автором изучен достаточный объем специальной литературы.

Тема работы раскрыта полностью и всесторонне. Содержание и структура изложения материала говорит о достаточной подготовленности и необходимой теоретической базе слушателя и его склонности к самостоятельной работе по обучаемой специальности.

Слушатель Серебренников Н.П. показал уверенные навыки владения компьютерными методами сбора, хранения и обработки информации,

применяемой в сфере профессиональной деятельности, умение и навыки работы с компьютерными программами (Word, PowerPoint, Excel), информационно-справочными ресурсами, работы в системе Интернет.

Тема работы раскрыта полностью и всесторонне. Содержание и структура изложения материала говорит о достаточной подготовленности и необходимой теоретической базе автора и его склонности к самостоятельной работе по обучаемой специальности.

В заключении необходимо добавить, что в ходе выполнения выпускной квалификационной работы Н.П. Серебренников сформировал о себе мнение, как подготовленном к работе в оперативных подразделениях сотруднике, ставящим конкретные и реальные цели и стремящимся к их исполнению.

В целом работа выполнена на высоком квалификационном уровне, допускается к защите и заслуживает оценки «отлично».

Научный руководитель

кандидат юридических наук, доцент
доцент кафедры ОРД КЮИ МВД России

полковник полиции А. И. Музеев

"28" июня 2020 г.

С отзывом ознакомлен: _____ Н.П. Серебренников.
(подпись)

РЕЦЕНЗИЯ
На выпускную квалификационную работу

слушателя 051 учебной группы
Серебренникова Николая Петровича
на тему: «Тактика ОРД по раскрытию мошенничеств связанных с использованием компьютерных и информационных технологий»

Выпускная квалификационная работа слушателя Серебренникова Н.П. выполненная на тему: «Тактика ОРД по раскрытию мошенничеств связанных с использованием компьютерных и информационных технологий», является актуальной, поскольку в данный момент совершается большое количество мошенничеств связанных в сфере высоких технологий, преступники используют новые способы хищения денежных средств.

Поставленные цели и задачи полностью соответствуют теме исследования. Работа полностью раскрыта и опирается на современные статические данные и статьи ученных, авторитетных в данной области.

Основные вопросы выпускной квалификационной работы полно, глубоко проработаны. Слушатель Серебренников Н.П. умело предлагает варианты решения поставленных задач. Предлагаемые решения основываются на проведенном анализе и в исследовании форм использования специальных знаний при раскрытии мошенничеств связанных с использованием компьютерных и информационных технологий.

Выпускная квалификационная работа состоит из введения, двух глав, заключения, списка использованной литературы и приложений. После каждой главы содержатся четкие выводы, тем самым показывая достаточный научный уровень и степень освещенности вопросов выбранной темы. Материалы работы изложены с соблюдением внутренней логики, между разделами имеется логическая взаимосвязь. Вся работа выполнена на основании научной литературы, нормативно-правовой базы, материалов судебно – следственной практики, профессиональной направленности и практических знаний.

Слушателем Серебренниковым Н.П. в ходе прохождения производственной (преддипломной) практики в отделе уголовного розыска УМВД России по г.Ижевску, были изучены дела оперативного учета находящиеся в архиве УМВД России по г.Ижевску. Также слушатель активно взаимодействовал с сотрудником подразделения и полученные знания активно применил при написании выпускной квалификационной работы.

Слушатель Серебренников Н.П. показал отличный уровень владения теоретической базой по выбранной теме исследования, способность формулировать собственную точку зрения на основе анализа мнений разных ученных в этой области, а также на основе изученных материалов в ходе прохождения преддипломной практики.

Оформление выпускной квалификационной работы осуществлено в соответствии с предъявленными требованиями, библиография составлена верно и является актуальной для анализа данной темы.

Существенных недостатков в работе не выявлено. В целом работа оставляет положительные впечатления, соответствует всем предъявляемым требованиям.

Выпускная квалификационная работа Серебренникова Н.П. представляет собой самостоятельное исследование и заслуживает оценки «отлично».

Оценка рецензента отлично

Рецензент

Начальник отдела уголовного розыска УМВД России
по г.Ижевску
майор полиции
Брыляков Вячеслав Николаевич

«01» 06 2020г.

С рецензией ознакомлен(а) _____ Н.П. Серебренников.
(подпись) (инициалы, фамилия обучающегося)

«01» 06 2020г.