МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»
(КЮИ МВД России)

Кафедра оперативно-разыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: **ВЫЯВЛЕНИЕ И ДОКУМЕНТИРОВАНИЕ С ПОМОЩЬЮ ОРД ОВД ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОГО БАНКИНГА**

Выполнил: **Кувина Екатерина Владимировна**
слушатель группы №042 факультета
по подготовке специалистов по программам
высшего образования КЮИ МВД России,
обучающейся по специальности 40.05.02 -
Правоохранительная деятельность,
2014 года набора

Руководитель: начальник кафедры оперативно- разыскной
деятельности КЮИ МВД России
полковник полиции Е.П. Шляхтин

Рецензент: начальник МО МВД России «Алатырский»
полковник полиции А.В. Боголюбов

К защите _____
Начальник кафедры ОРД _____Е.П. Шляхтин

Дата защиты: «___» _____ 2019 г. Оценка _____

Казань – 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Повсеместное внедрение информационно-телекоммуникационных технологий и информационых систем создало новые, уникальные возможности для активного и эффективного развития экономики и политики, государства, общества, граждан. На заседании Совета по стратегическому развитию и приоритетным проектам, Президент РФ В.В. Путин заявил, что «…формирование цифровой экономики – это вопрос национальной безопасности и независимости России, конкуренции отчественных компаний». Так, финансово-кредитные учреждения пытаются оптимизировать средства, в том числе и за счет миграции традиционных банковских услуг в дистанционные каналы обслуживания. Однако, распространение технологий несет не только позитивные, но и негативные последствия, такие как рост киберпреступлений.

Среди наиболее распространенных киберпреступлений в настоящее время следует назвать хищения денежных средств, совершаемых с использованием компьютерных технологий. Согласно данным официальной статистики МВД России, в 2018 году было зарегистрировано на 12,6% больше преступлений экономической направленности, совершенных с использованием компьютерных и телекоммуникационных технологий, соотвественно, 9,7 тысяч против 8,6 тысяч вышеуказанных противоправных деяний, зафиксированных по итогам 12 месяцев 2017 года.

Актуальность исследования главным образом обусловлена и подчеркнута необходимостью интенсификации тактики оперативно-розыскной деятельности ОВД по выявления и документированию относительно новых, технически и организационно сложных преступлений - хищений денежных средств с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, распространяемых в сети Интернет.

Выявление и документирование преступлений, совершаемых с ипользованием электронного банкинга представляет значительные трудности

для правоприменителей. Об этом свидетельствуют опросы практических сотрудников и изучение соответствующих материалов уголовных дел, дел оперативного и иного учета.

Практическая значимость заключается в том, что большинство преступлений, совершаемых с использованием электронного банкинга, обладают высокой степенью латентности, при чем для данных противоправных деяний одинаково характерны как естественная, так и искусственная латентность. Сокрытие преступлений от учета исключает уголовное преследование и, соответственно, препятствует реализации принципа неотвратимости наказания, а значит лица, их совершающие, не несут ответственность предусмотренную законодательством Российской Федерации. Что, в свою очередь, требует выработки новых тактических рекомендаций по оперативно-розыскному выявлению и документированию подобных видов преступлений.

Взаимосвязь с правоохранительными органами. Расследование преступлений, совершаемых с использованием электронного банкинга, осуществляется следователями территориальных и иных органов МВД России[1], так как подобные преступления подследственны именно этому ведомству. Кроме того, большинство данных преступлений раскрываются не без помощи сотрудников экспертно-криминалистических подразделений ОВД (проведение различного рода исследований и экспертиз возложено именно на это подразделение), участковых уполномоченных полиции и многих других подразделений и служб органов внутренних дел.

Анализ соответствующей оперативно-розыскной и следственно-судебной практики свидетельствует, что лица, совершающие вышеуказанные преступления, прекрасно осведомлены о возможных последствиях своей противоправной деятельности, и, как правило, желают их скорейшего наступления. Все вышеуказанное требует комплексного подхода к решению указанных проблем, в том числе с применением оперативно-розыскных сил,

[1] Далее – орган(ы) внутренних дел и (или) ОВД.

средств и методов и обуславливает необходимость исследования вопросов, связанных с совершенствованием организации и тактики оперативно-розыскной деятельности в этом направлении.

В последнее время вопросам противодействия преступлениям, связанных с хищениями денежных средств с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, в том числе и с помощью оперативно-розыскной деятельности органов внутренних дел, уделяется определенное внимание. Различные аспекты оперативно-розыскных проблем борьбы с преступлениями, в том числе и вышеуказанной категории, освещались в работах Б.В. Андреева, Р.С. Атаманова, В.Н. Бурлакова В.Б. Вехова, Е.Г. Гудзь, В.А. Голубева, М.Ю. Дворецкого, Б.Д. Завидова, А.Е. Шалагина, Н.Р. Шевко и др.

Уголовно-правовые, криминологические, оперативно-розыскные и иные аспекты вышеуказанных форм хищений чужого имущества стали предметом ряда диссертационных исследований (В.В. Воробьев, Н.И. Дикова, Т.П. Кесареева и др.).

В то же время проблема оперативно-розыскного выявления и документирования преступлений вышеуказанной направленности должным образом не исследовалась, в связи с чем по этому направлению деятельности органов внутренних дел отсутствует необходимое количество методических материалов, чем и обусловлен выбор темы и актуальность ее исследования.

Цель и основные задачи исследования. Целью выпускной квалификационной работы является разработка комплексных научно обоснованных предложений и практических рекомендаций по совершенствованию организационных и тактических основ оперативно-розыскной деятельности органов внутренних дел по выявлению и документированию преступлений, связанных с хищениями денежных средств с банковских счетов, а также электронных денежных средств,

совершаемых с использованием специализированных вредоносных компьютерных программ.

В соответствии с поставленной целью определен круг взаимосвязанных **задач,** теоретическое решение которых составляет содержание настоящего исследования. К ним относятся:

- Понятие и сущность преступлений, совершенных с использованием электронного банкинга.
- Оперативно – розыскная характеристика преступлений, совершенных использованием электронного банкинга.
- Динамика развития преступлений, совершенных с использованием электронного банкинга.
- Особенности выявления преступлений, совершенных с использованием электронного банкинга.
- Особенности оперативного документирования преступлений, совершенных с использованием электронного банкинга.
- Взаимодействие правоохранительных органов и служб безопасности банков при выявлении и документировании преступлений, совершенных с использованием электронного банкинга.

Объект и предмет исследования. Объектом исследования является оперативно-розыскная деятельность органов внутренних дел по выявлению и раскрытию преступлений связанных с хищениями денежных средств с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ.

Предмет исследования составляют тенденции и особенности вышеуказанных преступлений, связанных с хищениями денежных средств с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, их оперативно-розыскная и иная характеристика, организационные и тактические аспекты деятельности оперативных

подразделений полиции по выявлению и документированию рассматриваемых преступлений.

Методология и методика исследования. Методологической основой исследования является диалектический метод познания явлений и процессов реальной действительности, рассматривающий их в постоянном изменении, развитии, тесной взаимосвязи и взаимозависимости.

В процессе исследования предполагается использовать совокупность таких общенаучных методов исследования, как сравнение, анализ, синтез, а также формально-логический, сравнительно-правовой и другие частнонаучные методы, включая:

- статистический (при анализе данных о распространенности рассматриваемых деяний);
- конкретно-социологических исследований (при изучении уголовных дел, дел оперативного и иного учета, материалов первоначальной оперативной проверки и др.);
- контент-анализа (при изучении специальной литературы, законодательства и аналитических материалов).

В качестве нормативной базы будет использоваться Конституция Российской Федерации, действующее уголовное, уголовно-процессуальное, оперативно-розыскное законодательство, указы Президента РФ, постановления Правительства Российской Федерации, а также ведомственные нормативные правовые акты МВД Российской Федерации.

Теоретической основой исследования станут труды ученых в области теории оперативно-розыскной деятельности, криминалистики, уголовного, уголовно-процессуального права и других отраслей наук.

Эмпирическую базу исследования составят статистические данные МВД РФ, аналитические материалы ГУУР МВД России, МВД по республикам, ГУ (У) МВД России по иным субъектам Российской Федерации, результаты экспертных исследований, технические ориентировки, решения коллегий, указания, рекомендации МВД Российской

Федерации, материалы научно-практических конференций, относящиеся к теме исследования и др.

Научная новизна настоящей работы определяется комплексным подходом к рассмотрению проблемы законодательного регулирования противодействия вышеуказанным преступлениям, оперативно-розыскных и иных мер по их выявлению, предупреждению и раскрытию, повышение эффективности оперативно-розыскной деятельности оперативных подразделений полиции по борьбе с подобными противоправными деяниями. Положения настоящего исследования могут быть учтены при совершенствовании законодательства Российской Федерации, а также ведомственных нормативных актов.

Структурно выпускная квалификационная работа состоит из введения, двух глав, заключения, списка использованных источников и литературы.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОГО БАНКИНГА

§1.1. Понятие и сущность преступлений, совершенных с использованием электронного банкинга.

Развитие информационных технологий в России, как и во всем мире, обусловило расширение сфер применения мобильных платежей, интернет-банкинга с подтверждением транзакций по SMS, SMS-банкингу и банковским мобильным приложениям в повседневной жизни.

Среди наиболее актуальных тенденций в развитии банковских технологий почетное место занимает активное внедрение новых платформ электронного банкинга. При этом быстрое развитие таких технологий создает предпосылки для их использования в преступных целях.

Электронный банкинг – это деятельность банка по предоставлению комплекса услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей[2]. На сегодняшний день банки предлагают достаточно широкий спектр услуг, объединенных общим термином – дистанционное банковское обслуживание[3]. С точки зрения способов оказания услуг ДБО выделяют следующие его виды:

- классический банк-клиент;
- интернет-банкинг;
- мобильный банкинг;
- внешние сервисы (с использованием киосков, банкоматов, АТМ).

Классический банк – клиент представляет собой информационную систему, используемую для осуществления банковских операций, доступ к которой осуществляется через персональный компьютер. Для использования

---

[2] Гончар, В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий / В.В. Гончар // Вестник экономической безопасности, 2017. № 3. – С. 78-81.
[3] Далее – ДБО.

системы данного типа на персональном компьютере клиента устанавливается отдельная программа, которая хранит все данные (платежные документы, выписки по счетам) на компьютере клиента.

Интернет-банкинг — комплекс средств для управления банковскими счетами через Интернет. Операции производятся через сайт самого банка, на который можно зайти, используя стандартный интернет-браузер (Microsoft Internet Explorer, Mozilla Fire Fox и т. п.)[4].

Современный мобильный банкинг - это интернет-банкинг, но с разницей в том, что для его использования необходимо специальное приложение на телекоммуникационном устройстве (мобильном устройстве), а для интернет-банкинга достаточно интернет-браузера на портативном компьютере или ноутбуке. Мобильный банкинг представляет собой выполнение операций через смартфоны. Еще в 2012 году для клиентов стали доступны мобильные приложения на популярных платформах iOS, Android и WindowsPhone 7. Число клиентов, которые готовы обслуживаться через Интернет и мобильный телефон, растет благодаря повышению качества интернет-связи во всех регионах России[5].

В последнее время хищения денежных средств через системы ДБО, из банкоматов и с их использованием, путем несанкционированного входа в компьютерную систему кредитных организаций либо использования сбоев в ее работе стали острой проблемой для большинства банков и их клиентов.

В 2018 году правоохранительными органами было выявлено на 12,6 % больше, чем в предыдущем, самых прибыльных киберпреступлений – интернет-мошенничеств и хищений денежных средств из систем ДБО, а также со счетов физических лиц в банках: 9,7 тыс. против 8,7 тыс. в 2017 году. Эксперты отмечают, что системы ДБО наиболее часто подвергаются кибератакам. В 2017 году в Банк России была представлена информация о

---

[4] Дикова, Н. В. Квалификация преступлений, совершаемых с использованием электронных платежных средств и систем / Н.В. Дикова // Актуальные проблемы истории и права: сборник статей.– Оренбург: ОГИМ, 2011. – Вып. 2. – С. 170-177.

[5] Пойманова, Л. А. Мошенничество в банковской сфере: понятие, признаки, виды / Л.А. Пойманова // Государство и право. Юридические науки. - 2018. - № 2. – С. 67.

841 несанкционированной операции со счетов юридических лиц с использованием систем ДБО на общую сумму 1,57 млрд рублей.

В соответствии с федеральным законодательством, противоправные действия злоумышленников, направленные на хищение денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, попадают под признаки состава преступления, предусмотренного статьей 159.6 УК РФ[6].

Данная статья была введена в действие федеральным законом от 29 ноября 2012 года № 207 – ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[7]. Федеральный закон от 23 апреля 2018 года № 111 – ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[8] дополнил часть 3 статью 159.6 УК РФ пунктом «в», который предусматривает уголовную ответственность за мошеннические действия в сфере компьютерной информации, совершенные с банковского счета, а равно в отношении электронных денежных средств.

Статья 159.6 УК РФ криминализирует «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». В профессиональном сообществе это нововведение вызвало в основном положительные отзывы.

Согласно Постановлению Пленума Верховного Суда РФ от 30.11.2017

---

[6] Третьяк, М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М.И. Третьяк // Законность. 2016. № 7. – С. 54-56.

[7] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 29.11.2012 № 207-ФЗ (в ред. от 03.07.2016) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

[8] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 23.04.2018 №111-ФЗ (в ред. от 23.04.2018) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

№ 48 "О судебной практике по делам о мошенничестве, присвоении и растрате"[9], под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. До вступления в силу указанного выше постановления Пленума Верхового суда РФ, в практической деятельности правоохранительных органов отмечались и некоторые недостатки новой статьи УК РФ. В частности, возникновение конкуренции норм со ст. 272 УК РФ, которой предусмотрен «причинивший крупный ущерб или совершенный из корыстной заинтересованности» «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование компьютерной информации».

Диспозиция ст. 159.6 УК РФ предусматривает дополнительные способы совершения преступления, такие как «ввод» компьютерной информации и «иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или «информационно-телекоммуникационных сетей». Кроме того, обеспечивается дифференциация уголовной ответственности за счет введения большего количества квалифицирующих признаков, предусмотренных частями 2-4 статьи 159.6 УК РФ.

---

[9] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (в ред. от 30.11.2017) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

В настоящее время 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 статье 272, 273 или 274.1 УК РФ.

Санкции ч. 1 и 2 ст. 272 УК РФ строже, нежели санкция ч. 1 ст. 159.6 УК РФ. Более того, крупным ущербом в ст. 272 УК РФ, согласно примечанию, признается ущерб, сумма которого превышает один млн. руб.

В квалифицированных составах ст. 159.6 УК РФ (ч.3 и 4) предусматривается совершение преступлений в крупном и особо крупном размерах. Согласно примечанию к ст. 159.1 УК РФ, крупным размером признается стоимость имущества, превышающая один миллион пятьсот тысяч руб., а особо крупным — шесть миллионов рублей.

В результате введения ст. 159.6 УК РФ фактически произошло снижение ответственности для наиболее опасной и квалифицированной части преступников, прежде всего, из числа профессиональных и организованных. На практике это привело к переквалификации ряда уголовных дел в начале 2013 года и даже в некоторых случаях к вынужденному изменению мер пресечения обвиняемым и осужденным на не связанные с лишением или ограничением свободы.

Сейчас статья 159.6 УК РФ более всего подходит для квалификации хищений, совершаемых с использованием вредоносных компьютерных программ. Российский законодатель явно отделил мошенничества в сфере компьютерной информации, сопряженные с воздействием на нее, от иных случаев мошенничества, в которых средства обработки компьютерной информации используются только в качестве вспомогательных средств совершения преступлений. Разумеется, перечисленные в диспозиции ст. 159.6 УК РФ манипуляции с компьютерной информацией возможны не только при использовании вредоносных компьютерных программ для совершения хищений в системах дистанционного банковского

обслуживания. Однако, учитывая относительную редкость нетипичных преступлений и устойчивый рост числа типовых хищений, необходимо полагать, что статистика по данной статье отображает в большей части именно интересующие нас хищения[10].

В заключении необходимо отметить, что среди наиболее актуальных тенденций развития банковских технологий почетное место занимает электронный банкинг, что в свою очередь делает его объектом преступных посягательств. Противоправные действия злоумышленников, направленные на хищение денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, попадают под признаки состава преступления, предусмотренного статьей 159.6 УК РФ. 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 статье 272, 273 или 274.1 УК РФ, которую необходимо знать и учитывать при планировании и осуществлении конкретных оперативно-розыскных мероприятий и следственных действий, проводимых в целях их выявления и документирования.

§1.2. Оперативно – розыскная характеристика преступлений, совершенных использованием электронного банкинга.

В современных условиях развития информационных технологий большую опасность представляют так называемые интеллектуальные преступники, которые используют в своей деятельности достижения современных технологий.

[10] Колычева, А. Н. К вопросу об использовании ресурсов сети Интернет в преступной деятельности / А.Н. Колычева // Российский следователь. 2016. - № 24. – С.48-52.

Подобные деяния представляют повышенную общественную опасность. Это обусловлено трансграничным характером используемых при их совершении сетевых ресурсов; изменчивостью и скоростью уничтожения цифровой информации; высоким уровнем латентности, при чем для данных преступлений одинаково характерны как естественная, так и искусственная латентность. Так же данные преступления являются обезличенными: достаточно сложно вычислить виновного в совершении преступления, так как интернет гарантирует анонимность. В связи с этим, поиск первоисточника становится достаточно трудозатратным процессом.

Для успешного расследования подобных преступлений требуется своевременное, оперативное установление следов совершенного преступления и их надлежащее закрепление, что зачастую связано с необходимостью анализа значительных массивов информации.

Как уже ранее было отмечено, противоправные действия злоумышленников, направленные на хищение денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, попадают под признаки состава преступления, предусмотренного статьей 159.6 УК РФ.

Нами был проведен анализ открытых статистических данных, экспертных оценок и результатов оперативно-следственной деятельности органов внутренних дел, который позволил обозначить четкую картину оперативной обстановки по данной линии преступлений.

На Центральный банк Российской Федерации сравнительно недавно была возложена обязанность сбора статистических данных об инцидентах в области информационной безопасности при осуществлении переводов денежных средств. Согласно указанию ЦБ РФ от 9 июня 2012 г. № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных

средств»[11], операторы обязаны предоставлять в ЦБ России ежемесячно отчетность по двум формам:

- форме 0409258 «Сведения о несанкционированных операциях, совершенных с использованием платежных карт»,
- форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

На основе сведений, представленных в Банк России в рамках указанных форм отчетности, Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее - ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка России был подготовлен обзор несанкционированных операций за 2017 год.

По данным Банка России об операциях, совершенных на территории Российской Федерации и за ее пределами с использованием платежных карт , эмитированных на территории Российской Федерации, количество и объем соответствующих операций неизменно увеличиваются. Рост показателей 2017 г. составил около 25% относительно аналогичных значений за 2016 год[12].

Объем всех несанкционированных операций, совершенных с использованием платежных карт в 2017 г., составил 961,3 млн рублей. Основную долю в разрезах объема и количества несанкционированных операций составляют CNP–транзакции (операция, осуществленная в сети Интернет с использованием реквизитов платежной карты).

На сегодняшний день формой отчетности 0403203 предусмотрены следующие возможные причины несанкционированных операций:

---

[11] Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств : указание ЦБ РФ от 9 июня 2012 г. № 2831-У (в ред. от 30.03.2018) [Электронный ресурс] // Доступ из справочной правовой системы «Гарант» (дата обращения: 12.04.2019).

[12] Центральный банк Российской Федерации [Электронный ресурс]. — Режим доступа. — URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet007.htm&pid=psRF&sid=ITM_12859 (дата обращения 20.03.2019).

- использование электронного средства платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности;
- нарушение клиентом порядка использования электронного средства платежа;
- побуждение владельца электронного средства платежа к совершению операции путем обмана или злоупотребления доверием;
- воздействие вредоносного кода и так далее.

В качестве причины возникновения большей части несанкционированных операций (более 90%) отчитывающимися операторами указывается использование электронного средства платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности и аутентификационной информации.

Стоит отметить, что отчитывающиеся операторы при указании причины несанкционированной операции основываются на данных, представленных клиентом в заявлении. С учетом использования отчитывающимися операторами различных технологий для дополнительных проверок права пользования платежной картой причина «использование электронного средства платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности» в большинстве случаев может быть сведена к воздействию вредоносного кода или побуждению владельца электронного средства платежа к совершению операции путем обмана или злоупотребления доверием[13].

По 97% несанкционированных операций с использованием платежных карт отсутствуют сведения о направлении информации в

[13] Саблина, Т. И., Никитенко, И. В. Мошенничество с использованием платежных карт: вопросы теории, законодательства и практики его применения / Т.И. Саблина, И.В. Никитенко // Молодой ученый. — 2017. — №48. — С. 274-276.

правоохранительные органы или соответствующая информация не направлялась[14].

На долю несанкционированных операций, совершенных за пределами Российской Федерации, приходится 40% от количества и 44% от объема всех несанкционированных операций. Нахождение злоумышленника вне российской юрисдикции существенно затрудняет его привлечение к ответственности российскими правоохранительными органами.

В 2017 году в Банк России была представлена информация о 841 несанкционированной операции со счетов юридических лиц с использованием систем ДБО на общую сумму 1,57 млрд рублей[15].

Объемы операций со счетов юридических лиц значительно превышают аналогичные значения для операций с использованием платежных карт как по абсолютным показателям, так и в рамках отдельных операций. Если для осуществления несанкционированной операции с использованием платежной карты злоумышленники вынуждены учитывать максимальные размеры суммы операции (лимиты на операции со счета, установленные банком или клиентом), то при проведении подобной операции со счетов юридических лиц злоумышленники для успешного ее осуществления в лучшем случае вынуждены имитировать модель операций юридического лица, а в худшем – ограничены только количеством денежных средств на банковском счете юридического лица. Таким образом, для несанкционированных операций со счетов юридических лиц формируется особенность в виде больших сумм каждой несанкционированной операции в отдельности.

Основное количество несанкционированных операций приходится на сегмент от 100 тыс. до 10 млн рублей.

Причинами осуществления несанкционированных операций со счетов юридических лиц являются, в частности, нарушение порядка использования

---

[14] Киберпреступники за 2017 год нанесли 1,3 млрд ущерба банковской сфере РФ [Электронный ресурс] // Режим доступа: https://regnum.ru/news/2381125.html.

[15] Центробанк сообщил о 40 млн рублей хищений из банкоматов [Электронный ресурс] // Режим доступа: https://лига-закон.рф/main/16248-centrobank-soobschil-o-40-mln-rubley-hischeniy-iz-bankomatov.html

электронного средства платежа и использование электронного средства платежа без согласия клиента. С учетом того, что юридические лица в основном осуществляют операции через системы ДБО со стационарных компьютеров, причины, указываемые отчитывающимися операторами, в большинстве случаев могут быть сведены к воздействию вредоносного кода.

При несанкционированных операциях со счетов юридических лиц операторы по переводу денежных средств и операторы услуг платежной инфраструктуры обладают большим объемом (по каждой третьей несанкционированной операции) данных о факте обращения в правоохранительные органы, чем в случае подобных операций с использованием платежных карт (по каждой 20-й несанкционированной операции)[16].

Стоит отметить, что, не обращаясь в правоохранительные органы и не требуя от государства принятия предусмотренных законом мер, занимая тем самым пассивную позицию, пострадавшие сами фактически оправдывают действия злоумышленников, формируют иллюзию их безнаказанности и провоцируют их дальнейшую активность.

В отсутствие сведений о действиях злоумышленников правоохранительные органы не имеют возможности их раскрыть. Злоумышленники совершают не единичную несанкционированную операцию, а занимаются этим зачастую на постоянной основе, оставляя за собой многочисленные следы. Поэтому обращение в правоохранительные органы имеет смысл для того, чтобы в будущем, когда преступный путь злоумышленника будет все-таки прерван, были бы правовые основания для его привлечения к ответственности за все прошлые несанкционированные операции[17].

---

[16] По следам CyberCrimeCon 2017: Тенденции и развитие высокотехнологичной преступности [Электронный ресурс] // Режим доступа: https://habr.com/ru/company/group-ib/blog/341812/ (дата обращения: 23.04.2019).

[17] Яни, П. Специальные виды мошенничества / П. Яни // Законность. 2015. - № 5. – С.18.

Согласно результатам интервьюирования оперативных работников следует, что следственными органами возбуждаются уголовные дела не более чем по одному из примерно двадцати сообщений о хищениях денежных средств с банковских счетов или из электронных кошельков. Однако и сами заявления, по мнению оперативных работников, подавались не более чем в половине случаев хищений денежных средств со счетов юридических лиц и не более чем в 1 из 3-5 случаев хищений денежных средств со счетов физических лиц.

В типовом случае обращения потерпевшего по факту хищения в правоохранительные органы в заявлении сообщается только о несанкционированном переводе денежных средств на неизвестный потерпевшему счет (или счета). Поскольку такие преступления происходят в условиях почти полной неочевидности, факт использования вредоносных компьютерных программ и несанкционированного доступа к электронным средствам платежа на момент обнаружения хищения, как правило, не может быть подтвержден. В случае успешного совершения хищения и применения злоумышленником достаточных средств и методов удаления или сокрытия следов — это событие однозначно выглядит как преступление только с точки зрения бывшего владельца похищенных средств. Причем сам владелец денежных средств обычно не понимает, каким именно способом совершено преступление[18].

Отсутствие осведомленности и правильного криминалистического определения ситуации, а также выработанного унифицированного подхода к проведению комплекса первоначальных проверочных мероприятий приводит к ошибочному выбору тактики раскрытия, выполнению тех или иных безрезультатных действий и, следовательно, к затягиванию процессуальных сроков рассмотрения сообщении о преступлениях». К сказанному остается добавить, что во многих случаях факт совершения хищения с

[18] Кушниренко, С. П. Преступления в сфере высоких информационно-телекоммуникационных технологий: анализ региональной судебно-следственной практики / С.П. Кушниренко // Библиотека криминалиста. Научный журнал. М.: Юрлитинформ. 2013. - № 5 (10). – С. 32.

использованием именно вредоносных компьютерных программ так и остается неизвестным как для сотрудников оперативных и иных подразделений органов внутренних дел, так и для самих владельцев денежных средств, что исключает возможность установления и привлечения всех виновных лиц к уголовной ответственности.

Основные доказательства использования вредоносной программы, а также «неправомерного доступа к охраняемой законом компьютерной информации» (с декабря 2012 г. — «ввода, удаления, блокирования, модификация компьютерной информации») находятся на компьютере или мобильном устройстве потерпевшего. Подтвердить указанные факты возможно только в результате сложного криминалистического исследования, которое провести на этапе предварительной оперативной проверки сообщения о подобном преступлении весьма затруднительно.

Обратимся к примеру. В одно из территориальных оперативно-технических подразделений по линии «К» поступила информация о появлении на территории Российской Федерации нового вида вредоносного программного обеспечения — «Faketoken.b-ruStels2» целью которого являются устройства, работающие на платформе «Android».

В результате проведения комплекса оперативно-розыскных и иных мероприятий, таких как, ОРМ «Снятие информации с технических каналов связи», «Наведение справок» и некоторых других, оперативникам удалось не только оперативным путем выявить участников преступной группы, в которую входило семь человек[19], но провести требуемое оперативно-розыскное документирование фактов их преступной деятельности, а также привлечь их к соответствующей уголовной ответственности. В ходе ОРМ было установлен примерный алгоритм преступных действий злоумышленников. Например, программу, которую они использовали после установки на устройство, запрашивала баланс привязанной к номеру

[19] Уязвимости мобильного Сбербанка обошлись в 5 млн рублей [Электронный ресурс] // Режим доступа: https://ib-bank.ru/news/4734 (дата обращения: 23.04.2019).

банковской карты, скрывала поступающие уведомления и начинала осуществлять переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.

В результате проведенных обысков было изъято значительное количество компьютерной техники со следами распространения в сети Интернет вредоносного программного обеспечения, 25 мобильных телефонов, более 150 сим-карт, электронные носители информации и свыше 100 банковских карт, на которые производилось зачисление похищенных денежных средств.

К сожалению, как показывает практика, не меньшее усердие в уничтожении следов совершения преступлений предпринимают и сами пострадавшие. По наблюдениям опрошенных сотрудников специализированных оперативных подразделений полиции, до половины пострадавших непосредственно сразу после выявления фактов хищений денежных средств (что часто сопровождается выведением из строя компьютеров) самостоятельно или силами сторонних специалистов производят восстановление вышедших из строя компьютеров, их проверку антивирусными программами (с обязательным удалением найденных вредоносных программ). Иногда — полную замену операционных систем, в том числе с переустановкой платежного программного обеспечения (если таковое имеется), и даже замену носителей информации. После этого уже следуют их обращения в правоохранительные органы[20].

В результате при рассмотрении заявлений по фактам совершенных хищений денежных средств правоохранительные органы в большинстве случаев не имеют подтверждений применения вредоносных компьютерных программ и несанкционированного доступа к электронным средствам платежа или их утраты, а, следовательно, и того, что вообще имел место неправомерный и несанкционированный перевод денежных средств.

[20] Рудьман, Д. С. Доступ к банковской тайне органов внутренних дел / Д.С. Рудьман // Информационное право. № 1 (28). - 2012. – С.11.

Предположение о том, что лицо, обратившееся по факту несанкционированного перевода денежных средств, таким способом на самом деле пытается отказаться от собственного легального перевода по каким-либо субъективным причинам, часто является основанием для принятия решения об отказе в возбуждении уголовного дела.

Однако даже если доводы пострадавшего и установленные обстоятельства происшествия оказываются достаточными для принятия решения о возбуждении уголовного дела, возникает проблема квалификации деяния[21].

В качестве вывода по параграфу необходимо отметить, что перспектива возбуждения дела с неопределенной квалификацией и возможной последующей переквалификацией, с отсутствующим или крайне затянувшимся экспертным исследованием, без выявленных лиц, без получателя денежных средств и с весьма слабой в целом перспективой раскрытия воспринимается сотрудниками полиции негативно. Поэтому зачастую на практике используется любая возможность и любые основания для отказа в возбуждении уголовного дела по поступившим заявлениям, что оставляет данные преступления безнаказанными.

Анализ статистических данных, предоставленных Центральным банком Российской Федерации, говорит об увеличение преступлений, совершаемых с использованием инструментов электронного банкинга, что, в свою очередь, требует разработку дополнительных алгоритмов и процедур по применению оперативно-розыскных и иных мероприятий, а также новых методов и способов реагирования.

§1.3. Динамика развития преступлений, совершенных с использованием электронного банкинга

В начале XXI века стало очевидно, что дальнейшее развитие процессов финансовой глобализации будет невозможно представить без

[21] Тактика допроса подозреваемого по преступлениям, совершаемым с использованием интернет-технологий (на примере статьи 272 УК РФ): методические рекомендации. Омск, 2014.

информационно-коммуникационных технологий (далее - ИКТ). Проникнув во все сферы жизни современного общества, они являются их неотъемлемой составляющей и охватывают все ресурсы, обеспечивающие управление информацией, такие как компьютеры, телекоммуникационные сети, программное оборудование и обеспечение.

Динамичное развитие электронных систем и коммуникаций и их повсеместное внедрение способствовало увеличению количества совершаемых в указанных сферах преступлений. При этом большая часть посягательств совершается в сфере дистанционного банковского обслуживания и электронной коммерции, что напрямую влияет на устойчивость экономики государства[22].

В последние годы активное развитие сферы информационно-коммуникационных технологий и внедрение новых цифровых технологий в банковский бизнес привело не только к распространению технологий электронного банкинга, но и к стремительному росту киберпреступлений в кредитно-финансовой сфере. Наиболее негативные последствия связаны с вложением похищенных денежных средств в организацию новых (более масштабных) преступлений с использованием электронных средств платежа, в частности, технологий электронного банкинга[23].

В Российской Федерации число преступлений, совершаемых с применением современных информационно-коммуникационных технологий, с 2013-го по 2016 г. существенно увеличилось. За I полугодие 2017 г. их число выросло на 26% и составило 40 тыс., а ущерб от киберпреступлений за этот же период превысил 18 млн. дол. США.

Согласно сведениям отчета «Тенденции высокотехнологичных преступлений за 2017 год» компании Group-IB1, размер ущерба от хищений в

---

[22] Шмонин, А. В. и др. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий: аналитический обзор / А.В. Шмонин. - М.: Академия управления МВД России, 2015. – С.48-50.

[23] Буцкова, О. И. Особенности проведения доследственной проверки и возбуждения уголовных дел о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи [Текст] / О.И. Буцкова // Право: история, теория, практика: материалы IV Междунар. науч. конф. (г. Санкт-Петербург, июль 2016 г.). — СПб.: Свое издательство, 2016. – С.16-17.

системах интернет-банкинга физических лиц с использованием вредоносных программ за последний год возрос в 2,3 раза, а от хищений в системах мобильного банкинга граждан – в 2,2 раза.

Объем денежных средств, обналиченных в результате похищения, в 2017 г. составил 1,3 млрд. руб. (в 2016 г. – 1,7 млрд руб.). Более подробно сведения о хищениях в результате совершенных киберпреступлений за 2016–2017 гг. представлены в таблице 1.

Указанные выше сведения в целом релевантны официальной статистике Банка России, формируемой на основе обязательных форм отчетности субъектов национальной платежной системы: 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и 0409258 «Сведения о несанкционированных операциях, совершенных с ис- пользованием платежных карт».

Согласно сведениям Обзора несанкционированных переводов денежных средств за 2016 год Банка России, объем несанкционированных операций, совершенных с использованием платежных карт, эмитированных на территории Российской Федерации, в 2016 г. составил 1,08 млрд. руб., а объем несанкционированных операций, осуществленных с банковских счетов юридических лиц, – 1,89 млрд руб.

Тенденцией последнего времени является ориентация киберпреступников на атаки, целью которых становится непосредственно информационная инфраструктура операторов по переводу денежных средств и операторов услуг платежной инфраструктуры[24].

Это подтверждается сведениями об инцидентах, произошедших при эксплуатации операторами по переводу денежных средств и операторами услуг платежной инфраструктуры объектов информационной инфраструктуры: в 2016 г. общая сумма несанкционированных операций с

[24] Никитенко, И. В., Якушева, Т. В. Координация преступных действий организованных групп: проблемы законодательства и правоприменительной практики / И.В. Никитенко, Т.В. Якушева // Вестник Дальневосточного юридического института МВД России. — 2017. — № 2 (39). – С.20-22

корреспондентских счетов, открытых в расчетном центре платежной системы Банка России, составила 2,18 млрд. руб. При этом окончательность перевода денежных средств наступила на сумму 1,5 млрд. руб. По оценкам отчитывающихся операторов, ущерб от указанных атак составил 712 млн. рублей. Причиной осуществления таких несанкционированных операций является воздействие вредоносного кода на объекты информационной инфраструктуры. Рост числа атак и сумм хищений является ярким индикатором финансовой активности киберпреступников, изменения их тактики и целей.

Большая часть хакеров следует за деньгами. Если они находят новые, более высокооплачиваемые и безопасные способы заработка, то начинают инвестировать именно туда, создавая новые инструменты, услуги, схемы проведения атак. Снижение уровня безопасности и бесперебойности оказания платежных услуг и возникновение крупных финансовых потерь в результате действий киберпреступников могут привести к негативным последствиям для экономического развития. А также, повлечь социальные волнения, спровоцировать значительный отток денежных средств из банковской системы, как это наблюдалось в 2014 г. после приостановления операций по банковским картам международными платежными системами[25].

Обеспечение безопасности платежных услуг, противодействие киберпреступности в финансовой сфере, в том числе легализации (отмыванию) доходов, полученных преступным путем с применением электронных платежных средств, являются важнейшими направлениями деятельности Банка России, что подтверждается документами стратегического характера[26].

Согласно основным направлениям развития финансового рынка Российской Федерации на период 2016– 2018 годов, одним из приоритетов

---

[25] Соколов, Ю. Н. Электронный носитель информации в уголовном процессе / Ю.Н. Соколов // Информационное право. 2017. № 3. – С.29.

[26] Карнаухова, Е. Ю. Мошенничество в сфере безналичных расчетов с использованием банковских платежных карт [Текст] / Е.Ю. Карнаухова // Юридические науки: проблемы и перспективы: материалы II Междунар. науч. конф. (г. Пермь, январь 2014 г.). — Пермь: Меркурий, 2014. — С. 42-44.

Банком России является разработка совместно с заинтересованными органами власти мероприятий по обеспечению кибербезопасности и противодействию киберпреступности, а также обеспечение бесперебойного и безопасного предоставления финансовых услуг.

В соответствии со Стратегией развития национальной платежной системы (одобрена Советом директоров Банка России 15.03.2013) целью развития национальной платежной системы (далее - НПС) является обеспечение эффективного и надежного функционирования субъектов НПС для удовлетворения текущих и перспективных потребностей национальной экономики в платежных услугах. А также для реализации денежно-кредитной политики, обеспечения финансовой стабильности, повышения качества, доступности и безопасности платежных услуг[27].

Решение задач по развитию НПС будет осуществляться при следовании Банком России, в частности, принципу соразмерности регулирования, надзора и наблюдения в НПС рискам, присущим деятельности субъектов НПС и связанным с нарушением бесперебойности функционирования платежных систем. А также ухудшением качества, снижением безопасности оказания платежных услуг, легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма (ОД/ФТ)[28].

В заключении следует отметить, что клиентам, которые при взаимодействии с банками используют технологии электронного банкинга и иные новейшие технологии без непосредственного контакта с банком, часто устанавливается более высокий уровень риска легализации (отмывания) доходов, полученных преступным путем.

---

[27] Кузин, М. В.. Современные методы противодействия мошенничеству с банковскими картами / М.В. Кузин. // безопасность информационных технологий. 2012. № 3. – С. 29-31.

[28] Иконников, Д. Н. Предупреждение преступлений, совершаемых с использованием банковских карт / Д.Н. Иконников // Расчеты и операционная работа в коммерческом банке. — 2011. — № 3– С. 28.

Таблица 1. Сведения о хищениях в результате совершенных киберпреступлений за 2016–2017 гг. по данным компании Group-IB[29]

Сегмент рынка в Российской Федерации и странах СНГ	Количество групп	Общее количество результативных атак в день	Средняя сумма одного хищения	Объем хищений в день	H2 2016 – H1 2017 (руб.)	H2 2015 – H1 2016 (руб.)	% роста к прошлому периоду
Хищения в интернет-банкинге у юридических лиц с использованием вредоносного программного обеспечения (ПО)	**3**	**2**	**1 250 000**	**2 500 000**	**622 500 000**	**956 160 000**	**-35**
Хищения в интернет-банкинге у физических лиц с использованием вредоносного ПО	**1**	**1**	**63 000**	**63 000**	**15 687 000**	**6 424 200**	**144**
Хищения у физических лиц с Android-троянами	**10**	**300**	**11 000**	**3 300 000**	**821 700 000**	**348 600 000**	**136**
Целевые атаки на банки	**2**	**-**	**-**	**-**	**1 630 000 000**	**2 500 000 000**	**-35**
Фишинг	**15**	**950**	**1 000**	**950 000**	**236 550 000**	**-**	**-**
Обналичивание похищаемых средств	**-**	**-**	**-**	**2 638 350**	**1 390 449 150**	**1 715 032 890**	**-19**
Итого				**6 813 000**	**4 716 886 150**	**5 526 217 090**	**-15**

[29]Group-IB представила отчет о киберпреступности и призвала рынок к хантингу// https://www.group-ib.ru/media/hi-tech-crime-trends-2018/

ГЛАВА 2. ДЕЯТЕЛЬНОСТЬ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД ПО ВЫЯВЛЕНИЮ И ДОКУМЕНТИРОВАНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОГО БАНКИНГА

§ 2.1. Особенности выявления преступлений, совершенных с использованием электронного банкинга

Выявление преступлений, совершенных с использованием электронного банкинга, является для правоохранительных органов особенно трудной задачей вследствие относительной новизны и высокой технической сложности таких преступлений, организованного характера преступной деятельности и межрегионального характера большинства совершаемых преступлений.

Существенные проблемы имеются в информационно-аналитической деятельности, подразумевающей регистрацию и изучение количественных и качественных показателей преступности; в деятельности по выявлению предупреждению, пресечению и раскрытию преступлений, осуществляемой оперативными подразделениями; в деятельности следственных подразделений по расследованию преступлений. При этом, как уже было отмечено, вопросы борьбы с хищениями денежных средств с использованием систем электронного банкинга пока еще недостаточно исследованы и освещены в научной литературе.

Изучение данной темы, по сути, только начинается. Основную работу по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации выполняют оперативные подразделения органов внутренних дел, такие как оперативно-технические подразделения, как центрального аппарата МВД России, так региональных, районных или городских территориальных органов МВД России, а также иные оперативные подразделения различного уровня, например, специализированные подразделения ЭБиПК и уголовного розыска.

Несмотря на успешное пресечение вышеуказанными оперативными подразделениями полиции в течение последних лет преступной деятельности ряда групп, занимавшихся хищениями денежных средств с использованием вредоносных компьютерных программ, такая целенаправленная работа с использованием возможностей сил, средств и методов оперативно-розыскной деятельности ведется, по сути, без надлежащего информационно-аналитического обеспечения[30].

Как справедливо указывает А.Н. Волощук: - «… оперативные подразделения правоохранительных органов, несмотря на активное стремление перестроить свою работу в сложившихся условиях, пока не в состоянии в полной мере контролировать складывающуюся обстановку из-за того, что возникают существенные трудности не только в выявлении, но и в комплексной систематизации сведений о криминальных процессах, происходящих в Интернет пространстве. Все это негативно влияет на уровень эффективности, поэтому требуются новые подходы, основанные на системно-масштабном анализе разнородной информации. И важную роль в этом процессе играет информационно-аналитическое обеспечение борьбы с Интернет преступностью»[31].

Основными направлениями информационно-аналитической деятельности в борьбе с преступлениями, совершаемыми в сфере электронных платежей, по мнению С.В. Воронцовой, должны являться:

- формирование и анализ базы данных о таких преступлениях,
- комплексный анализ информации о состоянии борьбы с преступлениями в сфере оборота электронных расчетов и платежей в целях выработки решений,

---

[30] Халиуллин А.И. Подходы к определению киберпреступления / А.И. Халиуллин // Российский следователь. 2015. - № 1. – С.114-115.

[31] Волощук А.Н. Особенности выявления преступлений в Интернет-пространстве / А.Н. Волощук // Законность. 2014. - №8. – С.28.

- проведение целенаправленных криминологических и социологических исследований в целях оценки складывающейся оперативной обстановки и прогнозирования,
- подготовка на основе анализа разнообразных документов (материалов, докладов, оценок, проблемных записок, предложений и др.)[32].

Формирование массивов данных должно производиться, в первую очередь, оперативными подразделениями. Большой объем разнородных сведений из различных источников, касающейся всех сторон преступной деятельности и сопутствующих процессов и событий поступает в оперативные подразделения при проведении оперативно-розыскных мероприятий, в ходе проверок по сообщениям о преступлениях, а затем и следственных действий по делам о преступлениях, совершенных с использованием электронного банкинга. Однако эти данные в настоящее время в каких-либо централизованных базах данных не сохраняются и системному анализу не подвергаются. Большая часть информации, представляющей иногда весьма значительную ценность, остается в распоряжении лишь их непосредственных получателей — отдельных оперативных подразделений и их сотрудников. Через некоторое время информация фактически теряется, оставаясь в лучшем случае в материалах дел оперативного учета или уголовных дел. Информационный обмен не только между подразделениями, но и между сотрудниками одного и того же подразделения во многих случаях фактически не налажен[33].

Поскольку централизованной базы данных оперативно-розыскной информации по преступлениям в сфере компьютерной информации в органах внутренних дел в настоящее время не существует, рассуждать о модели данных, ее системе управления, аппаратной и сетевой инфраструктуре, а

---

[32] Воронцова С. В. Борьба с преступлениями, совершаемыми в сфере электронных платежей /С.В. Воронцова // Законность. 2016. - №4. – С.15.

[33] Турышев, А. А. Уголовно-правовые инструменты защиты информационного общества / А.А. Турышев // Законы России: опыт, анализ, практика. 2017. - № 10. – С.69-71.

также о способах и порядке наполнения и использования можно только теоретически.

Вероятно, такая база должна быть общей для всех преступлений указанной категории. Выделение данных, относящихся к хищениям денежных средств с использованием электронного банкинга, должно производиться внутри общего массива в связи с особенностями характера и объема данных.

Необходимо будет учитывать, что некоторые сведения, касающиеся хищений рассматриваемого типа, будут иметь особый правовой статус (сведения, составляющие банковскую тайну, персональные данные)[34].

Для обеспечения эффективного информационно-аналитического обеспечения деятельности по борьбе с описываемыми хищениями должны сохраняться следующие данные:

1. Сведения обо всех переводах денежных средств, как состоявшихся, так не завершенных, в процессе совершения хищений. Сведения о счетах (банковских, карточных, остатках электронных денежных средств), имеющих отношение к совершению хищений: счетах законных владельцев денежных средств; счетах, используемых для вывода и обналичивания похищенных денежных средств, счетах, используемых участниками преступной деятельности для расчетов между собой и т. и.

2. Сведения о физических лицах (персональные данные, псевдонимы, приметы и т. п.), имеющих любое отношение к хищениям. Должны учитываться сведения об установленных и неустановленных участниках преступной деятельности; о законных владельцах денежных средств, в отношении которых совершились или планируются совершиться; о владельцах любых счетов, банковских карт, средств связи, учетных записей любого типа и т. д., задействованных любым образом при совершении хищений.

---

[34] Манжуева О.М. Феномен информационной безопасности: сущность и особенности: дис. ... докт. фил.наук: 09.00.11. Улан-Удэ, 2015. – С.95-99.

3. Сведения о юридических лицах, имеющих отношение к хищениям. Должны учитываться сведения об организациях, которыми открыты любые счета, а также которым принадлежат любые средства связи, учетные записи любого типа и т. д,, задействованные при совершении хищений.

4. Сведения о сетевых адресах (IP-адресах), с которых осуществлялись какие-либо соединения в процессе подготовки и совершения хищений и в целом в процессе осуществления преступной деятельности.

5. Сведения о доменных именах веб-сайтов, использовавшихся в процессе подготовки и совершения хищений.

6. Сведения обо всех телефонных номерах, адресах электронной почты, аккаунтах систем мгновенного обмена сообщениями, почтовых и юридических адресах, MAC-адресах устройств и т.д.

Нетрудно заметить, что разработка и создание базы данных, необходимой для сохранения и обработки перечисленных сведений и медиа объектов, является исключительно сложной и трудоемкой комплексной задачей. Не будет преувеличением сказать, что для ее реализации необходимо проведение отдельного научно-практического исследования, участие в котором должны принимать сотрудники научных подразделений, представители технических подразделений, которые в дальнейшем будут обеспечивать функционирование необходимой аппаратной и сетевой инфраструктуры, а также представители оперативных подразделений будущих пользователей базы данных. В структуре МВД России в настоящее время существуют подразделения оперативно-розыскной информации (УОРИ МВД России, ПОРИ МВД по республикам и иным субъектам Российской Федерации и др.), на которые должна быть возложена эксплуатация базы оперативно-розыскных и иных данных, а также ведение части аналитической работы. Указанные подразделения осуществляют свою деятельность в интересах оперативных подразделений МВД России[35].

[35] Шутова, А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: дис. ... канд. юрид. наук: 12.00.08. Н.Новгород, 2017.

Оперативные подразделения, занимающиеся борьбой с преступлениями в сфере компьютерной информации, должны будут обеспечивать наполнение базы данных. Для работы с ней потребуется организация непосредственного доступа к базе на рабочих местах сотрудников подразделений, так как внесение и получение сведений в бумажной форме невозможно в силу характера сохраняемой информации, а также для обеспечения оперативности. Создание и функционирование базы данных потребует соответствующих изменений в структуре как подразделений оперативно-розыскной информации, так и в структуре оперативных подразделений непосредственных пользователей баз данных. Вероятно, потребуется введение отдельных должностей для сотрудников, работающих с базой данных, так как ввод, поиск данных и проведение аналитической работы являются трудоемкими задачами, и их вряд ли возможно совмещать с выполнением иных трудовых обязанностей. На определенном этапе в составе оперативных подразделений, занимающихся борьбой с преступлениями в сфере компьютерной информации, потребуется создание отдельных аналитических подразделений, на которые в числе прочих задач будет возложена работа с рассматриваемой базой данных.

Подводя итоги данного параграфа, полагаем, что необходимо создание, наполнение и получение оперативно-розыскной информации из такой базы данных, которая позволят резко повысить эффективность борьбы с хищениями денежных средств, совершаемыми с использованием электронного банкинга. К сожалению, в настоящее время все рассуждения о ее будущих возможностях имеют, как уже было сказано, чисто теоретический характер. Однако предъявляемые обществом требования повышения эффективности борьбы с преступлениями, совершаемыми с использованием электронного банкинга рано или поздно приведут к осознанию руководством правоохранительных органов необходимости создания централизованного учета оперативной информации и налаживания информационно-аналитической деятельности.

§2.2. Особенности оперативного документирования преступлений, совершенных с использованием электронного банкинга

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

Проведение оперативно-розыскных и иных мероприятий по преступлениям, связанным с неправомерным доступом к компьютерной информации и использованием вредоносного программного обеспечения, требует от сотрудников оперативных подразделений полиции специальных познаний в области компьютерной информации и должно осуществляться в тесном взаимодействии со специализированными оперативно-техническими подразделениями полиции, например, по линии «К».

На первоначальном этапе предварительной оперативной проверки признаки совершения подобных преступлений могут выражаться 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, размещенной 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 оперативно-розыскные мероприятия.

1. В рамках ОРМ «Опрос» 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 рамках ОРМ «Сбор образцов для сравнительного исследования» и (или) ОРМ «Получение компьютерной информации» 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 предварительной оперативной проверки компьютерную технику в комплексе (системный блок, смартфон) либо накопитель информации (жесткий диск, флэш-карту и т.п.).

4. В рамках ОРМ «Исследование предметов и документов» и (или) ОРМ «Получение компьютерной информации» 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 (присутствие файлов, созданных вредоносным программным обеспечением и т.п.);
- иные сведения, представляющие интерес.

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

5. Организовать взаимодействие с оперативно-техническим подразделением по линии «К» регионального уровня по существу проведения дальнейших совместных оперативно-розыскных мероприятий.

6. В рамках ОРМ «Наведение справок» направить запрос и постановление суда в банк, или направить запрос в платежную систему, оператору связи, где обслуживается расчетный счет, на который были перечислены похищенные денежные средства.

7. При получении сведений от операторов электронных платежных систем, банков, операторов сотовой связи проанализировать полученные сведения и принять одно из следующих решений:

- если установлено место совершения преступления, направить материал проверки по территориальности (подведомственности);
- если установлено, что преступление совершено на обслуживаемой территории, принять решение о возбуждении уголовного дела;

- если место совершения установить не представляется возможным, принять решение о возбуждении уголовного дела;
- если отсутствуют основания для возбуждения уголовного дела, отказать в его возбуждении.

Здесь же необходимо организовать и провести комплекс ОРМ по одной из возможных оперативно-тактических схем. Например, от преступления к преступнику, либо от лица, обоснованного заподозренного в преступной деятельности, к конкретным фактам его противоправной деятельности. В случае задержания преступника применяется схема «От задержанного лица к другим ранее не известным фактам его преступной деятельности и (или) другим участникам преступной группы».

Анализ оперативной обстановки и имеющиеся оперативные данные свидетельствует о том, что в настоящее время на территории Российской Федерации существует обширный рынок сбыта вредоносных программ, широко развернута деятельность ряда глубоко законспирированных, либо с закрытым доступом, то есть требующих специального «инвайта», а также «открытых» и «полуоткрытых» Интеренет-ресурсов, на которых происходит рекламирование, распространение, обмен и продажа вредоносных программ, в том числе с участием несовершеннолетних. Также не стоит забывать и об Интренет-ресурсах бесплатных объявлений – излюбленное место распространителей вредоноса[36].

Как одним из типичных примеров, на наш взгляд, следует привести следующий. В СУ УМВД России по Н-ской области был направлен материал предварительной оперативной проверки по факту распространения неким гражданином вредоносных компьютерных программ за денежное вознаграждение, собранный в рамках материалов ОРД ОВД в отношении фигуранта по признакам преступления по ст. 273 УК РФ[37]. Для наглядности

---

[36] Дуленко, В. А. Преступление в сфере высоких технологий : учебное пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. – М.: ЦОКР МВД России, 2010. – С. 28-29.

[37] Дело № 1-826/ 2016. Архив Ленинского районного суда г.Кирова. – 2016. – Режим доступа: https://sudact.ru

используются материалы оперативных разработок, реализованных сотрудниками подразделения «К» БСТМ УМВД России по Н-ской области, а также материалы расследования уголовного дела (№ 2012-ннн) в отношении лица, обвиняемого в преступлении, предусмотренном статьей 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.

Также например, обратимся к такому примеру. В марте 2014 года в отдел «К» БСТМ УМВД России по Н-ской области поступила оперативная информация, о том, что гражданин, имеющий ник в сети Интернет и в программе видеозвонков «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[38]. Продажа вредоносных компьютерных программ «51» (Ф.И.О.) осуществляется с использованием возможности сети Интернет (в том числе через сайты объявлений), а так же через форумы Интернет-ресурсов.

[38] Дело № 1- 228/2014// Архив Канашского районного суда Чувашской Республики. – 2014. – Режим доступа: https://sudact.ru

В целях конспирации «51» никаких контактных данных в сети не оставлял, кроме почты «51@gmail.ru» и ника в «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 проведён мониторинг (наблюдение), поиск и анализ информации, размещенной на сайтах, расположенных на информационных ресурсах Н-ских провайдеров сети Интернет, на англо- и 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 базам данных.

Проведен сбор и анализ дополнительно полученной оперативной информации, по результатам которой был намечен 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 распространяемую 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-нибудь пользоваться данным программным продуктом?

После проведения первого ОРМ «Проверочная закупка» в рамках ОРМ «Исследование предметов и документов» было назначено исследование в

ЭКЦ УМВД России по Н-ской области закупленного образца компьютерной программы. На разрешение исследования поставлены следующие вопросы:

1. Содержатся ли на представленном для исследования USB-флеш-носителе какие-либо программные продукты? Если да, то, какие именно.

2. Является ли находящееся на представленном для исследования USB-флеш-носителе программное обеспечение вредоносным?

3. Детектируются ли антивирусным программным обеспечением программные продукты, содержащиеся на предоставленном USB-флеш-носителе? Если да, то, к какому семейству вредоносных программ относятся данные программные продукты.

4. Какими признаками вредоносности обладают компьютерные программы, находящиеся на представленном USB-флеш-носителе?

Так, например, после проведения исследования предварительно закупленной в рамках ОРМ «Проверочная закупка» компьютерной программы, 15 апреля 2014 года на основании постановления заместителя начальника УМВД РФ по Н-ской области – начальника полиции о проведении ОРМ, в соответствии с ФЗ «Об ОРД» в установленном месте сотрудниками отдела «К» БСТМ УМВД России по Н-ской области произведена проверочная закупка образцов вредоносной компьютерной программы «Spy-Net 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 статье 273 Особенной части УК РФ. Данный материал проверки был направлен в следственный орган для решения вопроса о возбуждении уголовного дела.

В заключении необходимо сделать вывод, что как бы ни складывалась та или иная оперативно-следственная ситуация, в любом случае оперативные

сотрудники, наделенные правами документирования фактов, имеющих отношение к преступной деятельности разрабатываемых лиц, и последующего эффективного расследования уголовного дела, всегда должны знать о предпочтительной последовательности и нюансах практической реализации полученных следов, которые в дальнейшем можно будет приобщить к материалам уголовного дела в качестве вещественного доказательства. В ходе взаимодействия оперативных сотрудников ОВД со следователями при проведении оперативно-технических мероприятий иногда возникают и типичные ситуации, которые поддаются алгоритмизации и программированию. Однако все принимаемые решения должны носить законную правовую основу и содержать в себе обоснованность, мотивированность, своевременность и реальность их исполнения. Законность предполагает, что принимаемое решение предусмотрено действующим законодательством и полностью ему соответствует.

§2.3. Взаимодействие правоохранительных органов и служб безопасности банков при выявлении и документировании преступлений, совершенных с использованием электронного банкинга

Банковская система, связанная с накоплением, распределением и использованием государственных и частных средств, является одной из наиболее привлекательных для отдельных преступников и организованных преступных групп. В современных условиях в этой системе осуществляется неимоверное множество различных афер, среди которых наиболее распространенными являются мошенничества, совершаемые в сфере функционирования электронных расчетов. Выявление и расследование таких преступлений является одной из приоритетных задач, стоящих перед правоохранительными органами. Важное значение в решении данного

вопроса принадлежит налаженному взаимодействию ОВД с банковскими учреждениями[39].

Вопросам взаимодействия при расследовании преступлений в банковской сфере уделяли внимание в своих исследованиях многие ученые, между тем на практике остаются нерешенными вопросы, связанные с совместной деятельностью и оказанием содействия со стороны банковских учреждениях сотрудникам правоохранительных органов. Именно этим, зачастую, и обусловливаются низкий уровень эффективности расследования хищений денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ.

Современные банковские учреждения являются относительно закрытыми для контроля со стороны государства, в связи с чем в случае выявления признаков преступлений руководители банков обращаются за помощью в правоохранительные органы лишь в единичных случаях. Данное обстоятельство стало объективным условием выявления и документирования мошенничеств, совершаемых в сфере функционирования электронных расчетов, сотрудниками служб безопасности банков. Такое положение вещей вполне обосновано, поскольку нормативные документы большинства банковских учреждений РФ закрепляют такие обязанности служб банковской безопасности, как: выявление признаков подготавливаемых и совершенных преступлений, применение мер по их предупреждению и прекращению; подготовка материалов в правоохранительные органы для решения вопроса о возбуждении уголовного дела; участие в предварительном расследовании уголовных дел; направление правоохранительным органам информации, имеющей отношение к расследованию; применение в пределах компетенции мер по возмещению причиненного банку вреда. Помимо этого, такие

[39] Анапольская, А. И. Деятельность преступных организаций, осуществляющих «отмывание» денежных средств с использованием электронных расчетных операций / А.И. Анапольская // Материалы Международной научно-практической конференции. Тамбов. 2015. - С. 52.

обязанности были закреплены в приказе МВД России от 4 января 1996 г. №4 «О реализации Соглашения между МВД России и Ассоциацией российских банков»[40]. Однако вышеуказанный приказ МВД России утратил силу на основании приказа МВД России от 26 февраля 2008 г. № 176 «О признании утратившим силу приказа МВД России от 4 января 1996 г. №4»[41], а в замен нового нормативного правового акта МВД России предложено не было. Таким образом, отсутствие в законодательстве прямых предписаний по выполнению вышеперечисленных обязанностей приводит к тому, что на практике в большинстве случаев они не выполняются.

Как правило, в процессе «внутренних» проверок нарушения порядка осуществления банковских операций сотрудникам служб безопасности банков удается выявить приблизительно 10-15% мошенничеств, совершенных уполномоченными сотрудниками банков. Между тем, как справедливо указывает А.Ф. Волобуев, деятельность банков как структур рыночной экономики во многих аспектах связана с охранением коммерческой (банковской) тайны. Поэтому различного рода имущественные злоупотребления персонала банка становятся известными правоохранительным органам только тогда, когда на это дает разрешение руководство[42].

Как показало проведенное нами исследование, внутренними пользователями (сотрудниками банков) совершаются 79% преступлений данного вида, тогда как внешними пользователями – только 21%. Полученные данные корреспондируются с результатами исследований, проведенными О.П.Дубовым, М.В. Салтевским и П.Ю. Тимошенко, которые указывают, что основная опасность в процессе совершения данного вида преступлений исходит от внутренних пользователей. Ими совершаются 94%

---

[40] О реализации Соглашения между МВД России и Ассоциацией российских банков: приказ МВД России от 04.01.1996 г. № 4 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

[41] О признании утратившим силу приказа МВД России от 04.01.96 г. №4: приказ МВД России от 26.02.2008 г. №176 [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

[42] Волобуев, А. Ф. Проблемы методики расследования хищений имущества в сфере предпринимательства / А.Ф. Волобуев. - Харьков 2015. – С.46-49.

преступлений, тогда как внешними пользователями – только 6%, при этом 76% из числа внешних пользователей – это клиенты-пользователи компьютерной системы, а 24% - обслуживающий персонал[43].

Результаты, выявления мошенничеств, совершаемых сотрудниками, руководители банков также стремятся отнести к охраняемой законом банковской тайне, не дав ей официального хода[44]. Однако институт банковской тайны в законодательстве РФ существует не для уклонения от предоставления соответствующей информации, а для обеспечения защиты законных прав и интересов участников правоотношений в кредитно-финансовой сфере.

В ситуации, когда заявление все-таки подается в органы внутренних дел, представители банковского учреждения, как правило, ограничивают процесс ознакомления правоохранителей с реальной противоправной ситуацией, результатами собственных расследований. В свою очередь, сотрудники правоохранительных органов, не имея прямого доступа к операциям и документам банка, нередко вынуждены ограниваться лишь поверхностным исследованием имеющихся доказательств, не использую процессуальные и оперативно-розыскные средства для получения новых.[45] Данные обстоятельства не лучшим образом сказываются на процессе доказывания и судебного рассмотрения уголовных дел о мошенничествах, совершаемых в сфере функционирования электронных расчетов, а в ряде случаев – делают этот процесс просто невозможным.

Между тем взаимодействие банков с органами предварительного расследования могло бы значительно ускорить процесс расследования преступлений данного вида, сделать его более эффективным. Результаты

---

[43] Биленчук, П. Д. Криминалистика : учебное пособие / П.Д. Биленчук, О.П. Дубовой, М.В. Салтевский, П.Ю. Тимошенко. – М: НИЦ ИНФРА-М, 2016. - С. 414.

[44] О банках и банковской деятельности: Федеральный закон от 02.12.1990 г. №395-1 (в ред. от 29.05.2019) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

[45] Анапольская, А. И. Использование оперативно-технических средств подразделениями уголовного розыска в процессе раскрытия хищений денежных средств в сфере электронных расчетов / А.И. Анапольская //Научные перспективы XX1 века. Достижения и перспективы нового столетия: материалы 5 Международно-практической конференции. – 2014. – С.152-156.

опроса, проведенного В. О. Финагеевым, показали, что совместная деятельность сотрудников банковской безопасности и следователей целесообразна в случае:

- предоставления службами безопасности правоохранительным органам материалов для решения вопроса о возбуждении уголовного дела (88 и 92%);
- доступа в помещения, к документам и техническим средствам банка, необходимым для проведения следственных действий, и оказания помощи в их применении (51 и 76%);
- налаживания связей и получения информации от иных банков по вопросам незаконного перечисления средств (42 и 68%);
- участие в розыске лиц, посягавших на интересы банка или подозреваемых в их совершении, а также применения в пределах компетенции мер по возмещению причиненного ущерба (35 и 44%)[46].

Указанные данные свидетельствуют от осознании практическими сотрудниками как правоохранительных органов, так и банковских учреждений необходимости разрешения отмеченных нами вопросов взаимодействия и закрепления их на законодательном уровне.

В частности, в целях разрешения возникающих проблем взаимодействия правоохранительных органов с банковскими учреждениями, предлагаем установить исчерпывающий перечень органов государственный власти, имеющих право получения из банков сведений, составляющих государственную тайну, а также сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков. Кроме того, с целью сокращения временных рамок исполнения запросов правоохранительных органов, а также устранения необходимости нагромождения уголовного дела лишней информацией рекомендуется предоставить банкам возможность передавать сведения, составляющие

[46] Финагеев, В. А. Проблемы взаимодействия правоохранительных органов и подразделений банковской безопасности в выявлении расследования преступлений / В.А. Финагеев. – 2015. – С.74.

банковскую тайну, на электронных носителях с заверением ее подлинности в сопроводительных письмах.

По делам о хищениях денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, криминалистическая методика имеет некоторые особенности, которые обусловлены необходимостью обеспечения сотрудничества следователей и сотрудников служб безопасности банков. Подобное взаимодействие особенно необходимо при выявлении и расследовании хищений денежных средств с платежных карт с банкоматов или путем снятия денежных средств через кассу банка. При втором варианте всегда можно выдвинуть версию о причастности к хищениям сотрудников банка.

УПК РФ предусматривает взаимодействие сотрудников оперативных и иных подразделений полиции и работниками служб безопасности банков только по делам, которые находятся в производстве предварительного следствия, и в трех основных формах[47]:

- производство службой безопасности банков розыскных и следственных действий по указаниям и поручениям следователя, обязательные для исполнения;
- оказание содействия при производстве отдельных оперативно-розыскных мероприятий и следственных действий;
- уведомление следователя о результатах собственного внутреннего расследования[48].

Конечно же, сотрудники служб безопасности банков не являются дознавателями, для которых следователь может давать любые поручения.

---

[47] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в ред. от 01.04.2019, с изм. от 17.04.2019) (с изм. и доп., вступ. в силу с 12.04.2019) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

[48] Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук: 12.00.08. Казань, 2017.

Однако есть Федеральный закон «О полиции»[49], в п. 3 ст. 13 которого императивно установлено, что сотрудник полиции имеет право вызывать в полицию должностных лиц по расследуемым уголовным делам, а также в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, разрешение которых отнесено к компетенции полиции; получать по таким делам, материалам, заявлениям и сообщениям, в том числе по поручениям следователя и дознавателя, необходимые объяснения, справки, документы (их копии). Кроме того, в этом же пункте установлено, что если должностное лицо игнорирует требование сотрудника полиции о явке в полицию, то подвергать приводу в полицию должностных лиц, которые уклоняются без уважительных причин от явки по вызову.

При взаимодействии следователя с сотрудниками служб безопасности банков основное внимание уделяется проверке и закреплению имеющихся фактических данных, установлению новых эпизодов краж денежных средств с платежных карт, обеспечению полноты и всесторонности исследования обстоятельств кражи денежных средств с платежной карты.

Оперативно-розыскные мероприятия – один из способов получения информации о признаках кражи денежных средств с платежной карты. В самом банке важную оперативную информацию можно получить у служб безопасности банков, а также у сотрудников отдела пластиковых карт. В этом отделе имеется база данных обо всех клиентах банка, у которых есть пластиковая карта их банка. Доступ к этой информации имеют не только начальник отдела пластиковых карт, но и администратор компьютерных баз данных, а также несколько экономистов. Работа этих экономистов заключается в том, что они каждый день сводят балансы и следят за тем,

[49] О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ (в ред. от 01.04.2019) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс» (дата обращения: 12.04.2019).

чтобы запрошенные клиентами суммы не превышали остатков на пластиковой карте[50].

Взаимодействие сотрудников оперативных подразделений полиции и служб безопасности банков может быть осуществлено в различных формах:

- анализ первичных данных о краже денежных средств с платежной карты;
- совместное планирование раскрытия и расследования кражи денежных средств с платежной карты;
- выдвижение оперативно-розыскных и следственных версий по поводу кражи денежных средств с платежной карты.

В заключении необходимо отметить, что определение принципов и форм взаимодействия правоохранительных органов со службами безопасности банков, разработка соответствующих методик документирования и изобличения преступников, а также проведение совместных семинаров и тренингов для сотрудников практических подразделений при участии специалистов из банковской сферы и сферы компьютерных технологий позволят надлежащим образом организовать борьбу с мошенничествами, совершенными в сфере функционирования электронных расчетов. Поэтому считаем целесообразным введение нового нормативного правового акта, регламентирующего деятельность по взаимодействию служб безопасности банков и правоохранительных органов при выявлении и документировании преступлений, совершенных с использованием электронного банкинга (приложение №1).

[50] Романовский Г.Б. Банковская тайна и оперативно-розыскная деятельность правоохранительных органов / Г.Б. Романовский // Электронный научный журнал «Наука. Общество. Государство». — 2016. — Т. 4, № 1 [Электронный ресурс]. — Режим доступа: http: //esj.pnzgu.ru.

ЗАКЛЮЧЕНИЕ

Подводя итоги настоящей выпускной квалификационной (дипломной) работы, нам хочется отметить, что среди наиболее актуальных тенденций в развитии банковских технологий почетное место занимает активное внедрение новых платформ электронного банкинга.

Электронный банкинг – это деятельность банка по предоставлению комплекса услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей.

Однако быстрое развитие таких технологий создает предпосылки для их использования в преступных целях. Эксперты отмечают, что системы дистанционного банковского обслуживания наиболее часто подвергаются кибератакам. В 2017 году в Банк России была представлена информация о 841 несанкционированной операции со счетов юридических лиц с использованием систем ДБО на общую сумму 1,57 млрд рублей. Выявление и документирование преступлений, совершаемых с ипользованием электронного банкинга, представляет значительные трудности для правоприменителей. Об этом свидетельствуют опросы практических сотрудников органов внутренних дел и изучение материалов уголовных дел, дел оперативного и иного учета.

Основные выводы проведенного выпускного квалификационного исследования, сделанные на основании анализа действующих правовых норм отечественного законодательства, теоретических положений, материалов оперативно-розыскной практики, а также мнения практических сотрудников, нашли свое отражение в следующих положениях:

1. В связи с массовой компьютеризацией населения и растущим числом клиентов банка, готовых обслуживаться через Интернет и мобильный телефон, среди наиболее актуальных тенденций развития банковских технологий почетное место занимает электронный банкинг, что в свою

очередь делает его объектом преступных посягательств. Противоправные действия злоумышленников, направленные на хищение денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, попадают под признаки состава преступления, предусмотренного статьей 159.6 УК РФ. 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 статьям 272, 273 или 274.1 УК РФ.

2. Перспектива возбуждения дела с неопределенной квалификацией и возможной последующей переквалификацией, с отсутствующим или крайне затянувшимся экспертным исследованием, без выявленных лиц, без получателя денежных средств и с весьма слабой в целом перспективой раскрытия воспринимается сотрудниками полиции негативно. Поэтому зачастую на практике используется любая возможность и любые основания для отказа в возбуждении уголовного дела по поступившим заявлениям, что оставляет данные преступления безнаказанными. Согласно статистике, предоставленной Центральном банком Российской Федерации, число преступлений, совершаемых с использованием инструментов электронного банкинга, увеличивается, что наталкивает на необходимость дополнительной разработки новых методов реагирования.

3. Клиентам, которые при взаимодействии с банками используют технологии электронного банкинга и иные новейшие технологии без непосредственного контакта с банком, часто устанавливается более высокий уровень риска легализации (отмывания) доходов, полученных преступным путем.

4. Отсутствует единая оперативно-розыскная база, общая для всех преступлений указанной категории. Выделение данных, относящихся к

хищениям денежных средств с использованием инструментов электронного банкинга, должно производиться внутри общего массива в связи с особенностями характера и объема данных. Необходимо будет учитывать, что некоторые сведения, касающиеся хищений рассматриваемого типа, будут иметь особый правовой статус (сведения, составляющие банковскую тайну, персональные данные). Создание, наполнение и получение информации из такой базы данных позволят резко повысить эффективность работы оперативных подразделений в борьбе с хищениями денежных средств, совершаемыми с использованием инструментов электронного банкинга.

5. Основную работу по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации выполняют оперативные подразделения органов внутренних дел, такие как Управление «К» БСТМ МВД России, отделы «К» БСТМ МВД, ГУ (У) МВД России регионального уровня, специализированные отделы ГУЭБиПК МВД России и подразделений экономической безопасности МВД, ГУ (У) МВД России по субъектам РФ, а также некоторые подразделения уголовного розыска.

По нашему мнению, целесообразно проводить специализированное обучение и подготовку специалистов по противодействию компьютерным преступлениям для более эффективной оперативно-розыскной и иной деятельности специализированных оперативных подразделений полиции, например, по линии уголовного розыска либо экономической безопасности и противодействия коррупции, а именно создание специализированных курсов повышения квалификации для наработки теоретических знаний, практических навыков и умений по техническому обеспечению оперативного выявления и документирования преступлений в сфере высоких технологий. Необходимо проводить заслушивания по данным делам в территориальных подразделениях с участием представителей или руководителей специализированных подразделений или консультантами отдела «К».

6. Сотрудники, наделенные правами документирования фактов, имеющих отношение к преступной деятельности разрабатываемых лиц, и

последующего эффективного раскрытия и расследования уголовного дела, всегда должны знать о предпочтительной последовательности и нюансах практической реализации полученных следов, которые в дальнейшем можно будет приобщить к материалам уголовного дела в качестве вещественного доказательства. В ходе взаимодействия оперативных сотрудников ОВД со следователями при проведении оперативно-технических мероприятий иногда возникают и типичные ситуации, которые поддаются алгоритмизации и программированию. Однако все принимаемые решения должны носить законную правовую основу и содержать в себе обоснованность, мотивированность, своевременность и реальность их исполнения. Законность предполагает, что принимаемое решение предусмотрено действующим законодательством и полностью ему соответствует.

7. В целях разрешения возникающих проблем взаимодействия правоохранительных органов с банковскими учреждениями, предлагаем установить исчерпывающий перечень органов государственный власти, имеющих право получения из банков сведений, составляющих государственную тайну, а также сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков. Кроме того, с целью сокращения временных рамок исполнения запросов правоохранительных органов, а также устранения необходимости нагромождения уголовного дела лишней информацией рекомендуется предоставить банкам возможность передавать сведения, составляющие банковскую тайну, на электронных носителях с заверением ее подлинности в сопроводительных письмах.

8. Определение принципов и форм взаимодействия правоохранительных органов со службами безопасности банков, разработка соответствующих методик документирования и изобличения преступников, а также проведение совместных семинаров и тренингов для сотрудников практических подразделений при участии специалистов из банковской сферы и сферы компьютерных технологий позволят надлежащим образом

организовать борьбу с мошенничествами, совершенными в сфере функционирования электронных расчетов. Считаем необходимым введение нового нормативного правового акта, регламентирующего особенности взаимодействия служб безопасности банков и правоохранительных органов на этапе выявления и документирования преступлений, совершенных с использованием инструментов электронного банкинга.

9. В работе приведен алгоритм реагирования оперативных подразделений на рассматриваемые преступления, проведение ОРМ на первоначальном и дальнейшем этапе, который в дальнейшем можно использовать как методические рекомендации для подразделений уголовного розыска.

10. На начальном этапе раскрытия преступлений в сфере телекоммуникаций и компьютерной информации немаловажное значение имеет своевременное получение информации о совершенном или готовящемся преступлении данной направленности. Полученная информация позволит оперативным сотрудникам подразделения «К» избрать правильную тактику проведения необходимых мероприятий, направленных, в том числе, на установление конкретных лиц, причастных к совершенному преступлению, и изобличение виновных.

В процессе подготовки выпускной квалификационной работы нами осуществлялось интервьюирование практических работников по месту проведения производственной, в том числе, преддипломной, практики, а также подготовка тезисов для выступления на научно-представительских мероприятиях, в частности, 17 мая 2019 года на всероссийской научно-практической конференции адъюнктов, курсантов, слушателей и студентов «Совершенствование правоохранительной деятельности органов внутренних дел (проблемы теории, практики и правового регулирования)», 7 июня 2019 года на всероссийской научно-практической конференции «Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе». Результаты исследования была представлены на

Всероссийском конкурсе молодёжи образовательных учреждений и научных организаций на лучшую работу «Моя законотворческая инициатива» в 2016 году.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации от 12 декабря 1993 г. : с учетом поправок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 05 февраля 2014 г. №2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.04.2019).

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ : в ред. от 29.05.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : в ред. от 01.04.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : в ред. от 29.05.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

5. О банках и банковской деятельности :Федеральный закон от 2 декабря 1990 г. № 395-1 (в ред. от 29.05.2019) // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

6. Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ : в ред. от 06.07.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

7. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства: Федеральный закон РФ от 20 августа 2004 г. № 119-ФЗ : в ред. от 07.02.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.04.2019).

8. О деятельности по приему платежей физических лиц, осуществляемой платежными агентами : Федеральный закон от 3 июня 2009

г. № 103-ФЗ (в ред. от 18.04.2018) // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

9. Об информации, информационных технологиях и о защите информации : Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ : в ред. от 18.03.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 29.04.2019).

10.О персональных данных : Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ : в ред. от 31.12.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 29.04.2019).

11.О полиции : Федеральный закон РФ от 7 февраля 2011 г. № 3-ФЗ : в ред. от 01.04.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

12.Об электронной подписи : Федеральный закон РФ от 06 апреля 2011 г. № 63-ФЗ : в ред. от 23.06.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.04.2019).

13.О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ (в ред. от 28.11.2018) // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.04.2019).

14.О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 31 декабря 2015 г. № 683 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

15.Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 № 646 : в ред. 05.12.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

16.О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 01.06.2019).

17.О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (вместе с "Правилами создания, формирования и ведения единой автоматизированной информационной системы "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", "Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети "Интернет", распространение которых в Российской Федерации запрещено") : постановление Правительства РФ от 26 октября 2012 г. № 1101 : в ред. от 21.03.2019 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

18.Об утверждении государственной программы Российской Федерации "Обеспечение общественного порядка и противодействие преступности" : постановление Правительства РФ от 15 апреля 2014 г. № 345 : в ред. от 28.03.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.04.2019).

Решения судебных инстанций различного уровня

19.Дело № 1-228/2014 [Электронный ресурс] // Архив Канашского районного суда Чувашской Республики. - 2014. – Режим доступа: https://sudact.ru Дата доступа: 03.06.2019.

20.Дело № 1-826/2016 [Электронный ресурс] // Архив Ленинского районного суда г. Кирова. - 2016. – Режим доступа:https://sudact.ru. Дата доступа: 03.06.2019.

21.О некоторых вопросах, связанных применением ст.ст.23 и 25 Конституции РФ : постановление Пленума Верховного Суда РФ от 24.12.1993 № 13 : ред. от 06.02.2007 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

22.О некоторых вопросах применения судами Конституции Российской Федерации : постановление Пленума Верховного Суда РФ от 31.10.1995 № 8 : в ред. от 03.03.2015 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

23.О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней): постановление Пленума Верховного Суда РФ от 10.06.2010 № 12 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

24.О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 : ред. от 29.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

25.О практике применения судами особого порядка судебного разбирательства уголовных дел при заключении досудебного соглашения о сотрудничестве: постановление Пленума Верховного Суда РФ от 28.06.2012 № 16 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

26.О применении судами законодательства, регламентирующего основания и порядок освобождения от уголовной ответственности : постановление Пленума Верховного Суда РФ от 27.06.2013 № 19 : ред. от 29.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 01.06.2019).

Нормативные правовые акты министерств и ведомств Российской Федерации

27.Об утверждении Инструкции о порядке использования полиграфа при опросе граждан : приказ МВД России от 28 декабря 1994 г. № 437дсп // СТРАС «Юрист» (дата обращения: 25.11.2017).

28.О деятельности органов внутренних дел по предупреждению преступлений : приказ МВД России от 17 января 2006 г. № 19 : ред. от 28.11.2017 // СТРАС «Юрист» (дата обращения: 01.06.2019).

29.Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации : приказ МВД России от 10 февраля 2006 г. № 70 : ред. от 11.09.2018 // СТРАС «Юрист» (дата обращения: 01.06.2019).

30.Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 октября 2006 г. : ред. от 22.09.2009 // СТРАС «Юрист» (дата обращения: 01.06.2019).

31.О некоторых организационных вопросах и структурном построении территориальных органов МВД России : приказ МВД России от 30 апреля 2011 г. № 333 : в ред. от 08.05.2019 // СТРАС «Юрист» (дата обращения: 01.06.2019).

32.Об утверждении Порядка выполнения сотрудниками полиции обязанностей и реализации прав за пределами обслуживаемой территории: приказ МВД России от 30 декабря 2011 г. № 1354 // СТРАС «Юрист» (дата обращения: 01.06.2019).

33.Об утверждении перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну : приказ МВД России от 11 января 2012 г. № 17 : ред. от 06.06.2018// СТРАС «Юрист» (дата обращения: 01.06.2019).

34.Об основах организации ведомственного контроля за деятельностью органов внутренних дел Российской Федерации: приказ МВД России от 3

февраля 2012 г. № 77 : ред. от 29.06.2018// СТРАС «Юрист» (дата обращения: 01.06.2019).

35.О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России : приказ МВД России от 19 июня 2012 г. № 608 : ред. от 14.08.2018 // СТРАС «Юрист» (дата обращения: 01.06.2019).

36.Об организации планирования в органах внутренних дел Российской Федерации : приказ МВД России от 26 сентября 2012 г. № 890 : ред. от 24.04.2019 // СТРАС «Юрист» (дата обращения: 01.06.2019).

37.Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации : приказ МВД России от 12 сентября 2013 г. № 707 : ред. от 01.12.2016 // СТРАС «Юрист» (дата обращения: 01.06.2019).

38.Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю или в суд : приказ МВД РФ, Минобороны РФ, ФСБ РФ, ФСО РФ, Федеральной таможенной службы, СВР РФ, ФСИН, Федеральной службы РФ по контролю за оборотом наркотиков и Следственного комитета России от 27 сентября 2013 г. №776/703/509/507/1820/42/535/398/68 // СТРАС «Юрист» (дата обращения: 01.06.2019).

39.Об утверждении Наставления по ведению и использованию централизованных оперативно-справочных, криминалистических и розыскных учетов, формируемых на базе органов внутренних дел Российской Федерации : приказ МВД России, Минюста РФ, МЧС РФ, Минфина РФ, Минобороны РФ, ФСБ РФ, ФСКН РФ, ФСО РФ, СВР России, ФТС РФ, ФМС России, Государственной фельдъегерской службы РФ, СК РФ, Генпрокуратуры РФ от 12 февраля 2014 г. №89 дсп/19 дсп/73 дсп/1 адсп/113 дсп/108 дсп/75 дсп/93 дсп/19 дсп/324 дсп/113 дсп/63 дсп/14/95 дсп // СТРАС «Юрист» (дата обращения: 01.06.2019).

40.Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел

Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях : приказ МВД России от 29 августа 2014 г. № 736 : ред. от 07.11.2016 // СТРАС «Юрист» (дата обращения: 01.06.2019).

41.Об организации взаимодействия территориальных органов МВД России на железнодорожном, водном и воздушном транспорте с иными территориальными органами МВД России и разграничении объектов оперативного обслуживания: приказ МВД России от 28 марта 2015 г. № 381 : ред. от 31.12.2016 // СТРАС «Юрист» (дата обращения: 01.06.2019).

42.Об объявлении Инструкции по организации совместной оперативно-служебной деятельности подразделений ОВД РФ при раскрытии преступлений и расследование уголовных дел : приказ МВД России от 29 апреля 2015 г. № 495дсп // СТРАС «Юрист» (дата обращения: 01.06.2019).

43.Об организации деятельности в органах внутренних дел Российской Федерации по обеспечению сохранности и учета вещественных доказательств и иных изъятых предметов и документов : приказ МВД России от 30 декабря 2016 г. № 946 // СТРАС «Юрист» (дата обращения: 01.06.2019).

44.Об утверждении Типового положения о подразделении оперативно-разыскной информации территориального органа Министерства внутренних дел Российской Федерации : приказ МВД России от 7 февраля 2017 г. № 45дсп // СТРАС «Юрист» (дата обращения: 01.06.2019).

45.Об утверждении Типового положения о подразделении уголовного розыска территориального органа Министерства внутренних дел Российской Федерации на региональном уровне : приказ МВД России от 19 января 2018 г. № 25: ред. от 26.05. // СТРАС «Юрист» (дата обращения: 01.06.2019).

46.Об утверждении Положения об организации и осуществлении розыска и идентификации лиц : приказ МВД России № 117дсп, Минюста России N 40дсп, Минздрава России N 88н, МЧС России N 82дсп, Минобороны России N 114дсп, СК России N 17дсп от 1 марта 2018 г. // СТРАС «Юрист» (дата обращения: 01.06.2019).

47.Об утверждении формы отчета о расходах на осуществление оперативно-розыскной деятельности : приказ МВД России от 24 апреля 2018 г. № 251дсп // СТРАС «Юрист» (дата обращения: 01.06.2019).

Книги, монографии, сборники научных трудов, учебные пособия

48.Андреев Б.В. Расследование преступлений в сфере компьютерной информации: учебное пособие / под ред. Б.В. Андреев. П.Н. Пак, В.П. Хорс. - М., 2012. - 152 с.

49.Атаманов, Р.С. Криминалистическая характеристика мошенничества в онлайн-играх / Р.С. Атаманов //. Российский следователь, 2011. - № 21. - 268 с.

50.Атаманов, Р.С. Некоторые вопросы расследования мошенничества в сети Интернет / Р.С. Атаманов. М., 2010. - № 4 (17). - 496 с.

51.Бурлаков, В.Н., Средства массовой информации и преступность (криминология СМИ) / В.Н. Бурлаков, Г.Н. Горшенков, С.В.Максина. М., 2012. - № 5. - 584 с.

52.Батурин Ю.М., Жодзишский А.М., Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин., А.М. Жодзишский - М.: Юрид. лит., 1991.

53.Быков В.М. Проблемы расследования групповых преступлений: автореф. дис. … д-ра юрид. наук. / В.М. Быков – М., 1992. – 262 с.

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

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

56.Волженкин, Б.В. Прозрачность правосудия и информационная безопасность. / Б.В. Волженкин. – Режим доступа: law.edu.ru/doc/document.asp

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

58.Голубев, В.А. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью / В.А. Голубев // – Режим доступа: http://www.crime-research.ru/articles/2011/

59.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.

60.Голубева В.А., Рыжкова Э.В., Компьютерная преступность и кибертерроризм: сборник научных статей / В.А. Голубева, Э.В. Рыжкова. // - Запорожье: Центр исследования компьютерной преступности, 2012. – Вып. 3. – 448 с.

61.Дикова Н.И. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : автореф. дис. … канд. юрид. наук. / Н.И. Диков - С., 2011.- 18-29 с.

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

63.Дуленко В.А. Преступление в сфере высоких технологий : учебное пособие / под ред., В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков - М.: ЦОКР МВД России, 2010. - 200 с.

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

65.Карчевский Н.В. Компьютерные преступления: определение, объект и предмет /Н.В. Карчевский - Режим доступа: http://www.ifap.ru/pi/05/karchev.htm

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

67.Крылов В.В. Расследование преступлений в сфере информации: учебное пособие / под ред., В.В. Крылов.- М., 2014. -164 с.

68.Крылов В. В. Расследование преступлений в сфере компьютерной информации: учебное пособие / под ред., В.В.Крылов. - М., 2012. - 615 с.

69.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.

70.Никифоров И., Уголовные меры борьбы с компьютерной преступностью: учебное пособие / под ред., И. Никифоров. - Защита информации, 2010. - № 5. - 258 с.

71.Номоконов В.А. Глобализация информационных процессов и преступность/ В.А. Номоконов // - Режим доступа: http://www.vkeys.kiev.ua/box/4/93.shtml

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

73.Основы оперативно-розыскной деятельности органов внутренних дел Российской Федерации: учебное пособие / авт. - сост. Е.П. Шляхтин, И.М. Усманов. – Казань. КЮИ МВД России, 2017. – 300 с.

74.Селиванов Н. А. Проблемы борьбы с компьютерной преступностью: учебное пособие / Н.А. Селиванов // - Законность, 2013. -№ 8. 37 с.

75.В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. - 352 с.

76.Федоров В.А. Компьютерные преступления: выявление, расследование и профилактика: учебное пособие / под ред., В.А. Федоров. - Законность, 2011, № 6. - 43 с.

77.Черкасов, В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий: учебное пособие / под ред., В.Н. Черкасов. - Саратов, 2015. - 81 с.

78.Чечетин, А. Е. Обеспечение прав личности при проведении оперативно-розыскных мероприятий: монография / А.Е. Чечетин. - СПб.: Изд-во СПб. ун-та МВД России, 2016. – 256 с.

79.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.

Информационные ресурсы

80.http://www.consultant.ru – Правовая система «Консультант Плюс»;

81.http://www.garant.ru – информационно-правовой портал «Гарант»;

82.http://www.ksrf.ru/ – Официальный сайт Конституционного суда Российской Федерации;

83.http://www.supcourt.ru – сайт Верховного Суда Российской Федерации;

84.http://www.vsrf.ru. – Официальный сайт Верховного суда РФ.

85.http://president.kremlin.ru/ – Официальный сайт Президента России;

86.http://www.government.ru – Официальный сайт Правительства России;

87.http://www.genproc.gov.ru – Официальный сайт Генеральной прокуратуры Российской Федерации;

88.http://www.mvd.ru – Официальный сайт Министерства внутренних дел РФ;

89.http://guebmvd.ru – сайт Главного управления экономической безопасности и противодействия коррупции МВД России.

90.http://www.minjust.ru – Официальный сайт Министерства юстиции РФ;

91.http://www.sledcom.ru – Официальный сайт Следственного комитета РФ.

ПРИЛОЖЕНИЕ №1
Проект

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

от _____ 20__ г. N __

О РЕАЛИЗАЦИИ СОГЛАШЕНИЯ МЕЖДУ МВД РОССИИ И АССОЦИАЦИЕЙ РОССИЙСКИХ БАНКОВ

В целях защиты банковской системы России от преступных посягательств, обеспечения ее безопасного функционирования приказываю:

СОГЛАШЕНИЕ

от _____ 20__ г.

МЕЖДУ

МИНИСТЕРСТВОМ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ И АССОЦИАЦИЕЙ РОССИЙСКИХ БАНКОВ О ВЗАИМОДЕЙСТВИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БАНКОВСКОЙ БЕЗОПАСНОСТИ

Министерство внутренних дел Российской Федерации и Ассоциация российских банков (АРБ), в дальнейшем именуемые "Стороны",

будучи обеспокоены осложнением криминогенной обстановки и повышением риска в банковском деле России,

учитывая исключительную важность и значимость финансово - кредитных учреждений в процессе рыночных преобразований,

желая объединить усилия по укреплению законности и правопорядка в сфере денежного обращения,

стремясь обеспечить безопасные условия персоналу банковских учреждений и клиентам,

принимая во внимание имеющийся опыт сотрудничества в рамках совместных мероприятий Министерства внутренних дел, Центрального Банка и Ассоциации российских банков,

руководствуясь соответствующими статьями Законов РФ "О полиции", "О банках и банковской деятельности",

согласились о нижеследующем:

Статья 1

Принципы и направления взаимодействия

1. Стороны, взаимодействуя в процессе предупреждения и раскрытия хищений денежных средств клиентов коммерческих организаций с

банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, желая создать систему надежной безопасности кредитных учреждений, отношения строят на основе следующих начал:

- законности;

- открытости и доверии;

- согласованности действий и взаимном информировании;

- добросовестности и надежности.

2. Основными направлениями взаимодействия МВД России и АРБ по обеспечению банковской безопасности являются:

- защита коммерческих банков от проникновения организованных преступных групп в их среду;

- разработка и внедрение специальных технологий по технической укрепленности и защите банковских объектов, средств связи и т.д.;

- совершенствование систем обеспечения безопасности банковских объектов;

- оказание помощи в обучении, переподготовке и повышении квалификации кадров для служб безопасности банков;

- разработка совместных предложений по совершенствованию правовой основы обеспечения банковской безопасности.

Статья 2

Предупреждение и раскрытие преступлений

1. Считать раскрытие преступных посягательств, связанных с хищением денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ и других криминальных проявлений, создающих угрозу безопасности банковской системы, приоритетным направлением в деятельности Службы

криминальной полиции МВД Российской Федерации и соответствующих подразделений на местах.

2. Устанавливать в Министерстве внутренних дел особый контроль и учитывать в отдельном разделе суточной сводки преступные посягательства, связанные с хищениями денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ, в том числе совершенные персоналом банков.

Привлекать при необходимости представителей служб безопасности коммерческих банков для оказания помощи следственно - оперативным группам в качестве специалистов. Оконченные производством уголовные дела этой категории докладывать коллективам кредитно - финансовых учреждений в порядке, определенном уголовно - процессуальным законом.

3. Информировать АРБ о лицах, объявляемых в местный и федеральный розыск, за преступления, совершаемые в кредитно - финансовой системе.

4. Обсуждать с приглашением в необходимых случаях представителей прокуратуры и следственного комитета состояние работы по делам о нераскрытых преступлениях, особенно возбужденных по фактам хищений денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных вредоносных компьютерных программ. Проводить дополнительные мероприятия, направленные на установление и изобличение виновных, и предание их суду. К разработке мероприятий привлекать сотрудников служб безопасности коммерческих банков, имеющих опыт работы в оперативно - следственных подразделениях МВД, ФСБ, органов прокуратуры.

5. Направлять в территориальные органы внутренних дел подробную информацию о всех фактах хищения денежных средств клиентов коммерческих организаций с банковских счетов, а также электронных денежных средств, совершаемых с использованием специализированных

вредоносных компьютерных программ

В сроки, установленные ст. 144 УПК РФ, рассматривать указанные материалы и принимать по ним процессуальные решения, уведомляя об этом руководителей соответствующих коммерческих банков.

Органам внутренних дел направлять сведения о таких лицах в Главный информационный центр МВД Российской Федерации для постановки на учет по информационно - поисковой системе.

6. Совершенствовать практику организации и проведения целевых мероприятий по выявлению и пресечению организованных преступных группировок, действующих в системе коммерческих банков страны.

При планировании таких мероприятий использовать по согласованию со службами безопасности кредитно - финансовых учреждений имеющийся у них информационно - аналитический потенциал.

Статья 3

Информационный обмен

1. Сведения, составляющие коммерческую тайну, не являются препятствием для получения в установленном порядке органами дознания и предварительного следствия сведений и документов о финансово - экономической деятельности, вкладах и операциях по счетам физических и юридических лиц, подозреваемых в участии и причастности к легализации (отмыванию) преступных доходов.

2. Запросы, исходящие из территориальных органов внутренних дел, в адрес банковских учреждений могут быть подписаны руководителем этого органа и заверены его печатью.

В центральном аппарате Министерства внутренних дел запросы об информации, являющейся коммерческой тайной, адресованные коммерческим банкам, кроме руководства (министр и его заместители) подписывают начальники главных управлений или их заместители. Запрос, подписанный следователем, заверяется печатью соответствующего

следственного подразделения или органа внутренних дел.

3. Должностные лица, указанные в п. 2 настоящей статьи, несут в установленном законом порядке ответственность за использование банковской информации исключительно в оперативно - служебных целях.

4. Министерство внутренних дел Российской Федерации, МВД, ГУВД, УВД осуществляют информационную поддержку коммерческих банков.

Для чего:

- сообщают руководителям финансово - кредитных учреждений о поступившей информации о возможных противоправных действиях в отношении данных учреждений и их персонала;

- обеспечивают отдельными аналитическими документами и - материалами о состоянии и тенденциях развития общеуголовной и организованной преступности. Направляют в АРБ ежеквартальные статистические сведения о преступных посягательствах на банки;

- совершенствуют схемы пользования некоторыми действующими базами данных органов внутренних дел;

- согласовывают тематику и осуществляют на регулярной основе совместную со службами безопасности коммерческих банков разработку рекомендаций по профилактике преступлений в кредитно - финансовой сфере.

5. Коммерческие банки инициативно уведомляют МВД России, его территориальные подразделения о всех необычных (подозрительных) перемещениях денежных средств. При этом необычные финансовые операции определяются с учетом всех признаков их совершения: суммы и характера платежа, характеристик клиента и других обстоятельств, прямо или косвенно свидетельствующих о возможном криминальном происхождении перемещаемых денежных средств.

Статья 4

Совершенствование законодательной базы

1. Признать целесообразным предварительно обсуждать руководством МВД России и руководством АРБ предложения по совершенствованию законодательства, обеспечивающего безопасность банковской деятельности, направляемые субъектам законодательной инициативы.