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

Кафедра оперативно-разыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему: «Организация и тактика выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну»

Выполнил:
Нургалиев Марсель Маратович,
специальность – Правоохранительная деятельность, год набора 2017,
072 учебная группа
Руководитель:
Кандидат юридических наук, доцент,
доцент кафедры оперативно-разыскной деятельности КЮИ МВД России
Музеев Айдар Иршатович
Рецензент: Начальник отделения по раскрытию преступлений совершенных с использованием информационно-телекоммуникационных технологий ОУР УМВД России по г. Казани старший лейтенант полиции
Алиев Валех Мубаризович

Дата защиты «___» _____2022 г. Оценка _____

Казань 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1. ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ ИНТЕРНЕТ 9

§1. Общая характеристика преступлений, совершаемых в сфере предоставления услуг интернет 9

§2. Особенности организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну 18

ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ ОРГАНИЗАЦИИ И ТАКТИКИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ УР МОШЕННИЧЕСТВ В СЕТИ ИНТЕРНЕТ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ БАНКОВСКУЮ ИЛИ ПЕРСОНАЛЬНУЮ ТАЙНУ 37

§1. Проблемы раскрытия мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну 37

§2. Совершенствование деятельности оперативных подразделений уголовного розыска в раскрытии мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну 45

ЗАКЛЮЧЕНИЕ 56

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 61

ВВЕДЕНИЕ

Актуальность. Современные технологии стремительно развиваются и невольно происходит коллаборация таких технологий практически во все сферы жизнедеятельности общества. В настоящий момент идет активное внедрение искусственного интеллекта, облачного хранения информации, дистанционного банковского обслуживания, технологии блокчейн и др. От этого большинство персональной информации граждан попадает в различные информационные системы, например, путем отправки различных документов (договоры, документы, удостоверяющие личность и другую информацию, являющуюся коммерческой, банковской или персональной тайной) посредством электронной почты, в социальных сетях и иных мессенджерах.

Однако, процесс цифровизации оказал влияние и на состоянии преступности, так как существования частной жизни граждан и деятельность различных государственных и частных учреждений окажутся под угрозой. Так, согласно данным ГИАЦ МВД России, за 2017 год было совершено 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, а в 2021 году их количество составило 517722. Количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, за последние 5 лет увеличилось почти в 6 раз. Также, согласно статистике МВД России, за последние 5 лет увеличилось число преступлений в сфере компьютерной информации в 4 раза, если в 2017 году было зарегистрировано 1883 таких преступлений, то в 2021 году – 6869. За 2017 год было совершено 222772

мошенничеств (ст.ст. 159-159.6), а за 2021 год – 249249, чем также подтверждается увеличение указанных преступлений в 1,5 раза[1].

Проблемам защиты персональных данных уделяется внимание и в различных действующих государственных документах. Например, в государственной программе «Информационное общество 2011–2020»[2] указывается на факт неконтролируемого роста объемов информации о гражданах и отсутствие эффективных механизмов контроля ее использования, прежде всего в государственных информационных системах, как самая актуальная угроза современного общества. В Новой редакции Доктрины информационной безопасности Российской Федерации[3] отмечается увеличение преступлений против неприкосновенности частной жизни, персональной, личной, банковской и семейной тайны при обработке персональных данных с использованием информационных технологий. В действующей Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы по вопросам защиты данных и информации указывается на «необходимость соблюдения баланса между своевременным внедрением современных технологий обработки данных с защитой прав граждан, включая право на личную и семейную тайну».

Разглашение или использование в личных корыстных и преступных мотивах сведений (об операциях, о счетах и вкладах, составляющих тайну, может причинить вред не только гражданину, чьи сведения использовались, но и обществу в целом. Понимание того, что включается в понятие банковской тайны, а также персональных данных клиента, которые неразрывно связаны между собой является принципиально важным

---

[1] Состояние преступности МВД России [Электронный ресурс]: база данных содержит сведения о всех видах преступлений. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/5/ — дата обращения: 22.01.2022.

[2] О государственной программе Российской Федерации «Информационное общество 2011–2020» : Утверждена Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р — Российская газета. – 2010. – 6 ноября.

[3] Доктрина информационной безопасности Российской Федерации : Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 — Российская газета. — 2016. – 6 декабря.

моментом для выявления оперативными подразделениями уголовного розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

Таким образом, согласно приведенной выше статистике совершенных преступлений в сети Интернет, а также отмеченной в решении Координационного совещания руководителей правоохранительных органов Российской Федерации от 23 сентября 2016 г. № 2 «Об эффективности работы по выявлению, пресечению, расследованию и предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий», и в решении Коллегии МВД России от 24 октября 2017 г. № 3 «О мерах по совершенствованию раскрытия и расследования мошенничеств», можно говорить о том, в МВД России недостаточно хорошо организована тактика выявления и документирования оперативными подразделениями мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

В Постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняются проблемы, которые возникают при правоприменении норм уголовного и уголовно-процессуального законодательства по данному направлению деятельности[1].

Важной проблемой при является то, что организация работы по проведению процессуальных проверок по сообщениям о преступлениях в сфере современных информационно-коммуникационных не отвечает требованиям организация работы по проведению процессуальных проверок. Таким образом, вышеописанные обстоятельства указывают на низкое качество работы МВД России и судебной системы, так как часто не

[1] О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 — Российская газета. — № 280 —11.12.2017.

принимаются необходимые меры к возмещению ущерба, причиненного данными преступлениями.

Степень научной разработанности темы исследования определяет место настоящего исследования в конкретной области знаний.

Объектом настоящего исследования выступают общественные отношения, связанные с организацией и тактикой выявления и документирования оперативными подразделениями уголовного-розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

Предметом исследования являются правовые нормы, материалы правоприменительной практики, теоретический данные и доктрины о преступлениях, совершенных в сети Интернет с использованием сведений, составляющий банковскую или персональную тайну.

Целью настоящей работы является исследование и анализ организации и тактики выявления и документирования оперативными подразделениями уголовного-розыска мошенничеств в сети Интерне, совершенных с использованием сведений, составляющий банковскую или персональную тайну. Для достижения указанной цели, необходимо решить следующие **задачи**:

1. Выявить особенности организации раскрытия преступлений, совершаемых в сфере предоставления услуг Интернет.
2. Проанализировать и выявить способы совершенствования организации и тактики выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

Методологическую основу исследования составляют базовые положения науки оперативно-розыскной деятельности, а также общенаучные методы познания (анализ и синтез), в том числе, системный метод, а также

частно-научные методы: историко-правовой, формально-юридический, сравнительно-правовой.

Краткая характеристика основных положений.

В ходе исследования было установлено, что преступления совершаются посредством использования программного обеспечения, компьютерных устройств и иной современной техники, а также совершения действий, которые сложно контролировать государственным и иным органам. Информация, которая является объектом посягательства представлена в математическом, символьном и другом виде и содержит сведения о различных лицах, фактах, событиях, явлениях и процессах.

В работе предлагаются решения названных проблем, в частности – внесения изменений в законодательстве, а именно в ст. 26 Федерального закона «Об оперативно-розыскной деятельности»:

- ст. 26 «….Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-разыскную деятельность, при выполнении ими функций по выявлению, предупреждению, пресечению раскрытию и расследованию преступлений по их запросам, направляемым в суд в порядке, предусмотренном статьей 9 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности»….».

Теоретическую основу исследования составили труды ученых из различных сфер научной деятельности, таких как теории государства и права, Административного, информационного права, социологии, уголовного права, криминологии и оперативно-розыскной деятельности. В настоящем исследовании были использованы научные работы следующих ученых: А.Б. Агапова, Т.В. Аверьяновой, С.С. Алексеева, А.А. Антопольского, А.Г. Арешева, Ю.М. Батурина, В.Б. Вехова, О.В. Волохова, Е.К. Волчинской, Р.Б. Головкина, В.А. Копылова, Д.И. Крутиковой, В.Н. Лопатин, В.А., Мазуров,

И.В. Смолькова, Э.В. Талапина, Л.К. Терещенко, Ю.А. Тихомирова, Л.С. Явича и др. Также были использованы труды молодых ученых В.Е. Зварыгина, А.Г. Курникова, Н.А. Падалкина и др.

Нормативную базу исследования составили Конституция Российской Федерации, федеральные конституционные и федеральные законы (Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О персональных данных», Федеральный закон «О банках и банковской деятельности», Федеральный закон «Об оперативно-розыскной деятельности» и др.), Гражданский кодекс РФ, Уголовный Кодекс РФ, указы Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации и иные нормативно-правовые акты.

Эмпирическую базу исследования составили статистика МВД РФ, материалы судебной практики, правоприменительной практики.

Апробация работы. Основные положения, выводы и предложения, которые были сформулированы в процессе написания выпускной квалификационной работы отражены при подготовке научной работы по одноименной теме, занявшей 2-е призовое место в конкурсе Казанского юридического института МВД России.

Структура работы. Настоящая работа состоит из введения, двух глав, заключения и списка использованной литературы.

ГЛАВА 1. ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ ИНТЕРНЕТ

§1. Общая характеристика преступлений, совершаемых в сфере предоставления услуг интернет

Цифровизация и внедрение современных технологий в различные сферы жизнедеятельности общества делают жизнь человека значительно комфортнее, удобнее и проще. Например, чтобы подписать с банком договор или получить информацию о своих расчетных счетах, выписках и прочее, не обязательно ехать в банк, можно просто направить запрос посредством использования сети «Интернет». Однако, современные технологии стали использоваться и в криминальной деятельности, технически оснащая преступников и облегчая им совершение противоправных деяний. Использование технических новшеств позволяет преступникам взаимодействовать между собой и координировать свои действия, тем самым избегая ответственности. Например, некоторые преступные группы могут создаваться в сети «Интернет» и участники могут не знать друг друга.

Конституция Российской Федерации защищает право человека на частную жизнь, личную и семейную тайну и никто не вправе без согласия лица осуществлять сбор, хранение, использование и распространение информации о его частной жизни[1]. В Постановлении Конституционного суда Российской Федерации разъясняется, что в случае, если в сети «Интернет» были обнародованы сведения личного характера определенного лица, которые были размещены без согласия лица или не соответствующие

[1] Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 — Официальный интернет-портал правовой информации http://www.pravo.gov.ru — ст. 23-24.

действительности, по заявлению потерпевшего лица должны быть удалены из свободного доступа и отказ в данных действиях означает отказ в защите чести и достоинства гражданина, его доброго имени и репутации[1]. Но лицо, чьи данные были использованы, не всегда может сразу увидеть распространение информации, составляющих личную тайну, банковскую и др.

На сегодняшний день, преступления, совершаемые с использованием компьютерных технологий, развиваются достаточно быстро, что сделало их предметом изучения и исследования ученых с позиций уголовного права, криминологии, криминалистики и многих других наук.

Такое разнообразное видение на проблему приводит к тому, что отсутствует единое понятия преступлений, совершаемых с использованием компьютерных технологий. Некоторые ученые понятие преступлений, совершаемых с использованием компьютерных технологий, соотносят с понятием «Киберпреступления», «Компьютерные преступления», «Преступления в сфере компьютерной информации». В настоящий момент в праве отсутствует единый подход к разрешению данного вопроса.

Под киберпреступлением во некоторой правовой литературе понимается такая преступная деятельность, цель которой состоит в неправомерном использовании компьютера или компьютерной сети (сетевого устройства).

Также, по мнению исследователя Кочкиной Эльвиры Леонидовны, киберпреступление следует понимать, как совокупность преступлений, которые запрещены Уголовным кодексом Российской Федерации и совершаются в киберпространстве, где основными непосредственными объектами преступного посягательства выступают:

- конституционные права и свободы человека и гражданина;

---

[1] По делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации : Постановление Конституционного суда Российской Федерации от 09.07.2013 №18-П/2013 — Российская газета. — 19.07.2013.

- общественные отношения в сфере компьютерной информации и информационных технологий;
- общественные отношения в сфере экономики и экономической деятельности;
- общественные отношения в сфере государственной власти;
- общественные отношения в сфере здоровья населения и общественной нравственности[1].

Можно сделать вывод о том, что киберпреступления включают в себя широкий спектр общественных отношений, огромное разнообразие способов совершения преступлений и обладают высокой общественной опасностью, так как подрывают информационную безопасность общества, общественный порядок государства в целом, а также наносят угрозу жизни и здоровья граждан.

Ученые-правоведы высказывают единое мнение о том, что борьба с киберпреступлениями должна осуществляться на международном уровне. Автор придерживается подобной позиции и также считает, что для того, чтобы механизмы выявления, расследования и раскрытия киберпреступности были эффективными необходимо активное международное сотрудничество взаимопомощь, поддержка, а также постоянная актуализация и обновление согласно современным реалиям межгосударственных, внутригосударственных законов.

Термин «компьютерное преступление» впервые появился в зарубежной литературе в начале 60-х годов прошлого века, когда появилась возможность регистрировать случаи совершения преступлений с использованием компьютера[2].

---

[1] Кочкина Э. Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. — 2017. — №3 (17).

[2] Беришвили Р.Ш. Компьютерные преступления // Символ науки. — 2021. — №12-1. — стр. 52-53.

Под компьютерным преступлением, исследователь Беришвили Р. Ш., понимает различные незаконные или неразрешенные законодательством Российской Федерации поведения, которые воздействует на автоматизированную обработку и передачу данных[1].

В юридической литературе существует несколько подходов к определению термина «компьютерные преступления». Одна категория ученых придерживается мнения, что «компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует»[2], а другая категория ученых разделяют мнение о том, что компьютерные преступления необходимо ассоциировать с частью общих всех групп информационных преступлений, так как присутствует мнение о том, что преступления не принято разделять по способам совершения преступлений, а именно по видам технических средств[3]. Есть еще одна позиция ученых, которые рассматривают компьютерные преступления с криминологической точки зрения, где центральным звеном исследования выступает личность преступника и способы совершения преступлений.

Можно сделать вывод о том, категория компьютерных преступлений шире, чем категория преступления в сфере компьютерной информации, однако, она входит в общую группу киберпреступлений.

Законодатель выделяет преступления в сфере компьютерной информации отдельно от иных преступлений, так как общественная опасность рассматриваемой категории преступлений заключается в посягательстве на общественные отношения в сфере компьютерной информации, являющейся технологически сложной и более распространённой в повседневном использовании.

---

[1] Беришвили Р.Ш. Компьютерные преступления // Символ науки. — 2021. — №12-1. — стр. 52-53.

[2] Коротких Н. Н., Останин М. Д. К вопросу о соотношении понятий «преступление в сфере компьютерной информации» и «компьютерное преступление» // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2018. — №3. — стр. 73.

[3] Коротких Н. Н., Останин М. Д. К вопросу о соотношении понятий «преступление в сфере компьютерной информации» и «компьютерное преступление» // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2018. — №3. — стр. 74.

В правовой литературе выделяют несколько групп компьютерных преступлений:

1. Преступления, совершаемые с применением компьютера:

- компьютерные преступления против государственной власти (государственная измена, шпионаж, разглашение государственной тайны[1]);
- компьютерные преступления экономического характера (кража, мошенничество[2], хищение предметов, которые имеют особую ценность и др.);
- компьютерные преступления против общественной безопасности и общественного порядка (заведомо ложное сообщение об акте терроризма (сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей, общества[3]);
- компьютерные преступления против личности, нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений[4].

2. Преступления в сфере компьютерной информации - незаконный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети[5].

Таким образом, под преступлениями в сфере компьютерной информации, автор понимает, предоставление незаконного доступа к компьютерной информации или противоправное деяние, посягающее на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

---

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст.ст. 275 – 276, 283.

[2] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст.ст. 159 – 159.6.

[3] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст.ст. 207, 237.

[4] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст.ст. 128.1, 138.

[5] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст.ст. 272-274.

Так, в 2017 году было зарегистрировано 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. За 2018 год было зарегистрировано 174674 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, за 2019 год было зарегистрировано 294409 аналогичных преступлений, за 2020 год в ГИАЦ МВД России было зарегистрировано 510396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, а в 2021 году – 517722 преступлений[1].

Рисунок 1.1

На рисунке 1.1 четко прослеживается рост количества данного вида преступлений. Данный феномен подтверждает все то, что было указано выше, а именно то, что в настоящее время современные информационные и телекоммуникационные технологии уже целиком овладели всеми сферами человеческой деятельности и недостаточный контроль государственных органов приводит к тому, что создается благоприятная обстановка для преступников в рассматриваемой сфере.

---

[1] Состояние преступности МВД России [Электронный ресурс]: база данных содержит сведения о всех видах преступлений. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/5/ — дата обращения: 22.01.2022.

Первым зарегистрированным в России, а точнее в РСФСР, стало противоправное деяние, которое было совершено в 1983 году (в августе) в г. Тольятти на Волжском автомобильном заводе. Данное преступление было резонансным ввиду отсутствия подобных деяний. Программист внес изменения в программу ЭВМ, которая отвечала за подачу механических узлов на главный сборочный конвейер для того, чтобы отомстить администрации. В конечном итоге 200 легковых автомобилей не смогли в установленное время сойти с конвейера, и заводу был причинен ущерб в размере 1 млн. рублей. Виновного обвинили в совершении преступления по ч. 2 ст. 98 УК РСФСР (повреждение государственного имущества, причинившее крупный ущерб) и назначили 3 года лишения свободы условно с возмещением причиненного ущерба[1].

В Российской Федерации принятия Федерального закона № 420 от 7 декабря 2011 г. «О внесении изменений в Уголовный кодекс Российской федерации и отдельные законодательные акты Российской Федерации»[2] и Федерального закона № 207 от 29 ноября 2012 г. «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[3], положение главы 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации были тщательно переработаны и актуализирована ответственность за совершение преступлений с использованием компьютерных технологий, а также были введены такие составы преступлений как мошенничество с использованием платежных карт, а также мошенничество в сфере компьютерной информации.

---

[1] Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. — 2020. — №1.

[2] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Текст]: Федеральный закон от 07.12.2011 № 420-ФЗ — Российская газета. — 09.12.2011.

[3] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Текст]: Федеральный закон от 29.11.2012 № 207-ФЗ — Российская газета. — 03.12.2012.

Автор выделил следующие особенности преступлений, совершаемых в сфере предоставления услуг Интернет:

1. Преступления совершаются посредством использования программного обеспечения, компьютерных устройств и иной современной техники, а также совершения действий, которые сложно контролировать государственным и иным органам. Информация, которая является объектом посягательства представлена в математическом, символьном и другом виде и содержит сведения о различных лицах, фактах, событиях, явлениях и процессах и др.

2. Способы совершения преступления уникальны.

3. Трансграничный характер преступных деяний. Преступники при совершении своих преступлений могут находится в любой точке мира, где есть доступ к сети «Интернет».

4. Высокий уровень латентности рассматриваемых преступлений[1]. По проведенным исследованиям, специалисты указывают на примерные данные уровня латентности, которые составляют 90%[2]. Важную роль играет то, что потерпевшие не всегда обращаются в правоохранительные органы за помощью в подобных случаях, а некоторые даже не знают, что в отношении их совершили преступное посягательство.

5. Данная категория преступлений обладает высокой степенью профессионализма и скрытности. Лица, совершающие преступления в сети «Интернет» обладают специальными знаниями, навыками и умениями в области информационно-телекоммуникационных технологий, программирования и защиты информации. При исследовании практических материалов по преступлениям, совершаемых в сфере предоставления услуг Интернет, можно говорить о том, лица, которые совершали подобные преступления, имели высшее или/и среднее специальное образование

---

[1] Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет // дисс.. канд. юр. наук // Волгоград. — 2008. — стр. 45

[2] Число интернет-преступлений в России [Электронный ресурс]: Коммерсарнт, 2021. — Режим доступа: https://www.kommersant.ru/doc/4654110. – дата обращения 23.01.2022.

(зачастую профильное, связанное с обработкой и защитой конфиденциальной информации). Практически в 80% случаев преступниками являлись сотрудники учреждений, предприятий и/или организаций, которые непосредственно работали с конфиденциальной информацией или использовали специальные интернет-технологии в профессиональной деятельности.

Таким образом, исследуемая категория преступлений является сложной для выявления и расследования оперативными подразделениями МВД России. Однако, количество зарегистрированных преступлений ежегодно растет, так как современные технологии вторгаются во все сферы жизни человека, создаются даже метавселенные, где человек может жить реальной виртуальной жизнью, делать реальные виртуальные покупки, а также совершать настоящие преступления против личности в виртуальной реальности. У государства и государственных органов должна стоять задача разработать и актуализировать механизмы выявления и расследования преступлений, совершаемых в сфере предоставления услуг Интернет.

§2. Особенности организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну

Для того, чтобы проанализировать особенности организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, необходимо исследовать понятия «банковская и персональная» тайна.

Понятие термина «банковская тайна» устанавливается законодателем во многих нормативно-правовых актах. Так, согласно Федеральному закону «О банках и банковской деятельности», банковская тайна – это тайная информация об операциях, о счетах и вкладах клиентов и корреспондентов кредитной организации, Банка России, организации, осуществляющей функции по обязательному страхованию вкладов[1]. Все служащие кредитной организации, Банка России, организации, осуществляющей функции по обязательному страхованию вкладов обязаны гарантировать тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов и сохранение ее, в том числе и иные сведения, устанавливаемые любой из вышеперечисленных организаций.

В Гражданском кодексе Российской Федерации под банковской тайной понимаются сведения по банковскому счету и банковскому вкладу, по операциям производимым по счету и иных сведений о клиенте[2].

Банк, различные кредитные организации, а также организации, осуществляющие функции по обязательному страхованию вкладов, дают гражданам, которые являются клиентами данных учреждений, гарантию

---

[1] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 05.02.1996. — ст. 26

[2] Гражданский кодекс Российской Федерации (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ. — Собрание законодательства РФ. — 29.01.1996. — ст. 857

сохранения информации об операциях, сведениях по расчетным счетам и иных данных о клиенте в тайне.

В банковскую тайну физического лица входят следующие сведения:

- о его операциях, в том числе осуществляемых банковскими платежными агентами (субагентами), о счетах и вкладах в банке;
- об остатках и переводах электронных денежных средств;
- персональные данные физического лица (клиента).

В качестве условий привлечения к ответственности выступают доказательства разглашения указанных сведений (любые письменные или электронные документы, из которых следует, что банковская тайна физического лица стала известна ненадлежащему субъекту).

В настоящий момент современное законодательство Российской Федерации предусматривает три вида ответственности за разглашение банковской тайны:

- гражданская ответственность.

Для того, чтобы можно было привлечь Банк, различные кредитные организации, а также организации, осуществляющие функции по обязательному страхованию вкладов, к гражданско-правовой ответственности в виде возмещения убытков физическому лицу, необходимо доказать факт разглашения банковской тайны, наличие и размер убытков физического лица, т.е. реального ущерба или упущенной выгоды. Также необходимо доказать причинно-следственную связь между действиями работников банка или иной соответствующей организации и причиненными убытками. Для этого необходимо в банк подать соответствующее требование или сразу обратиться в суд.

Согласно законодательству, Банк обязан возместить также вред, причиненный его работником при исполнении служебных обязанностей, даже если действия работника вызваны корыстными побуждениями, поскольку банк должен был обеспечить должную осмотрительность при подборе сотрудников, которым доверена банковская тайна, а также

персональные данные клиентов банка.

- Административная ответственность.

Согласно Административному кодексу Российской Федерации, Банк или его работник могут быть привлечены к административной ответственности за разглашение информации с ограниченным доступом. При этом основанием для возбуждения дела об административном правонарушении может быть заявление гражданина в полицию или прокуратуру[1].

- Уголовная ответственность.

Уголовная ответственность наступает в случае, если лицо, которому банковская тайна была доверена или стала известна по службе или работе, разгласило или использовало ее без согласия владельца, в том числе если это причинило крупный ущерб или было совершено из корыстной заинтересованности либо повлекло тяжкие последствия[2].

Для возбуждения уголовного дела необходимо направить в органы внутренних дел (полицию) сообщение о преступлении[3].

С банковской тайной неразрывно связана персональная тайна. В настоящий момент законодатель не закрепляет ни в одном нормативно-правовом акте понятия «персональная тайна». Так, Прокуратура Ставропольского края в своих разъяснениях указывает, что личная и семейная тайна - элементы частной жизни физического лица[4]. В комментарии к Конституции Российской Федерации под частной жизнью понимаются определенные стороны личной жизни человека, которые он в

---

[1] Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 07.01.2002. — ст.ст. 13.14, 28.1.

[2] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996. — ст. 183.

[3] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ. — Собрание законодательства РФ. — 24.12.200. — ст. 140.

[4] Право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23, 24 Конституции России) [Электронный ресурс]: Прокурор разъясняет, 2021 год —Режим доступа: https://epp.genproc.gov.ru/ru/web/proc_26/activity/legal-education/explain?item=61977689 — дата обращения 24.01.2022.

силу своей свободы не желает делать достоянием других[1]. В данном случае тайна рассматривается со стороны желания и стремления каждого человека на собственный мир, который скрыт от чужих глаз, а не на возможность прикрыть свою противоправную деятельность.

Согласно Определению Конституционного Суда РФ от 09.06.2005 № 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» под правом на неприкосновенность частной жизни понимается предоставление государством гарантированную Конституцией Российской Федерацией возможность контролировать гражданину информацию о самом себе, а также препятствовать разглашению личной или интимной информации[2].

Сперанская Л. В. под частной жизнью понимает индивидуальное и собственное пространство личности определенного гражданина[3].

При анализе законодательства Российской Федерации, автор выделил те сведения, которые относятся к тайне частной жизни относятся:

1. Личные сведения о происхождении гражданина, о месте пребывания и жительства гражданин, о личной, семейной жизни[4].

2. Сведения, которые связаны с профессиональной деятельностью гражданина и доступ к которым ограничен Конституцией Российской Федерации или/и иными нормативно-правовыми актами[1].

---

[1] Бархатова Е.Ю. Комментарий к Конституции Российской Федерации: новая редакция (постатейный). — 3-е изд., перераб. и доп. М.: Проспект, 2020. — ст. 23

[2] Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации: Определение Конституционного Суда РФ от 09.06.2005 № 248-О.

[3] Сперанская Л.В. Право на неприкосновенность частной жизни // СПС КонсультантПлюс. — 12.01.2022

[4] Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ. — Собрание законодательства РФ. — 05.12.1994. — ст. 152.2

3. Сведения о персональных данных[2].

4. Тайна усыновления[3].

5. Тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи[4].

6. Сведения об абонентах и оказываемых им услугах связи[5].

7. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, которые составляют врачебную тайну[6].

8. Сведения о страхователе и застрахованном лице, состоянии их здоровья, а также имущественном положении этих лиц[7].

9. Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю[8].

10. Банковская тайна[9].

11. Аудиторская тайна и иные данные.

Таким образом, автор под персональной тайной понимает сведения, относящиеся к тайне личной жизни гражданина, на которые направлены по желанию гражданина все установленные законодательством Российской Федерации средства и способы защиты данной информации, разглашение,

---

[1] Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 —Российская газета. — 14.03.1997

[2] О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ. — Российская газета. — 29.07.2006. — ст. 3

[3] Семейный кодекс Российской Федерации: Федеральный закон от 29.12.1995 № 223-ФЗ — Российская газета. — 27.01.1996. — ст. 139.

[4] О почтовой связи: Федеральный закон от 17.07.1999 № 176-ФЗ — Российская газета. — 22.07.1999. — ст. 15.

[5] О связи: Федеральный закон от 07.07.2003 № 126-ФЗ — Российская газета. — 10.07.2003. — ст. 53.

[6] Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ— Российская газета. — 23.11.2011. — ст. 13.

[7] Гражданский кодекс Российской Федерации (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ. — Собрание законодательства РФ. — 29.01.1996. — ст. 946

[8] Об адвокатской деятельности и адвокатуре в Российской Федерации: Федеральный закон от 31.05.2002 № 63-ФЗ — Российская газета. — 05.06.2002 —ст. 8

[9] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 05.02.1996. — ст. 26

распространение и использование третьими лицами которой могло бы повлечь для гражданина неприятные последствия.

В настоящее время с проникновением в жизнь общества современных технологий появились новые как новые преступления, так и новые способы совершения старых преступлений, регламентированных в законодательстве Российской Федерации.

Так, одним из распространенных преступлений в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, является мошенничество. Ущерб, причиняемый данным видом преступления, и выбор преступниками в качестве своих жертв социально незащищенной категории граждан, таких как инвалиды, либо пожилые люди, обуславливают повышенное внимание государственных органов и общества к результатам противодействия этим преступлениям.

Так, за 2017 год было выявлено 222772 преступлений, регламентированных ст.ст. 159 – 159.6 Уголовного кодекса Российской Федерации, за 2018 год было зарегистрировано 215036 мошеннических действий по аналогичным преступлениям. Снижение количества данных преступлений можно объяснить тем, что в 2018 году постепенно стал осуществляться переход к информационному обществу, о чем подтверждается указами Президента Российской Федерации «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[1], «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»[2], «Об утверждении Доктрины информационной безопасности Российской Федерации»[3], Основными направлениями деятельности Правительства

---

[1] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента РФ от 07.05.2018 № 204— Российская газета. — 09.05.2018.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: Указ Президента РФ от 09.05.2017 № 203— Собрание законодательства РФ. — 15.05.2017.

[3] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 — Собрание законодательства РФ. — 12.12.2016.

Российской Федерации на период до 2024 года, утвержденными Председателем Правительства Российской Федерации от 29 сентября 2018 г., и иными нормативно-правовыми актами, что привело к еще большей степени латентности рассматриваемых преступлений за данный период.

За 2019 год было зарегистрировано уже 257187 преступлений, регламентированных ст.ст. 159 – 159.6 Уголовного кодекса Российской Федерации, в 2020 – 335631 мошеннических действий, а в 2021 году – 339606 мошеннических действий[1].

Рисунок 2.1

Как показано на рисунке 2.1 количество зарегистрированных преступлений ежегодно растет.

В настоящее время МВД России столкнулось с такой проблемой как отсутствие единого мнения среди ученых и практиков о содержании оперативно-розыскной характеристики таких преступлений.

Так, по мнению П. И. Иванова, к наиболее значимым элементам организации раскрытия преступлений относятся:

[1] Состояние преступности МВД России [Электронный ресурс]: база данных содержит сведения о всех видах преступлений. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/5/ — дата обращения: 22.01.2022.

- Реальная статистика совершаемых преступлений;
- структура преступности;
- место, способ совершения преступлений и предмет преступного посягательства;
- общий портрет личности преступников[1].

А. М. Абрамов включает следующие оперативно-розыскной элементы:

- Уголовно-правовые, в том числе и недостатки судопроизводства по делам о преступлениях, вынесение необоснованно мягких приговоров.
- Криминологические. Согласно его мнению, криминологическая характеристика данного вида преступлений может обуславливать специфику всей оперативной работы сотрудников МВД России.
- Криминалистические. А. М. Абрамов отмечает, что данные признаки оказывают влияние на организацию и тактику работы по выявлению и документированию преступной деятельности разрабатываемых и предопределяют основные направления взаимодействия служб и подразделений органов внутренних дел.
- Нравственно-психологические. А. М. Абрамов утверждает, что данные признаки помогут определить особенности оперативной работы в среде лиц, которые могут быть причастны к совершению рассматриваемых преступлений.
- Специальные, которые включают в себя особенности использования негласных сотрудников; обстоятельства, облегчающие и осложняющие в различных ситуациях процесс оперативной разработки; лица, состоящие на оперативном учете в органе внутренних дел из числа ранее судимых, от которых можно ожидать совершения преступлений.

Автор придерживается мнения, что рассматриваемые выше признаки необходимы для правильного построения модели организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с

---

[1] Бегишев, И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, — 2020. — стр. 106.

использованием сведений, составляющий банковскую или персональную тайну.

Так, согласно статье для граждан с целью предотвратить совершение преступления, написанной Управлением МВД России по Костромской области в 2022 году, основными видами мошенничества в сети Интернет стали[1]:

1. Сообщение «Ваша банковская карта заблокирована». Нарушая персональную и банковскую тайну гражданина, преступники используют данные банковской карты. Таким образом происходит хищений денежный средств со счетов гражданина, который идет на уловки мошенников.

2. Различные виды телефонного мошенничества (родственник попал в беду, телефонный номер грабитель, смс-просьба о помощи и другие).

3. Остальные виды мошенничества с использованием сети Интернет.

При совершении противоправных действий мошенниками осуществляется неправомерный доступ к личной информации граждан, к банковской и персональной тайне:

• путём обмана в процессе общения по электронной почте, либо иной переписки в социальных сетях, Skype и т. д.;

• путём «фишинга»;

• путём подбора паролей, восстановления пароля пользователя;

• иными способами.

По мнению автора, сложность в организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений,

---

[1] Виды мошенничества в интернете [Электронный ресурс]: Управление МВД России по Костромской области. — Режим доступа: https://44.xn--b1aew.xn--p1ai/Dlja_grazhdan/%D0%BE%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D0%BE%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%B8-/%D0%B2%D0%B8%D0%B4%D1%8B-%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0-%D0%B2-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5 — (дата обращения: 25.01.2022).

составляющий банковскую или персональную тайну, заключается в следующих обстоятельствах:

- высокой степени латентности рассматриваемого вида преступности. Данное явление можно объяснить тем, что некоторые потерпевшие не сразу понимают, что в отношении них было совершено преступление, а многим не хочется проходить огромное количество бюрократических процедур при доказывании совершения преступления, а также подрыв доверия граждан к правоохранительным органам и опасениями потерпевших о выполнении преступниками угроз в случае непрофессиональных действий сотрудников правоохранительных органов;
- отсутствие физического контакта, приводящее к обезличиванию преступников и потерпевших, которое исключает возможность их опознания преступников в ходе следственных действий;
- использование мошенниками для общения с потерпевшими гражданами электронных почтовых ящиков, которые зарегистрированы на зарубежных Интернет-сервисах, систем электронных сообщений Skype и др., что способствует затруднению в установлении владельцев данных систем;
- использование мошенниками информации, относящейся к банковской и персональной тайне потерпевших граждан;
- использование мошенниками для получения денежных средств от потерпевших граждан электронных платёжных систем или банковских карт, которые оформлены на подставных лиц, что существенно затрудняет идентификацию фактического получателя денежных средств.

Важнейшую роль при организации расследования рассматриваемого вида мошенничества, по мнению автора, играют оперативно-розыскные мероприятия: опросы, исследование предметов и документов, получение компьютерной информации[1].

---

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995. — ст. 6

Опрос – это оперативно-розыскное мероприятие, которое заключается в сборе фактической информации, имеющей значение для решения конкретной задачи оперативными сотрудниками. Опрос проводится с гражданами, которые обладают какой-либо информацией о совершенном преступлении или причастных к нему лицах. Опрос проводится как по месту нахождения указанных выше граждан, так и в служебных помещениях правоохранительных органов. Результаты опроса в случае согласия опрашиваемого лица могут быть оформлены объяснением (заявлением, явкой с повинной) либо рапортом (справкой) должностного лица. Если информация получена при условии конфиденциальности, то рапорт (справка) хранится и используется по правилам секретного делопроизводства и к материалам уголовного дела приобщен быть не может.

Также важным оперативно-розыскным мероприятием (далее ОРМ) является исследование предметов и документов. Данный вид оперативно-розыскной деятельности, заключается в изучении предметов и документов лицом, обладающим специальными познаниями, с целью проверки, не являются ли исследуемые предметы и документы средствами или орудиями преступления, а также с целью выявления их особенностей и признаков в сфере расследуемого преступления. Данное ОРМ проводится на основании письменного обращения руководителя оперативного подразделения к руководителю экспертно-криминалистического подразделения либо к иным лицам (на возмездной основе).

И одно из важных ОРМ при организации раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, является получение компьютерной информации. Данное ОРМ достаточно новое, введенное лишь в 2016 году.

Под получением компьютерной информации необходимо понимать получение оперативными сотрудниками сведений, функционирующих на машинных носителях компьютерной информации, в том числе полученных

из сети Интернет, и их фиксация путем съема техническим специальными средствами характеристик электромагнитных полей, возникающих при обороте компьютерной информации в сети электрической связи.

Данный вид ОРМ ограничивает конституционные права граждан, поэтому может быть осуществлено как на основании судебного решения, так и без такого основания по веским доводам, регламентированным Законом «Об оперативно-розыскной деятельности». Рассматриваемое ОРМ проводится с использованием оперативно-технических сил органов внутренних дел и органов федеральной службы безопасности. Результаты получения компьютерной информации оформляются справкой, рапортом или актом. При необходимости данные материалы могут быть использованы следователем в качестве доказательств.

Согласно Федеральному закону от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», основаниями для проведения вышеуказанных оперативно-розыскных мероприятий являются[1]:

1. Наличие возбужденного уголовного дела.

2. Ставшие известными органам, осуществляющим оперативно-розыскную деятельность, сведения о:

1) признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;

2) событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации;

3) поручения следователя, руководителя следственного органа, дознавателя, органа дознания или определения суда по уголовным делам и

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995. — ст. 7

материалам проверки сообщений о преступлении, находящимся в их производстве;

4) запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье;

5) иные основания в соответствии с законодательством Российской Федерации.

Также законодательством установлены случаи, срочного проведения оперативно-розыскных мероприятий:

1)случаи, не терпящих отлагательства и которые могут привести к совершению тяжкого или особо тяжкого преступления;

2) при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

Руководитель органа, осуществляющий оперативно-розыскную деятельность, выносить мотивированное постановление, на основании которого допускается проведение вышеуказанных оперативно-розыскных мероприятий. Однако, законодатель указывает, что в случае срочного проведения оперативно-розыскных мероприятий, необходимо уведомить суд в течение 24 часов. В течение 48 часов с момента начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение[1].

Оперативные подразделения системы МВД России при наличии оснований для проведения ОРМ с целью выявления, предупреждения, пресечения и раскрытия преступлений, в том числе выявления и установления лиц, их подготавливающих, совершающих или совершивших, а также с целью осуществления розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также

---

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995. — ст. 9

розыска без вести пропавших, добывания информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации и установление имущества, подлежащего конфискации[1], создают и используют в своей деятельности специальные информационные системы и заводят дела оперативного учета.

При наличии всех вышеуказанных оснований, дела оперативного учета (далее – ДОУ) заводятся с целью систематизировать сведения, проверки и оценки результатов оперативно-розыскной деятельности и принятия решений органами, которые осуществляют оперативно-розыскную деятельности.

Вся информация, отраженная в ДОУ о лица, в отношении которых проводятся оперативно-розыскные мероприятия, попадает в специальный банк данных[2].

При заведении ДОУ ему присваивается название в соответствии с классификацией ДОУ, которая применяется оперативными сотрудниками МВД России и разрабатывается с учетом признаков конкретных составов преступлений, проверка обстоятельств вероятного совершения которых относится к оперативно-розыскной подведомственности соответствующего оперативно-розыскного органа. Название ДОУ отражается в постановлении о заведении ДОУ. Однако, название может быть изменено постановлением, в том случае, если будет получена информация, которая непосредственно влияет на изменение классификации. Все решения, которые принимается по материалам ДОУ, должны быть оформлены постановлением о заведении ДОУ, о прекращении ДОУ, о продлении и др.

---

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995. — ст. 2

[2] О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ— Российская газета. — 10.02.2011. — ст. 17

Прекращение ДОУ может быть осуществлено только на основании решения руководителя оперативно-розыскного органа, а также в связи с наличием следующих оснований:

- решение конкретных задач оперативно-розыскной деятельности, предусмотренных ст. 2 Закона «Об оперативно-розыскной деятельности»;
- установление обстоятельств, свидетельствующих об объективной невозможности решения задач, указанных в ст. 2 Закона «Об оперативно-розыскной деятельности» (напр., получение достоверной информации о не подтверждении сведений, на основании которых было заведено ДОУ).

В случае, если виновность лица, на которое заведено ДОУ не будет доказана, то ДОУ хранится в течение 1 года, а затем уничтожается. Однако, существенные сведения, указанные в ДОУ, переносятся в специализированные информационные системы.

ДОУ делятся на дела оперативной проверки и дела оперативной разработки в зависимости от решаемых задач, полномочий и специфики деятельности оперативно-розыскных органов. Отличие указанных видов ДОУ состоит в том, что дело оперативно проверки заводится с целью осуществить проверку определенного лица (субъекта), на вероятную причастность к совершению им преступления, а дело оперативной разработки заводится в случаях, когда имеются проверенные данные о совершенном преступлении.

В качестве нового вида социального пространства Интернет накладывает отпечаток на стратегию и тактику раскрытия и расследования преступлений. Возникающая при его использовании социальная среда порождает специфические виды социальных взаимодействий, сложнейшие процессы детерминации преступности, неизвестные ранее образцы криминальных формирований, без учета которых эффективная борьба с преступностью невозможна.

В социальной сети Интернет преступник-мошенник может совершать дистанционно ряд противоправных операций в нескольких вычислительных

системах, направленных на информационный объект, находящийся на значительном расстоянии или не имеющий физической привязки к конкретному месту. Определенные операции могут выполняться с мобильных устройств, в то время как их оператор перемещается в физическом пространстве.

В настоящий момент растет число сайтов, принадлежащих организованным преступным формированиям (ОПФ), через которые происходит обмен информацией и стараются распространить свой преступный образ жизни.

Рассматриваемый вид преступности можно охарактеризовать повышенной скрытностью совершения, обеспечиваемой за счет сложности сетевой инфраструктуры и развитых механизмов анонимности. Многие преступления имеют трансграничный характер, при котором преступник, объект преступного посягательства, жертва находятся под юрисдикцией различных государств. Способы совершения преступлений и применяемых специальных средств отличаются нестандартностью, сложностью, многообразием и частым обновлением. При этом реализация сложных сценариев может осуществляться одним человеком при объединении относительно слабых ресурсов отдельных компьютеров в мощное орудие совершения преступления. К тому же преступники широко обмениваются сведениями о способах совершения преступлений и результатами противоправной деятельности, которые могут использоваться при совершении новых преступлений.

Еще в большей степени затрудняет выявление преступной деятельности в сети Интернет ее многоэпизодный характер при множественности жертв в случаях, когда каждой из жертв наносится нечувствительный ущерб, но в целом преступник получает существенные преступные доходы (например, при снятии незначительных сумм со счетов владельцев кредитных карт). При этом эпизоды преступления, происходящие в пределах различных юрисдикций, по отдельности могут восприниматься

как не связанные друг с другом и не заслуживающие оперативно-разыскного реагирования.

Для организации и тактики расследования и раскрытия преступлений, совершаемых в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, важную роль играет разыскная информация. Под разыскной информацией понимаются данные, которые были получены органами следствия на различных этапах расследования. Автор также под разыскной информацией понимает специальные сведения, которые индивидуализируют объекты розыска (о внешности, особых приметах разыскиваемого, отличительных особенностях похищенных вещей и др.), которые позволяют вести непосредственный розыск.

По мнению Р. С. Белкина, под розыском можно понимать функцию органов дознания и предварительного следствия, а под объектами розыска понимаются такие, которые «находятся вне пределов досягаемости следователя и суда, а доказывание и процессуальная процедура требует реального (физического и психического) взаимодействия с ними и если их местонахождение в настоящий момент не известно».

Одним из самых актуальных и перспективных направлений оперативного поиска в сетевом информационном пространстве стал интернет-мониторинг, который представляет собой комплексную систему наблюдения за состоянием криминальных процессов в сетевой социальной среде, направленную на сбор, обработку и анализ информации о явлениях криминального плана. Основные направления этого мониторинга, способные обеспечить высокую интенсивность поступления криминалистически значимой информации:

а) автоматизированный поиск сетевых информационных ресурсов, содержащих запрещенную к распространению информацию;

б) изучение выявленных сетевых ресурсов, связанных с деятельностью преступных сообществ;

в) наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности.

Поисковые серверы могут применяться также для получения дополнительной информации о пользователе или группе пользователей сети. Сведения о разрабатываемых лицах возможно получить в открытом доступе на их личных страницах в социальных сетях (Одноклассники.ру, ВКонтакте.ру) либо в персональных блогах.

Интернет создает условия для использования новых форм привлечения граждан к содействию в раскрытии и расследовании преступлений. Одним из наиболее простых способов получения информации от граждан в сетевом пространстве может быть создание специализированных сайтов по регистрации сведений, представляющих оперативный интерес. На таких сайтах выделяются страницы, где можно заполнить форму сообщения о совершенных и подготавливаемых преступлениях, о предполагаемых преступниках, их связях и т. п. Передача сведений о противоправной деятельности может осуществляться с сохранением анонимности заявителя. Хотя анонимные сообщения о преступлениях в соответствии с ч. 7 ст. 141 УПК не могут служить поводом для возбуждения уголовного дела, при наличии в них сведений о совершении преступления или приготовлении к совершению преступления их следует рассматривать в качестве оснований для проведения проверочных мероприятий.

Таким образом, количество зарегистрированных преступлений, совершаемых в сети «Интернет», ежегодно растет, а способы совершения данного вида преступлений быстро видоизменяются в соответствии с изменениями общества и внедрения информационных технологий в жизни граждан. Самыми распространенными преступлениями, совершаемыми в сети Интернет, являются преступления с использованием сведений, составляющий банковскую или персональную тайну. Банковская и персональная тайна неразрывно связаны между собой и относятся к конфиденциальной информации граждан, которая защищается

законодательством Российской Федерации. При расследовании вышеуказанных преступлений особую роль играют ОРМ и ДОУ. Использование при проведении ОРМ современных информационных технологий позволит устранить факторы мобильности и скрытности использования современных средств получения, копирования, обработки компьютерной информации в целях борьбы с компьютерной преступностью.

ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ ОРГАНИЗАЦИИ И ТАКТИКИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ УР МОШЕННИЧЕСТВ В СЕТИ ИНТЕРНЕТ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИЙ БАНКОВСКУЮ ИЛИ ПЕРСОНАЛЬНУЮ ТАЙНУ

§1. Проблемы раскрытия мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну

Начиная с 2018 года, количество зарегистрированных преступлений в сети Интернет с использованием с использованием сведений, составляющих банковскую или персональную тайну, увеличилось несколько раз. Это можно также объяснить тем, что в апреле 2018 г. были внесены изменения в ст. 159.3 Уголовного кодекса Российской Федерации, которые расширили средства совершения преступления, а также увеличением электронного оборота финансовых средств, активным использованием гражданами специализированного программного обеспечения, предназначенного для осуществления оплаты товаров и услуг, распоряжения собственными денежными средствами[1].

Согласно данным Банка России, рост количества операций с использованием электронных средств платежа за 2018 г. (32 млрд) относительно аналогичного показателя за 2017 г. (24 млрд) составил 34,6%. Однако, статистика несанкционированных операций с использованием электронных средств платежа за 2018 г. увеличилась на 44,04% (1 384,7 млн руб.) по сравнению с 2017 г.(961,3 млн руб.) (Рис. 3.1).

---

[1] Перетолчин А. П. Применение защитником нормы, устанавливающей ответственность за мошенничество с использованием электронных средств платежа // Адвокатская практика. — 2019. — № 6. — стр. 13.

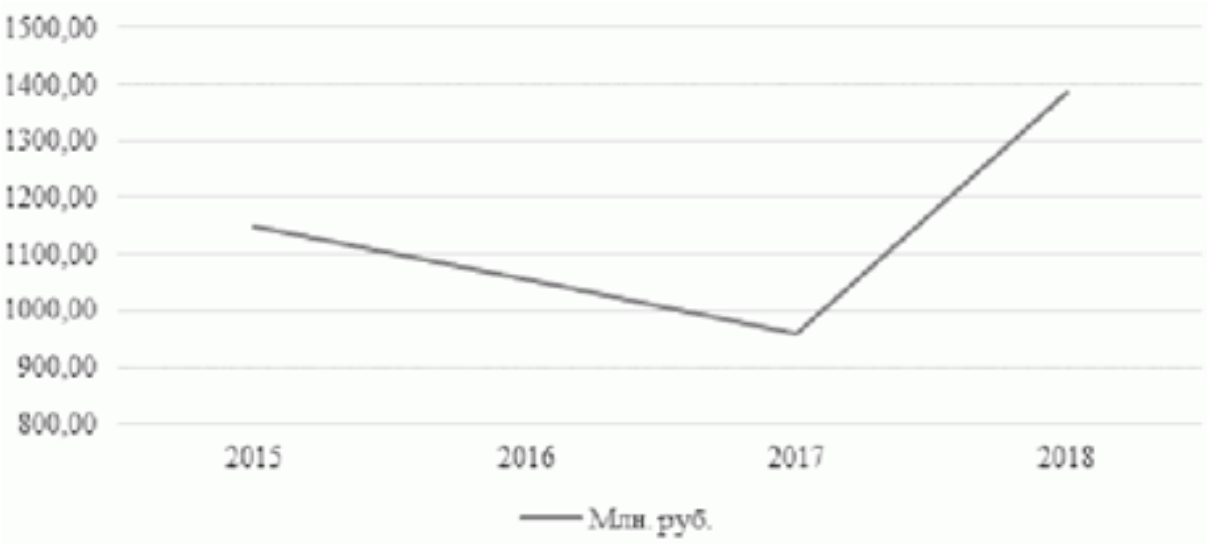

Рисунок. 3.1 Статистика объема несанкционированных операций с использованием электронных средств платежа.

Вышеуказанные данные свидетельствуют и подтверждают высокую степень общественной опасности подобных преступных посягательств, причиняющие вред не только гражданам, но и государству в целом.

На раскрытие и расследование рассматриваемых преступлений влияет множество факторов. Например, на практике решения требует вопрос о том, как необходимо рассматривать в качестве средства платежа подарочные карты или сертификаты, которые были приобретены в коммерческих организациях и дают право приобретения товара на сумму, эквивалентную своей стоимости. На эту тему в настоящий момент происходит множество споров, так как законодатель не дает однозначного ответа.

Также в настоящее время существуют проблемы отграничения преступлений, совершаемых с использованием банковской и персональной тайны, от иных смежных составов преступления.

Так, 10 декабря 2018 г. Кытмановским районным судом Алтайского края было рассмотрено дело в отношении Б., в котором было установлено, что через своего знакомого обвиняемый Б. приобрел сим-карту с целью использования сети Интернет через мобильный модем[1]. Подозреваемый Б.

[1] Перетолчин А. П. Применение защитником нормы, устанавливающей ответственность за мошенничество с использованием электронных средств платежа // Адвокатская практика. — 2019. — № 6. — стр. 14.

активировал свою сим-карту с помощью мобильного телефона и установил в устройство модем, получив доступ в сеть Интернет. 21 августа 2018 г. на номер сим-карты, купленной обвиняемым Б. пришло уведомление с сервисного номера о том, что на карту «Мир» были зачислены денежные средства в размере 27 360 рублей. У обвиняемого Б. такой банковской карты не было, и он осознал, что может получить доступ к зачисленным на банковскую карту «Мир» денежным средствам. Таким образом, у обвиняемого Б. возник умысел на хищение денежных средств с целью оплаты услуг в сети Интернет. Обвиняемый Б. смог осуществить свой умысел путем оплаты услуг в сети Интернет на общую денежную сумму потерпевшего 1 850 руб.

Таким образом, обвиняемый Б. был осужден по п. «г» ч. 3 ст. 158 Уголовного кодекса Российской Федерации, т.е. его действия были квалифицированы органами предварительного следствия и судом как тайное хищение чужого имущества. После вынесение обвинительного приговора у многих ученых-практиков возник вопрос о том, что может ли направление сервисной команды в банк посредством системы интернет-банкинга обвиняемым от имени потерпевшего, рассматриваться как введение в заблуждение специалистов банка относительно личности лица, направившего сервисную команду, и принадлежности ему денежных средств, привязанных к мобильному банкингу.

Также проблемой раскрытия мошенничеств в сети интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну является то, что рассматриваемый вид преступлений имеет сложную структуру. Так, они включают в себя создание и распространение различными техническими средствами вредоносного программного обеспечения или/и вирусных программ для того, чтобы получить неправомерный доступ к информации, составляющую персональную или банковскую тайну гражданина, и ее использования для своих дальнейших преступный действий (напр. неправомерное

осуществление онлайн-транзакций с расчетного счета потерпевшего гражданина). Такие деяние квалифицируются на практике по совокупности различных составов преступлений, но каждый из составов должен быть доказан в полном объеме. Однако на практике правоприменители часто испытывают трудности с корректным отграничением составов.

Проблемой при расследовании рассматриваемых преступлений является сложность в раскрытии личностей мошенников. В настоящий момент преступники используют различную новейшую технику, которая просто делает невозможным вычислить лиц, совершающий преступные деяния в рассматриваемой сфере, так как в настоящий момент много технологий, которые позволяют злоумышленникам менять свои точки нахождения ежеминутно или ежесекундно. Даже применение ОРМ мероприятий сотрудниками уголовного розыска не дают быстрых результатов в установлении личности мошенников. В законодательстве также установлено, что ОРМ не являются мерами ограничения прав и свобод граждан, т.е. все способы проведения ОРМ не должны противоречить Конституции Российской Федерации и иному законодательству в сфере обеспечения прав и свобод граждан.

Важным является то, что мошенничества в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, обладают, как было указано выше, высокой степенью латентности. Многие граждане не сразу понимают, что в отношении них было совершено преступление и не сразу обращаются в правоохранительные органы, тем самым давая преступникам время для того, чтобы «замести» свои следы.

Банк или иная организация создают самостоятельно условия для совершения мошенниками преступлений при раскрытии мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну. К числу таких условий, можно отнести:

1. Пробелы и просчеты банков в сфере создания системы предупреждения и выявления хищений мерами финансового, организационного, сыскного и криминалистического характера:

- недостатки в организации и планировании различных мероприятий финансового контроля, которые не способны быстро и в разумные сроки выявить факты хищения денежных средств. Как пример можно привести случай, когда бухгалтер Банка регулярно похищала денежные средства со счетов клиентов (потерпевших). Общая сумма похищенного составила 12,5 млн руб. Однако недостача была выявлена лишь спустя девять лет осуществления преступной деятельности.

- недоработанная до практического функционирования система конфиденциального делопроизводства. Банковские системы имеют свои программные обеспечения, в которых хранят все сведения свих клиентов, однако защита конфиденциальной информации во многих Банках защищается плохо, и мошенники могут незаконно получать и использовать сведения, составляющие банковскую тайну и персональные данные, для подготовки и совершения преступлений;

- неспособность сотрудников банка распознать признаки материальной подделки паспортов и иных документов (например, мошенники используют поддельные платежные поручения, которые содержали поддельные подписи сотрудников Пенсионного фонда и печати, а также не используемые ПФР коды бюджетной классификации).

2. Ошибки банков при осуществлении своей деятельности, которые способствуют хищениям денежных средств в сфере обслуживания счетов юридических лиц при использовании «бумажных» технологий:

- осуществление деятельности сотрудниками банков с нарушениями порядка приема банковских карточек, установленного типовым договором банковского счета. В соответствии с типовым договором банковского счета, банк должен получить специальное извещение о тех обстоятельствах, которые послужили основанием для замены карточки, но банк

проигнорировал данное условие с тем, что «так складывается практика делового оборота»;

- незнание сотрудниками банка о процедуре взыскания денежных средств клиента Банка в соответствии с Федеральным законом от 02.10.2007 № 229-ФЗ «Об исполнительном производстве»[1]. Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве» в ст. 70 регламентировано, что при получении банком или иной кредитной организацией исполнительного документа от судебного пристава-исполнителя на исполнение содержащихся в исполнительном документе требований о взыскании денежных средств с расчетного счета клиента данного банка осуществляется путем их перечисления на депозитный счет подразделения судебных приставов.

3. Ошибки банков при осуществлении своей деятельности, которые способствуют хищениям денежных средств в сфере обслуживания счетов юридических лиц с использованием систем удаленного управления счетом:

- существенные нарушения при организации системы защиты информации, составляющей банковскую или персональную тайну клиента, в том числе код настройки компьютерной системы банкомата, позволяющая преступникам самостоятельно завышать обменный курс одной из валют;

- несовершенства системы физической защиты компьютера банка или иной кредитной организации от неправомерного доступа;

- отсутствие автоматизированных средств контроля за деятельностью системного администратора банка;

- несовершенства организации системы информационной защиты процессингового центра от несанкционированного доступа к операциям по счету.

4. Ошибки использования клиентами своих личных кабинетов в банковской сфере:

---

[1] Об исполнительном производстве: Федеральный закон от 02.10.2007 № 229-ФЗ — Российская газета. — 06.10.2007. — ст. 70

- существенные недостатки защиты ключевой и парольной информации, взломав которые мошенники могут совершать операции от имени клиента (потерпевшего). В данном случае в преступную организацию могут входить сотрудники банка.

5. Недостаточная защищенность системы обслуживания карточных счетов от преступных посягательств со стороны персонала банка и иных кредитных организаций:

- недостатки мер организационного и технологического характера, призванных предотвращать несанкционированный выпуск карт;

- нарушения порядка хранения и уничтожения невостребованных и бракованных карт;

- отсутствие или несоблюдение банковским персоналом требований по разграничению уровня, предоставляемого руководством банка сотрудникам доступа к конфиденциальной информации;

- нарушения или несоблюдения в полной мере законодательства в сфере защиты персональных данных граждан, сбора и обработки информации из банкоматов и процессингового центра.

Количество рассматриваемых преступлений может быть снижено, если Банки начнут постепенно устранять вышеуказанные недочеты и нарушения со своей стороны, а также при правильной организации системы защиты банковских счетов граждан раскрытие и расследование преступлений, связанных с использованием сети Интернет, совершаемых с использованием банковской и персональной тайны граждан, будет осуществляться более успешно, по мнению автора.

Еще одной проблемой раскрытия и расследования преступлений, связанных с использованием сети Интернет, совершаемых с использованием банковской и персональной тайны, является то, процесс документирования и раскрытия преступлений в информационной среде или с ее использованием, основанный на существующем механизме документооборота между правоохранительными органами, операторами связи и поставщиками

интернет-услуг, значительно растянут по времени. И даже полнота, качество и оперативность предоставляемой информации не всегда отвечают требованиям законодательства Российской Федерации.

Появляется проблема установления подлинной личности преступников, так как зачастую деньги, похищенные у потерпевших, зарегистрированы в других субъектах Российской Федерации. Ввиду срок получения от операторов связи, находящихся в других регионах, составляет от 1 до 3 месяцев.

Помимо этого, возникают трудности в проведении технических мероприятий, в том числе установлении фактического местонахождения злоумышленников ввиду использования ими VPN- и хостинг-серверов для сокрытия своего настоящего IP-адреса.

Помимо того, что банки и иные кредитные организации пренебрежительно относятся к хранению конфиденциальной информации граждан, то операторы сотовой связи, IP-телефонии, интернет-провайдерами халатно относятся к правилам хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи. Все указанные материалы обязаны храниться в течение 6 месяцев с даты окончания их приема, передачи, доставки и (или) обработки.

Таким образом, из всего вышесказанного можно сделать вывод о том, что в настоящий момент существует множество проблем в сфере раскрытия мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну. Банки и иные кредитные организации сами же и создают условия для совершения мошенниками своих преступлений и для того, чтобы осуществить противодействие данному виду преступности необходимо, чтобы система МВД России действовала совместно и сообща с другими организациями (Банками и иными кредитными организациями).

§2. Совершенствование деятельности оперативных подразделений уголовного розыска в раскрытии мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну

По современным данным, предоставленным Генеральной прокуратурой Российской Федерации, преступления, которые совершены с использованием сети Интернет и конфиденциальной информации, составляют уже каждое четвертое зарегистрированное преступное деяние.

Согласно Федеральному закону от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» органы предварительного следствия в отличие от органов, осуществляющих ОРД, вправе запрашивать информацию, составляющую банковскую и персональную тайну, без определенных дополнительных процедур (напр., отсутствует необходимость обращения в суд для получения разрешения на данную процедуру)[1].

По мнению автора, ввиду устоявшихся проблем раскрытия и расследования мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, в настоящее время необходимо актуализировать и дополнить законодательство Российской Федерации, которое регламентирует порядок предоставления доступа к указанной выше информации, и также посредством дополнения законодательства снять ограничения на получение информации, которая составляет банковскую или персональную тайну, у органов, осуществляющих ОРД, т.е. модифицировать перечень органов, которые вправе запрашивать такие сведения.

---

[1] Демин Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств // Российский следователь. — 2021. — № 1. — стр. 64

В Федеральном законе от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» указывается, что информацию, составляющую банковскую тайну, вправе предоставлять оперативно-розыскным органам в случае выполнения выявления, предупреждения и пресечения преступлений[1]. Автора считает, что данную формулировку необходимо дополнить функциями «раскрытия и расследования преступлений», так как это указано в Федеральном законе «Об ОРД»[2] и изложить в следующей редакции:

- ст. 26 «….Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-разыскную деятельность, при выполнении ими функций по выявлению, предупреждению, пресечению раскрытию и расследованию преступлений по их запросам, направляемым в суд в порядке, предусмотренном статьей 9 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности»….».

В своей работе Романовский Г.Б. указывает, что законодатель придерживается мнения о том, что действия следователя при расследовании рассматриваемого вида преступлений носит самостоятельный характер и именно из-за этого следователь вправе получать конфиденциальную информацию без определенного ограничения[3]. Автор не согласен с данной точкой зрения, так как деятельность органов, осуществляющих ОРД, может вестись абсолютно самостоятельно, например в случае, если лицо, которое совершило преступление, еще не обнаружено, без зависимости от процессуальной деятельности следственных органов.

---

[1] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 05.02.1996. — ст. 26

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995. — ст. 2

[3] Романовский Г.Б. Банковская тайна и оперативно-розыскная деятельность правоохранительных органов // Наука. Общество. Государство. — 2016. — Т.4. № 1 (13). — стр. 58.

При расследовании мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, сотрудники МВД России используют не только различные ОРМ, рассмотренные выше, но и процессуальные действия, например «получение информации о соединениях между абонентами и (или) абонентскими устройствами», «контроль и запись телефонных и иных переговоров»[1]. Много времени затрачивается на то, чтобы получить разрешение суда на проведение данных мероприятий. Такая бумажная «волокита», по мнению автора, приводит к тому, что замедляется документирование преступных действий мошенников, а также установление их личности, задержании и т.д. Ввиду этого, автор предлагает внести изменения в действующее законодательство Российской Федерации и разрешить по веским и обоснованным причинам на основании разрешения руководителя следственного или оперативного подразделения, проводить различные ОРМ для достижения целей, согласно ст. 2 Федерального закона «Об оперативно-розыскной деятельности».

Данная правка позволит оперативно реагировать органам, осуществляющим ОРД, на полученную информацию о готовящемся, совершающемся или совершившемся мошенничестве в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

Распространение преступлений в сети Интернет в настоящее время носит волновой характер, и ежегодно накрывает статистику преступлений как «Цунами». Для эффективной системы раскрытия мошенничеств в сети интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, необходимо регламентировать для органов, осуществляющих ОРД, едины алгоритм действий, который основывается на уже новом актуализированном законодательстве.

---

[1] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 177-ФЗ— Российская газета. — 22.12.2001. — ст.ст. 186-186.1

В своем выступлении на расширенном заседании коллегии МВД России Министр внутренних дел Российской Федерации Владимир Колокольцев акцентировал внимание на значительных масштабах распространения киберпреступлений, разнообразии схем и методов их совершения, отсутствии единых алгоритмов выявления и раскрытия указанных преступлений и пояснил, что мерами исключительно организационного и оперативно-разыскного характера добиться кардинального улучшения ситуации невозможно[1].

В связи с этим дальнейшее совершенствование правового регулирования в сфере противодействия хищениям денежных средств граждан, совершаемых с использованием информационно-телекоммуникационных технологий, в оперативно-разыскной деятельности невозможно без развития тех отраслей знания, которые на основе достижений науки и практики позволяют разрабатывать научно обоснованные рекомендации по оптимальному разрешению проблем, стоящих перед оперативными подразделениями органов внутренних дел.

В настоящее время хищение денежных средств, совершенное дистанционным способом, является одним из распространенных, приносящих значительный материальный ущерб, трудно раскрываемых и еще более трудно доказуемых преступлений. Оно отличается многообразием способов совершения. Мошенники используют не только старые, но по-прежнему «рабочие», проверенные способы и приемы обмана, они создают и постоянно совершенствуют новые, все более изощренные схемы противоправного обогащения с использованием -технологий. Постоянное совершенствование способов мошеннических действий приводит к тому, что

---

[1] Контемирова Ю.В., Тарасова М.Ю. Современное состояние деятельности оперативных подразделений по противодействию хищениям денежных средств граждан, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Волгоградской академии МВД России. 2021. №1 (56). URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-deyatelnosti-operativnyh-podrazdeleniy-po-protivodeystviyu-hischeniyam-denezhnyh-sredstv-grazhdan (дата обращения: 01.04.2022).

правоохранительные органы не всегда оперативно и своевременно успевают реагировать на изменения криминогенной обстановки.

Проведенное исследование дает понять, что преступления, совершаемые в сети Интернет, совершаются посредством Р-телефонии («МТТ», «Ростелеком», «Квантум» и др.) с абонентских номеров, зарегистрированных в других регионах страны. Потерпевшими становятся граждане разного возраста и социального статуса, проживающие в различных городах и районах Волгоградской области.

Выявление, расследование, раскрытие и профилактика преступлений, совершенных с использованием - технологий, является одним из приоритетных направлений в деятельности органов внутренних дел.

Низкий уровень раскрываемости преступлений указанной категории наблюдается практически во всех территориальных органах МВД России, а многие территориальные органы внутренних дел некоторых сельских районов вообще не имеют результатов в раскрытии мошенничеств общеуголовной направленности, совершенных с использованием - технологий.

Причинами таких проблем могут выступать плохой анализ поступающих обращений, отсутствие проведения оперативно-разыскных мероприятий и следственных действий и прочее, а также:

- неполнота сбора материалов в дежурные сутки;
- несвоевременность возбуждения уголовных дел указанной категории;
- некачественное оперативное сопровождение уголовных дел;
- отсутствие контроля со стороны руководящего состава за указанным направлением деятельности;
- недостаточная профилактика;
- неиспользование базы данных «Дистанционное мошенничество»;
- отсутствие дел оперативного учета по указанной линии работы.

Вместе с тем практическая работа по раскрытию преступлений в сфере -технологий сталкивается со следующими проблемами:

1. Действующий правовой механизм получения сведений из кредитных организаций, относимых к категориям «Банковская тайна» и «Персональные данные», требует большого количества времени, что не позволяет сотрудникам органов внутренних дел оперативно получать сведения о пользователях банковских карт, об -адресах удаленного администрирования операций по расчетным счетам банковских карт.

2. Отсутствует система электронного документооборота с банками, операторами сотовой связи, интернет-провайдерами и владельцами сайтов объявлений, позволяющих оперативно получать информацию, за исключением Сбербанка России. Решение вопроса о заключении соглашений на региональном уровне с указанными организациями не представляется возможным ввиду отсутствия таких полномочий у региональных филиалов.

3. Отсутствие эффективных механизмов блокировки банковских счетов и телефонных номеров, используемых при совершении преступлений.

4. Проблема получения информации о банковских реквизитах, используемых при перечислении денежных средств со счетов абонентских номеров и некоторых кредитно-финансовых учреждений, которые предоставляют неполную информацию о номере карты (отсутствует полный номер: 4276**********), ссылаясь на защиту системы VISA и MasterCard, что не позволяет установить лиц, возможно причастных к совершению преступлений указанной категории.

5. Кроме того, существует проблема в подписании судебных постановлений, ограничивающих конституционные права граждан, в том числе на банковскую тайну в сельских ТОВД.

Основная задача оперативных подразделений состоит в разработке и принятии закона, который бы четко регулировал информационно-телекоммуникационную сферу: мобильную связь, IP-телефонию, интернет (при этом исключил возможности использования анонимных номеров,

приложений по подмене абонентских номеров, IP-адресов, VPN-сервисов), - а также банковскую сферу, что гарантировало бы гражданам безопасность проводимых операций.

Вместе с тем приведенная статистика доказывает необходимость повышения эффективности принимаемых мер со стороны государства и органов власти в век высоких технологий.

В процессе анализа типичных форм совершения мошенничества и правоприменительной практики выявлены пробелы в действующем законодательстве.

Так, на основании п. 5 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 мошенничество признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность в зависимости от потребительских свойств этого имущества пользоваться или распорядиться им по своему усмотрению[1].

Если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 Гражданского кодекса Российской Федерации содеянное должно рассматриваться как хищение чужого имущества. Такое преступление, в результате которого владельцу этих денежных средств причинен ущерб, следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств.

---

[1] Контемирова Ю.В., Тарасова М.Ю. Современное состояние деятельности оперативных подразделений по противодействию хищениям денежных средств граждан, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Волгоградской академии МВД России. 2021. №1 (56). URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-deyatelnosti-operativnyh-podrazdeleniy-po-protivodeystviyu-hischeniyam-denezhnyh-sredstv-grazhdan (дата обращения: 06.05.2022).

Согласно ч. 2 ст. 152 УПК РФ если преступление было начато в одном месте, а окончено в другом, то уголовное дело расследуется по месту окончания преступления.

Однако в соответствии с приказом МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» принятие решения о возбуждении уголовного дела по указанным фактам осуществляется в органе, в который поступило первоначальное сообщение о преступлении; кроме того, этот орган обязан обеспечить организацию надлежащего расследования данных преступлений, доказывание обстоятельств, предусмотренных ст. 73 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), направление необходимых поручений о производстве процессуальных действий по месту нахождения других участников уголовного судопроизводства. Направление уголовного дела в порядке, предусмотренном ст. 152 УПК РФ, осуществляется только после получения достаточных доказательств о совершении преступления на территории обслуживания другого территориального органа МВД России и выполнения всех возможных процессуальных действий по месту возбуждения уголовного дела.

Имеющиеся разногласия между постановлением Пленума Верховного Суда Российской Федерации № 48 и приказом МВД России № 196 позволяют руководителям органов внутренних дел отдельных регионов согласовать решение по передаче материала по подследственности (территориальности) со своим надзирающим прокурором и направлять в территориальный орган другого субъекта Российской Федерации, где в итоге возбуждается уголовное дело, либо, если нарушены требования приказа МВД России № 196, материал проверки направляется обратно.

Кроме того, расследование уголовного дела требует достаточного объема проведения следственных действий, при необходимости получение

судебных решений, направление поручений в орган дознания о проведении оперативно-разыскных мероприятий.

Кроме того, согласно ч. 2 ст. 7 ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ (далее — ФЗ «Об ОРД») одним из оснований для проведения оперативно-разыскных мероприятий являются ставшие известными органам, осуществляющим ОРД, сведения о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела.

В связи с этим очевидно, что при наличии информации о фактах совершения дистанционных преступлений, связанных с мошенничеством и кражами с банковских карт, оперативные подразделения заводят дела оперативного учета и проводят комплекс оперативно-разыскных мероприятий, направленных на установление фигуранта.

В рамках дела оперативного учета систематизируется информация о держателе банковской карты или расчетного счета, привязке абонентских номеров, информация о регионе Российской Федерации, где «работает» карта, с использованием которой совершено преступление. Кроме того, истребуются видеозаписи с банкоматов и филиалов банков. Однако получить информацию «по банковским операциям» злоумышленника подразделения, уполномоченные на осуществление оперативно-разыскной деятельности, исходя из нормы ст. 26 Федерального закона «О банках и банковской деятельности», без возбуждения уголовного дела органом предварительного расследования не могут.

Для исключения пробела в законодательстве, на наш взгляд, необходимо дополнить ст. 26 Федерального закона «О банках и банковской деятельности» в части «...а также при вынесении постановления о предоставлении информации, утвержденного руководителем органа, уполномоченным на осуществление оперативно-розыскной деятельности».

Указанный вариант повысит эффективность взаимодействия оперативных подразделений и сотрудников службы безопасности банков по противодействию мошенничествам и кражам с банковских карт, совершаемых дистанционным способом.

Помимо всех вышеуказанных действий, необходимо проводить профилактические работы и мероприятия с гражданами, которые особо подвержены на уловки мошенников (старики, инвалиды и т.д.). Например, периодически транслировать в средствах массовой информации (далее – СМИ) самые популярные в настоящий момент виды мошенничества, совершаемого путем использования сети Интернет, улучшить отклик от работников Банков и иных кредитных организаций, в случае сообщения гражданами о совершенных в отношении их преступных действий, проводить проверки на соблюдения законодательства в рассматриваемых организациях в сфере защиты персональных данных граждан.

На сегодняшний день создаются различные подразделения по борьбе с преступлениями, ИБД-Ф «Дистанционное мошенничество» и прочее. Однако борьба должна проходить при взаимодействии правоохранительных органов, различных иных учреждений (Банков, иных организаций, операторов сотовой связи и т.д.), и граждан, которые стали потерпевшими в совершении рассматриваемых преступлений. Много проблем при раскрытии данного вида преступности было выявлено. Именно поэтому автор предлагает решить данные проблемы комплексным подходом ко всему, начиная с внесения изменений в законодательство Российской Федерации, заканчивая проведением практических профилактических мероприятий с гражданами. Также автор считает, что необходимо регламентировать порядок взаимодействия различных учреждений, которые занимаются собиранием и хранением информации, составляющую банковскую и персональную тайну, путем создания и введения в действие «Инструкции по взаимодействию учреждений, чья деятельность связана с банковской или персональной тайной граждан Российской Федерации, с правоохранительными органами»,

где будет четко регламентирован порядок проведения взаимодействия и предоставления указанной информации с мерами предупреждения таких преступлений.

ЗАКЛЮЧЕНИЕ

На сегодняшний день, одним из самых быстро распространяемых и быстрорастущих преступлений, является мошенничество в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну. О чем свидетельствует статистика зарегистрированных преступлений, где в 2017 году было зарегистрировано 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. За 2018 год было зарегистрировано 174674 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, за 2019 год было зарегистрировано 294409 аналогичных преступлений, за 2020 год в ГИАЦ МВД России было зарегистрировано 510396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, а в 2021 году – 517722 преступлений[1].

Автор выделил следующие особенности преступлений, совершаемых в сфере предоставления услуг Интернет:

1. Преступления совершаются посредством использования программного обеспечения, компьютерных устройств и иной современной техники, а также совершения действий, которые сложно контролировать государственным и иным органам. Информация, которая является объектом посягательства представлена в математическом, символьном и другом виде и содержит сведения о различных лицах, фактах, событиях, явлениях и процессах и др.

2. Способы совершения преступления уникальны.

---

[1] Состояние преступности МВД России [Электронный ресурс]: база данных содержит сведения о всех видах преступлений. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/5/ — дата обращения: 22.01.2022.

3. Трансграничный характер преступных деяний. Преступники при совершении своих преступлений могут находится в любой точке мира, где есть доступ к сети «Интернет».

4. Высокий уровень латентности рассматриваемых преступлений. По проведенным исследованиям, специалисты указывают на примерные данные уровня латентности, которые составляют 90%. Важную роль играет то, что потерпевшие не всегда обращаются в правоохранительные органы за помощью в подобных случаях, а некоторые даже не знают, что в отношении их совершили преступное посягательство.

5. Данная категория преступлений обладает высокой степенью профессионализма и скрытности. Лица, совершающие преступления в сети «Интернет» обладают специальными знаниями, навыками и умениями в области информационно-телекоммуникационных технологий, программирования и защиты информации. При исследовании практических материалов по преступлениям, совершаемых в сфере предоставления услуг Интернет, можно говорить о том, лица, которые совершали подобные преступления, имели высшее или/и среднее специальное образование (зачастую профильное, связанное с обработкой и защитой конфиденциальной информации). Практически в 80% случаев преступниками являлись сотрудники учреждений, предприятий и/или организаций, которые непосредственно работали с конфиденциальной информацией или использовали специальные интернет-технологии в профессиональной деятельности.

Таким образом, исследуемая категория преступлений является сложной для выявления и расследования оперативными подразделениями МВД России. Однако, количество зарегистрированных преступлений ежегодно растет, так как современные технологии вторгаются во все сферы жизни человека, создаются даже метавселенные, где человек может жить реальной виртуальной жизнью, делать реальные виртуальные покупки, а также совершать настоящие преступления против личности в виртуальной

реальности. У государства и государственных органов должна стоять задача разработать и актуализировать механизмы выявления и расследования преступлений, совершаемых в сфере предоставления услуг Интернет.

В настоящий момент современное законодательство Российской Федерации предусматривает три вида ответственности за разглашение банковской тайны: гражданская, административная и уголовная.

Автор под персональной тайной понимает сведения, относящиеся к тайне личной жизни гражданина, на которые направлены по желанию гражданина все установленные законодательством Российской Федерации средства и способы защиты данной информации, разглашение, распространение и использование третьими лицами которой могло бы повлечь для гражданина неприятные последствия.

При расследовании вышеуказанных преступлений особую роль играют ОРМ и ДОУ. Использование при проведении ОРМ современных информационных технологий позволит устранить факторы мобильности и скрытности использования современных средств получения, копирования, обработки компьютерной информации в целях борьбы с компьютерной преступностью.

Автор рассмотрел различные проблемы раскрытия мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, такие как смежность различных составов и сложность доказывания этих составов при совокупности преступлений, наличие проблем создание условий для совершения мошенниками преступлений внутри банковской и иной кредитной организации, проблемы в проведении ОРМ и затяжной срок получения информации о совершении противоправных действий от учреждений, которые могут иметь информацию об осуществлении рассматриваемого вида преступности.

Автор предлагает внести изменения и изложить в следующей редакции ст. 26 Федерального закона «Об оперативно-розыскной деятельности»:

- ст. 26 «….Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-разыскную деятельность, при выполнении ими функций по выявлению, предупреждению, пресечению раскрытию и расследованию преступлений по их запросам, направляемым в суд в порядке, предусмотренном статьей 9 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности»….».

Автором было предложено внести изменения в действующее законодательство Российской Федерации и разрешить по веским и обоснованным причинам на основании разрешения руководителя следственного или оперативного подразделения, проводить различные ОРМ для достижения целей, согласно ст. 2 Федерального закона «Об оперативно-розыскной деятельности». Такая правка сможет позволить оперативно реагировать органам, осуществляющим ОРД, на полученную информацию о готовящемся, совершающемся или совершившемся мошенничестве в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну.

Также для эффективной системы раскрытия мошенничеств в сети интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну, необходимо регламентировать для органов, осуществляющих ОРД, едины алгоритм действий, который основывается на уже новом актуализированном законодательстве.

Помимо всех вышеуказанных действий, необходимо проводить профилактические работы и мероприятия с гражданами, которые особо подвержены на уловки мошенников (старики, инвалиды и т.д.). Например, периодически транслировать в средствах массовой информации (далее – СМИ) самые популярные в настоящий момент виды мошенничества, совершаемого путем использования сети Интернет, улучшить отклик от

работников Банков и иных кредитных организаций, в случае сообщения гражданами о совершенных в отношении их преступных действий, проводить проверки на соблюдения законодательства в рассматриваемых организациях в сфере защиты персональных данных граждан.

Автор придерживается мнения о том, что в настоящий момент в законодательстве отсутствует нормативно-правовой акт, который бы регламентировал порядок взаимодействия различных учреждений, занимающихся собиранием и хранением информации, составляющую банковскую и персональную тайну, путем создания и введения в действие «Инструкции по взаимодействию учреждений, чья деятельность связана с банковской или персональной тайной граждан Российской Федерации, с правоохранительными органами», где будет четко регламентирован порядок проведения взаимодействия и предоставления указанной информации с мерами предупреждения таких преступлений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 — Официальный интернет-портал правовой информации http://www.pravo.gov.ru.

2. Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ. — Собрание законодательства РФ. — 05.12.1994.

3. Гражданский кодекс Российской Федерации (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ. — Собрание законодательства РФ. — 29.01.1996.

4. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 05.02.1996.

5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07.12.2011 № 420-ФЗ — Российская газета. — 09.12.2011.

6. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 № 207-ФЗ — Российская газета. — 03.12.2012.

7. Об исполнительном производстве: Федеральный закон от 02.10.2007 № 229-ФЗ — Российская газета. — 06.10.2007.

8. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ— Российская газета. — 18.08.1995.

9. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ— Российская газета. — 23.11.2011.

10. О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ. — Российская газета. — 29.07.2006

11. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ— Российская газета. — 10.02.2011.

12. О почтовой связи: Федеральный закон от 17.07.1999 № 176-ФЗ — Российская газета. — 22.07.1999.

13. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ — Российская газета. — 10.07.2003.

14. Об адвокатской деятельности и адвокатуре в Российской Федерации: Федеральный закон от 31.05.2002 № 63-ФЗ — Российская газета. — 05.06.2002.

15. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 02.12.1990 № 395-1. — Собрание законодательства РФ. — 07.01.2002.

16. Семейный кодекс Российской Федерации: Федеральный закон от 29.12.1995 № 223-ФЗ — Российская газета. — 27.01.1996.

17. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ. — Собрание законодательства РФ. — 24.12.200.

18. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. — Собрание законодательства РФ. — 17.06.1996.

19. Доктрина информационной безопасности Российской Федерации: Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 — Российская газета. — 2016. – 6 декабря.

20. О государственной программе Российской Федерации «Информационное общество 2011–2020»: Утверждена Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р — Российская газета. – 2010. – 6 ноября.

21. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собрание законодательства 2017. — № 20. —Ст. 2901.

22. По делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации: Постановление Конституционного суда Российской Федерации от 09.07.2013 №18-П/2013 — Российская газета. — 19.07.2013.

23. Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации: Определение Конституционного Суда РФ от 09.06.2005 № 248-О.

24. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 —Российская газета. — 14.03.1997

Монографии, учебники, учебные пособия, статьи, научные публикации

25. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации: новая редакция (постатейный). — 3-е изд., перераб. и доп. М.: Проспект, 2020. — с. 256

26. Бегишев, И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, — 2020. — стр. 300

27. Беришвили Р.Ш. Компьютерные преступления // Символ науки. — 2021. — №12-1. — стр. 52-54.

28. Демин Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств // Российский следователь. — 2021. — № 1. — стр. 64 - 68.

29. Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет // дисс.. канд. юр. наук // Волгоград. — 2008. — стр. 228

30. Кочкина Э. Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. — 2017. — №3 (17).

31. Коротких Н. Н., Останин М. Д. К вопросу о соотношении понятий «преступление в сфере компьютерной информации» и «компьютерное преступление» // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2018. — №3. — стр. 69 – 77

32. Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. — 2020. — №1. — 52 - 62

33. Перетолчин А.П. Применение защитником нормы, устанавливающей ответственность за мошенничество с использованием электронных средств платежа // Адвокатская практика. — 2019. — № 6. — стр. 13 - 18.

34. Романовский Г.Б. Банковская тайна и оперативно-розыскная деятельность правоохранительных органов // Наука. Общество. Государство. — 2016. — Т.4. № 1 (13). — стр. 56 - 66

Практические материалы

35. О судебной практике по делам о мошенничестве, присвоении и растрате [Текст]: Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 — Российская газета. — № 280 — 11.12.2017.

Электронные ресурсы

36. Виды мошенничества в интернете [Электронный ресурс]: Управление МВД России по Костромской области. — Режим доступа: https://44.xn--b1aew.xn--

p1ai/Dlja_grazhdan/%D0%BE%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D0%BE-%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%B8-/%D0%B2%D0%B8%D0%B4%D1%8B-%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0-%D0%B2-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5 — дата обращения: 25.01.2022.

37. Состояние преступности МВД России [Электронный ресурс]: база данных содержит сведения о всех видах преступлений. — Режим доступа: https://xn--b1aew.xn--p1ai/reports/5/ — дата обращения: 22.01.2022.

38. Сперанская Л.В. Право на неприкосновенность частной жизни // СПС КонсультантПлюс. — 12.01.2022

39. Право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23, 24 Конституции России) [Электронный ресурс]: Прокурор разъясняет, 2021 год —Режим доступа: https://epp.genproc.gov.ru/ru/web/proc_26/activity/legal-education/explain?item=61977689 — дата обращения 24.01.2022.

40. Число интернет-преступлений в России [Электронный ресурс]: Коммерсарнт, 2021. — Режим доступа: https://www.kommersant.ru/doc/4654110. – дата обращения 23.01.2022.

РЕЦЕНЗИЯ
на выпускную квалификационную работу
обучающегося 072 учебной группы очной формы обучения 2017 года набора
по специальности «Правоохранительная деятельность»
Нургалиева Марселя Маратовича

На тему: Организация и тактика выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети «Интернет», совершенных с использованием сведений, составляющих банковскую или персональную тайну

Тема выпускной квалификационной работы, представленной слушателем 072 учебной группы ФПС по ПВО КЮИ МВД России младшим лейтенантом полиции Нургалиевым Марселем Маратовичем, представляется весьма актуальной и практически значимой. Автором верно отмечается, что проблема организация работы по проведению процессуальных проверок по сообщениям о преступлениях в сфере современных информационно-коммуникационных не отвечает требованиям организация работы по проведению процессуальных проверок. Отсутствие качественной работы МВД России и судебной системы, принятие необходимых мер к возмещению ущерба, причиненного данными преступлениями.

Тема работы «Организация и тактика выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети «Интернет», совершенных с использованием сведений, составляющих банковскую или персональную тайну.

Структура выпускной квалификационной работы подчинена внутренней логике, направлена на решение задач исследования и состоит из введения, двух глав, четырех параграфов, входящих в них, заключения, списка использованных источников.

В проекте введения автор обосновал актуальность, новизну исследования, определил цели, задачи, объект и предмет исследования.

В первой главе «Особенности организации раскрытия преступлений, совершаемых в сфере предоставления услуг Интернет» исследуется понятие и

сущность киберпреступлений, также анализируются причины возникновения и условия функционирования киберпреступлений в современном мире.

Во второй главе «Совершенствование организации и тактики выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющий банковскую или персональную тайну» автором раскрываются проблемы установления подлинной личности преступников, так как зачастую деньги, похищенные у потерпевших, зарегистрированы в других субъектах Российской Федерации. В ВКР проводится анализ практики назначения наказания за совершение вышеуказанного преступления.

Научный стиль изложения, используемый категориальный аппарат, позволяют говорить о хорошем владении автором исследуемой проблематикой.

Приведенные в работе рекомендации и выводы могут быть использованы в практической деятельности сотрудников органов внутренних дел. В работе все законодательные источники использованы с учетом их последних изменений, приведены выдержки из диссертационных исследований, научной литературы, каждый из которых соответствует рассматриваемой автором теме.

Выпускная квалификационная работа выполняется Нургалиевым М.М. в соответствии с планом-графиком, раскрывает заявленную автором тему исследования, по структуре, объему и содержанию разделов, глубине проработки материала соответствует предъявляемым требованиям к выпускной квалификационной работе и заслуживает положительной оценки по завершению исследования.

Рецензент
Начальник отделения по
раскрытию преступлений,
совершенных с использованием
информационно-телекоммуникационных
технологий, ОУР УМВД России по г. Казани
старший лейтенант полиции В.М. Алиев

04.05.2022

С рецензией ознакомлен 06.05.2022 М.М. Нургалиев

Отзыв

о работе обучающегося 072 учебной группы очной формы обучения, 2017 года набора, по специальности 40.05.02 Правоохранительная деятельность Нургалиева Марселя Маратовича в период подготовки выпускной квалификационной работы на тему «Организация и тактика выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети "Интернет", совершенных с использованием сведений, составляющих банковскую или персональную тайну»

Данная тема автором уточнена в процессе производственной, в том числе преддипломной практики. Нургалиев М.М. проявил заинтересованность к данной тематике, изучал данную проблему с различных позиций.

Автором обработано достаточное количество научного материала, на хорошем теоретическом и методологическом уровне проведено исследование особенностей тактики оперативно-розыскной деятельности ОВД по раскрытию преступлений, связанных с мошенничеством в сети Интернет. Материал в выпускной квалификационной работе изложен с соблюдением внутренней логики, между разделами прослеживается логическая взаимосвязь.

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

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

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

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

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

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

Слушатель Нургалиев М.М. показал уверенные навыки владения компьютерными методами сбора, хранения и обработки информации, применяемой в сфере профессиональной деятельности, умение и навыки работы с компьютерными программами (Word, PowerPoint, Excel), информационно-справочными ресурсами, работы в системе Интернет.

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

Результаты работы прошли Основные положения, выводы и предложения, которые были сформулированы в процессе написания выпускной квалификационной работы отражены при подготовке научной работы по одноименной теме, занявшей 2-е призовое место в конкурсе Казанского юридического института МВД России.

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

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

Научный руководитель:

кандидат юридических наук, доцент
доцент кафедры ОРД КЮИ МВД России

полковник полиции А. И. Музеев

"05" мая 2022 г.

С отзывом ознакомлен: М.М. Нургалиев

"07" 06 2022 г.

Подпись Музеева А.И.
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

Казанский юридический институт МВД России

о результатах проверки текстового документа
на наличие заимствований

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Нургалиев Марсель Маратович
Самоцитирование рассчитано для: Нургалиев Марсель Маратович
Название работы: Организация и тактика выявления и документирования оперативными подразделениями уголовного розыска мошенничеств в сети Интернет, совершенных с использованием сведений, составляющих банковскую или персональную тайну
Тип работы: Выпускная квалификационная работа
Подразделение:

РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

ЗАИМСТВОВАНИЯ		27.85%	**ЗАИМСТВОВАНИЯ**		27.85%
ОРИГИНАЛЬНОСТЬ		51.5%	**ОРИГИНАЛЬНОСТЬ**		51.5%
ЦИТИРОВАНИЯ		20.65%	**ЦИТИРОВАНИЯ**		20.65%
САМОЦИТИРОВАНИЯ		0%	**САМОЦИТИРОВАНИЯ**		0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 29.03.2022

ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 07.06.2022 14:31

Модули поиска: ИПС Адилет; Библиография; Сводная коллекция ЭБС; Интернет Плюс; Сводная коллекция РГБ; Цитирование; Переводные заимствования (RuEn); Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по Интернету (EnRu); Переводные заимствования издательства Wiley (RuEn); eLIBRARY.RU; СПС ГАРАНТ; Модуль поиска "КЮИ МВД РФ"; Медицина; Сводная коллекция вузов МВД; Диссертации НББ; Перефразирования по eLIBRARY.RU; Перефразирования по Интернету; Патенты СССР, РФ, СНГ; Коллекция СМИ; Шаблонные фразы; Кольцо вузов; Издательство Wiley

Подпись Музеева А.И.
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

Работу проверил: Музеев Айдар Иршатович
ФИО проверяющего

Дата подписи: 07.06.2022

Подпись проверяющего

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

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