МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КРАЖ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Назаров Ленар Наилевич
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2017 года набора, 714 учебного взвода

Руководитель
доцент кафедры криминалистики,
кандидат юридических наук
Низаева Светлана Рамилевна

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2022 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность данного исследования заключается в том, что на сегодняшний день человек не представляет свою повседневную деятельность и досуг без различных электронных устройств и приспособлений. Данная тенденция тесно связана с научно техническим прогрессом, который продолжается и по сей день, появлением цифровых систем различных наукоемких производств, изобретением средств связи, информационно-телекоммуникационных систем, электронно-вычислительных устройств различных видов. В жизни человека ежедневно присутствуют информационно-телекоммуникационных системы, отказаться от которых невозможно!

Все достижения науки и техники облегчают жизнедеятельность человека. Они проникли и в индустрию развлечений, в сферу предоставления государственных и банковских услуг. Появились удобные интернет-магазины, в которых можно приобретать практически любые необходимые товары[1].

Но наряду с положительными свойствами информатизации общества, имеются и отрицательные. Преступность также осваивает интернет пространство. Данная ситуация складывается в связи с тем, что совершать преступления в информационной среде, при условии соблюдения правил конспирации и сокрытия преступной деятельности, безопаснее[2].

Проблема латентности преступлений в сфере информационно-телекоммуникационных систем является наиболее острой и актуальной как для России, так и для всего. Именно от них терпят колоссальные имущественные потери и убытки физические лица, организации, государства и мировая экономика в целом.

Наибольшую часть преступлений в информационной среде составляют мошенничества, кражи, преступления, связанные с незаконным оборотом

---

[1] Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. С. 37 – 45.

[2] Першин А. Н. Документированная коммуникация как социальный след преступной деятельности // Психопедагогика в правоохранительных органах. 2015. № 4. С. 73 – 76.

наркотических средств. При их совершении вышеуказанных преступлений также нередко в совокупности совершаются преступления предусмотренные главой 28 Уголовного кодекса Российской Федерации от 13 июня 1996 года № 63-ФЗ (Далее – УК РФ)[1].

В данном исследовании детально будут изучены теоретические и практические основы раскрытия и расследования краж, совершаемых с использованием информационно-телекоммуникационных систем.

Объектом исследования выступают закономерности механизма совершения краж, совершенных с использованием информационно-телекоммуникационных систем, а также закономерности деятельности правоохранительных органов по раскрытию и расследованию преступлений указанной категории.

Предмет исследования составляют тактические особенности производства первоначальных следственных действий, организация взаимодействия следователя с оперативными работниками по раскрытию и расследованию краж, совершенных с использованием информационно-телекоммуникационных систем.

Целью данного исследования является изучение методики расследования краж, которые совершаются с использованием информационно-телекоммуникационных систем, проблем возникающих при раскрытии и расследовании данного вида преступления, рекомендаций по возможному решению данных проблем.

Задачи исследования заключаются в следующем:

– исследование истории возникновения краж, совершаемых с использованием информационно-телекоммуникационных систем и изменений в способах совершения данного вида преступлений;

– определение понятий и терминов информационно-телекоммуникационных систем, и их значение;

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // Собрание законодательства Российской Федерации. 1996 г. № 25. Ст. 2954.

– изучение основных актуальных способов совершения данного вида краж;

– исследование методики расследования краж, совершаемых с использованием информационно-телекоммуникационных систем, тактики производства первоначальных и последующих следственных действий при их расследовании;

– выявление теоретических и практических проблем, возникающих в ходе взаимодействия служб и подразделений органов внутренних дел при раскрытии и расследовании данного вида кражи;

– определение типичных ошибок, возникающих в деятельности правоохранительных органов при раскрытии и расследовании данного вида кражи;

– формирование рекомендаций для решения данных проблем.

Методологическую основу настоящей выпускной квалификационной работы составляют: диалектический, системно-структурный, сравнительно-правовой, частно-научный и логико-теоретический методы познания.

Правовой основой настоящей работы выступают Конституция Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, федеральный закон «Об информации, информационных технологиях и о защите информации», иные федеральные законы и нормативные правовые акты.

Теоретической основой являются фундаментальные положения различных отраслей знаний в сфере криминалистики, уголовного процесса, оперативно-розыскной деятельности.

Структура выпускной квалификационной работы состоит из введения, двух глав, включающих в себя пять параграфов, заключения и списка использованной литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАССЛЕДОВАНИЯ КРАЖ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

§ 1. История возникновения краж, совершенных с использованием информационно-телекоммуникационных систем и изменения способов совершения данных преступлений

Существенное значение для изучения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, имеет анализ истории их развития. Говоря о ретроспективе преступного использования компьютерных технологий и его законодательного ограничения, следует принимать во внимание, что динамика данных процессов существенно различалась в России и в странах, где компьютерные технологии стали частью общественной жизни значительно раньше[1].

В нашей стране еще в период существования СССР компьютерные технологии в основном использовались для работы в правоохранительной и банковской сферах, в целях обеспечения обороноспособности страны, в то время как в зарубежных странах компьютер практически сразу стал существенной частью жизни обычных граждан.

Таким образом, в мире проблема противодействия преступлениям, совершаемым с использованием компьютерных технологий, проявилась гораздо раньше и до конца 1990-х гг. стояла гораздо острее, чем в России[2].

Так, первенство в совершении киберпреступлений принадлежит США. В 1966 г. компьютер был впервые использован как инструмент для совершения кражи из Банка Миннесоты[3].

---

[1] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2019. № 1. С. 45-55.

[2] Першин А. Н. Документированная коммуникация как социальный след преступной деятельности // Психопедагогика в правоохранительных органах. 2015. № 4. С. 73 – 76.

[3] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2019. № 1. С. 45-55.

В истории развития криминального использования компьютерных технологий можно отметить следующие наиболее значимые события:

– в 1973 году сотрудник АО КБ «Ситибанк» с помощью служебного компьютера похитил 2 миллиона долларов;

– в 1987 году – первый случай заражения компьютерным вирусом в СССР;

– в 1989 году – вирус в сети Пентагона Соединенных Штатов Америки, блокировка 6 000 компьютеров;

– в 1990 году – группа хакеров на 24 часа саботировала работу сети NASA;

– в 1995 году – покушение на кражу 2,8 млн долларов из АО КБ «Ситибанк» и других известных банков[1].

Постепенно единичные случаи стали системными, противоправное использование компьютерных технологий распространилось повсеместно, а ущерб от таких деяний стал исчисляться миллионами долларов. Так, например, в 2003 г. средние потери американских компаний от кражи конфиденциальной информации составили 2 699 842 $, от компьютерного саботажа – 214 521 $, повреждения информации – 199 871 $. В соответствии с отчетом компании «Нортон» в 2011 г. убытки от совершения киберпреступлений составили 388 млрд долларов, а жертвами стали 341 млн человек. Как показывают данные проведенного Старичковым М. В. опроса, 13,33 % респондентов сталкивались за последний год с противоправной деятельностью с использованием компьютерных технологий один раз, а 33,33 % – неоднократно[2].

Анализируя историю совершения преступлений с использованием компьютерных технологий, можно выделить закономерности их развития. Так, если на заре становления киберпреступности основной целью злоумышленника

---

[1] Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. № 1. С. 16-20.

[2] Морар И. О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? // Российский следователь. 2018. № 13. С. 34-38.

являлось личное обогащение, а компьютер использовался как инструмент хищения. В 1990-е годы основной целью лица, совершающего преступление с использованием компьютерных технологий, стал «интеллектуальный вызов», т. е. стремление показать свое превосходство в знании компьютерных систем и обходе средств их защиты. В настоящее время преступления с использованием компьютерных технологий часто становятся инструментом незаконного политического давления.

Например, в начале 2009 г. финансовые учреждения Индии, в том числе Государственный банк, подверглись атаке хакеров из Пакистана. Весной 2013 г. банковская система Южной Кореи оказалась выведена из строя в результате кибератаки. Власти страны обвинили в этом государственных хакеров Китая и спецслужбы КНДР[1].

В мае 2013 г. компьютерным атакам со стороны «Сирийской электронной армии» подверглись интернет-представительства СМИ США и телекомпании BBC. Кроме того, хакеры разместили в прессе информацию о взрыве в Белом Доме. Это вызвало обвал фондовых бирж США.

Как видно, компьютерное вмешательство может использоваться для причинения ущерба экономическим интересам либо безопасности страны, а также в качестве способа дестабилизации обстановки в обществе и даже провокации неконституционных политических процессов[2].

Межгосударственная интеграция, новые средства коммуникации, развитие международной электронной торговли породили такое негативное явление, как криминальную глобализацию, выражающуюся в том числе в высокотехнологичном мошенничестве, интеллектуальном пиратстве и отмывании преступных доходов, которые осуществляются международными преступными структурами с применением компьютерных технологий.

---

[1] Криминалистика: тактика и методика: учебник для вузов / И. В. Александров. М.: Издательство Юрайт, 2022. С. 57 – 61.

[2] Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98 – 106.

Таким образом, кражи, совершаемые с использованием информационно-телекоммуникационных систем, наряду с терроризмом и коррупцией, со временем стали представлять существенную угрозу не только отдельному человеку или государству, но и цивилизации в целом.

В заключение данного параграфа необходимо отметить, что изучение истории возникновения краж, совершаемых с использованием информационно-телекоммуникационных систем позволяет выявить те предпосылки, которые повлекли возникновение данного вида преступления, что позволяет более эффективно бороться с данным видом преступления.

§ 2. Понятия, применяемые при расследовании краж, совершенных с использованием информационно-телекоммуникационных систем

Для успешного и эффективного раскрытия и расследования преступления следователю и сотрудникам оперативного подразделения необходимо обладать знаниями и представлением о том, что такое информационно-телекоммуникационная система и как она устроена.

Интернет (от англ. Internet – объединение сетей) – всемирная информационно-телекоммуникационная сеть, объединяющая миллионы компьютеров в единую информационную систему.

Информационно-телекоммуникационная система, либо информационно-телекоммуникационная сеть, как ее называют большое количество ученных в области права и технических наук – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[1].

В законодательстве понятие банковского счета не определено, но есть упоминание о нем в статье 845 Гражданского кодекса Российской Федерации (далее – ГК РФ). По договору банковского счета банк обязуется принимать и

[1] Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации 2006. № 31 (часть I) ст. 3448.

зачислять поступающие на счет, открытый клиенту (владельцу счета), денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций по счету[1].

В пункте 2.1 главы второй инструкции Банка России от 30.05.2014 № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов» прописано, что банки открывают в валюте Российской Федерации и иностранных валютах: текущие счета; расчетные счета; бюджетные счета; корреспондентские счета; корреспондентские субсчета; счета доверительного управления; специальные банковские счета; публичные депозитные счета нотариусов, службы судебных приставов, судов, иных органов или лиц, которые в соответствии с законодательством Российской Федерации могут принимать денежные средства в депозит (далее – иные органы или лица); счета по вкладам (депозитам)[2].

Исходя из вышесказанного можно сделать вывод, что банковский счет – это открытые банком по договору банковского счета, заключенного с физическим или юридическим лицом, в валюте Российской Федерации и иностранных валютах текущие счета, расчетные счета, бюджетные счета, корреспондентские счета, корреспондентские субсчета, счета доверительного управления, специальные банковские счета, публичные депозитные счета нотариусов, службы судебных приставов, судов, иных органов или лиц, которые в соответствии с законодательством Российской Федерации могут принимать денежные средства в депозит, счета по вкладам (депозитам).

Согласно пункту 1.5 главы первой положения Банка России от 24.12.2004 г. № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» кредитная организация вправе осуществлять эмиссию банковских карт следующих видов: расчетных

---

[1] Гражданский кодекс Российской Федерации. Часть вторая: федеральный закон Российской Федерации от 26 января 1996 г. № 14-ФЗ // Собрании законодательства Российской Федерации. 1996. № 5. Ст. 410.

[2] Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов: инструкция Банка России от 30 мая 2014 года № 153 –И // Вестник Банка России № 60. 2014.

(дебетовых) карт, кредитных карт и предоплаченных карт, держателями которых являются физические лица, в том числе уполномоченные юридическими лицами, индивидуальными предпринимателями[1].

Расчетной (дебетовой) картой в свою очередь является электронное средство платежа используемое для совершения операций ее держателем в пределах расходного лимита – суммы денежных средств клиента, находящихся на его банковском счете, и (или) кредита, предоставляемого кредитной организацией – эмитентом клиенту при недостаточности или отсутствии на банковском счете денежных средств (овердрафт)[2].

Информационные технологии (IT технологии) – это приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.

Специалисты в области информационных технологий (IT технологий) – это лица, имеющие профессиональные познания и навыки в использовании информационных технологий, либо те лица, что имеют профессиональное образование информационно-технической сфере[3].

IT преступления – преступления, совершаемые с использованием информационных технологий[4].

Также существует преступная схема, в которой лица, совершающие преступления в сфере IT технологий используют определенный контингент граждан, а точнее банковские карты данных граждан. Их именуют «дропами».

Дропы – лица, которые оформляют на свое имя банковские карты и передают данные карты за определенную плату участникам организованной преступной группы (преступного сообщества). Как правило, к дропам относят студентов, лиц маргинального слоя общества, которые не подозревают о

[1] Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Банка России от 24.12.2004 № 266-П // Вестник Банка России № 17. 2005.

[2] Зубакина Ю. К. Интернет-банкинг как современная форма банковского обслуживания / // Молодой ученый. 2019. № 22. С. 526-528.

[3] Гриб Г. В., Тюнис И. О. Криминалистика и цифровые технологии // Российский следователь. № 9, 2019. С. 99 – 105.

[4] Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. №1. С. 152 – 157.

преступных целях использования банковских карт, оформленных на их же имя, либо относятся к данному факту безразлично, в силу того, что легкий заработок на данный момент им нужнее[1].

Понятие банковский онлайн сервис тесно связано с понятием интернет-банкинга, также существует мнение об отождествлении данных терминов. По мнению Ю. К. Зубакиной интернет-банкинг – это комплекс средств для управления банковскими счетами через Интернет[2].

Данное определение не в достаточной степени раскрывает его сущность, так как не сказано о его свойствах как информационно-технического средства, о разработчике или владельце и о пользователях данного средства.

Таким образом, банковский онлайн сервис – это издаваемый и контролируемый банком комплекс информационно-технических средств для управления клиентами банка банковскими счетами, совершения иных расчетно-финансовых операций.

Интернет – провайдер (провайдер) – это организация, которая предоставляет услуги связи и доступ к сети «Интернет» физическим лицам (абонентам) связи и имеет соответствующую лицензию на осуществление данной деятельности.

Хостинг – предоставление вычислительной мощности в информационной системе, либо памяти электронно – вычислительной машины, иного электронного носителя информации, для размещения информации в информационной системе, постоянно подключенной к сети «Интернет». Как правило информация в сети «Интернет» размещается на интернет сайтах[3].

Сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-

---

[1] Егоров Н. Н. Криминалистика: учебник и практикум для вузов, 2-е изд., испр. и доп. / Н. Н. Егоров, Е. П. Ищенко. М.: Издательство Юрайт, 2020. С. 73.

[2] Зубакина Ю. К. Интернет-банкинг как современная форма банковского обслуживания // Молодой ученый. 2019. № 22. С. 79 – 84.

[3] Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46-50.

телекоммуникационной сети «Интернет» (далее – сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет». Также данный термин используется и под другим названием как Интернет-ресурс.

Ip – адрес – это уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP. Internet Protocol (IP) – маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть.

Ip телефония – это телефонная связь по протоколу Ip. Под Ip телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям[1].

MAC-адрес (от англ. Media Access Control – надзор за доступом к среде, также Hardware Address, также физический адрес) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Интернет.

IMEI (англ. International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – это номер, обычно уникальный, для идентификации телефонов GSM, WCDMA и IDEN, а также некоторых спутниковых телефонов.

Провайдер хостинга – это лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет». Указанные услуги не являются услугами связи. Доступ к информационно-телекоммуникационной

[1] Разъяснения Роскомнадзора по вопросу лицензирования деятельности провайдеров хостинга от 20 августа 2016 года // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/it/control/p852 (дата обращения: 09.01.2022).

сети «Интернет» предоставляется провайдеру хостинга оператором связи на основании договора оказания услуг связи.

Хеширование (хеш – память) – преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины[1].

Таким образом, все действия, которые совершаются при помощи устройств ввода на ЭВМ шифруются при помощи определенного алгоритма шифрования в одну большую двоичную комбинацию, называемую массивом данных о совершенных действиях. Как правило хеш – функция задействуется вычислительными устройствами при работе в интернет браузере, что прекрасно знают опытные IT специалисты, а умелые преступники в сфере IT преступлений активно используют данную информацию.

Данная информация, при знании алгоритма дешифрования хеша, позволяет извлечь ценную для злоумышленников информацию, которая часто связана с финансовым состоянием жертвы, либо с логинами и паролями для доступа в личный кабинет сервиса интернет – банкинга, иных виртуальных финансовых сервисов, в том числе это виртуальные кошельки криптовалюты, также это могут быть данные о самой банковской карте или банковском счете. В связи с этим деятельность провайдеров хостинга в настоящее время не требует получения лицензии на оказание услуг связи[2].

В данном параграфе были рассмотрены основные понятия, применяемые при расследовании краж, совершаемых с использованием информационно-телекоммуникационных систем. Данные понятия являются основными, так как при расследовании данного вида краж встречаются наиболее часто и каждому лицу участвующему в раскрытии и расследовании данного вида преступлений необходимо знать значение и сущность данных понятий.

---

[1] Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. № 3. 2019. С. 37 – 45.

[2] Разъяснения Роскомнадзора по вопросу лицензирования деятельности провайдеров хостинга от 20 августа 2016 года // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https:// rkn.gov.ru/it/control/p852 (дата обращения: 09.01.2022).

ГЛАВА 2. КРИМИНАЛИСТИЧЕСКИЕ ОСНОВЫ РАССЛЕДОВАНИЯ КРАЖ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)

§ 1. Криминалистическая характеристика краж, совершаемых с использованием информационно-телекоммуникационных систем (по материалам территориального органа внутренних дел)

Исследуя криминалистическую характеристику преступлений, совершенных с использованием информационно-телекоммуникационных систем, следует отметить, что центральным ее элементом однозначно является способ совершения преступления, способ его сокрытия преступления, которые тесно связаны личностью преступника. Считаем целесообразным сначала рассмотреть личность преступника[1].

Особенностью, характеризующей личность преступника, является наличие профессиональных навыков и знаний в сфере IT технологий, наличие опыта использования аппаратно – программных средств в различных целях, в том числе для получения неправомерного доступа к информации на электронных носителях[2].

Такие личности с большой вероятностью могут получать непосредственный доступ путем удаленного подключения в различные информационные системы и сервисы, умеют анализировать компьютерную информацию, которая написана на языке компьютерных кодов, а также вводить различные изменения в данный компьютерный код, то есть данные лица в большинстве имеют техническое образование или самостоятельно углубленно изучили принципы и правила работы различных информационных систем. В

[1] Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2015. № 3. С. 127 – 132.

[2] Криминалистика: учебник для вузов / Белкин Р. С., Корухов Ю. Г., Российская Е. Р. М.: Издательство НОРМА. 2021. 990 с.

современной действительности важно осознавать тот факт, что существует угроза мировому сообществу, которая выражается в том, что преступники обладают обширными связями на всемирном уровне.

Возникают тесные связи и взаимодействие преступников, которые обмениваются преступным опытом, а также налаживают контакты для сокрытия похищенного имущества, либо обеспечения придания легального вида похищенного имущества на территории иностранных государств. Таким образом, существенно усложняется процесс раскрытия и расследования преступлений[1].

Согласно произведенному анализу деятельности преступников, которые осуществляют кражи, совершаемые с использованием информационно-телекоммуникационных систем, в обязательном порядке следует обращать внимание на тот факт, что основной массив краж, совершаемый в данной сфере не отражается в статистических данных, так как присутствует фактор латентности преступности в данной сфере[2].

Следует отметить, что кражи, совершаемые с использованием информационно-телекоммуникационных систем остаются латентными, так как жертвы преступлений либо боятся насмешек со стороны третьих лиц из – за того, что их ловко «одурачили», то есть ввели в заблуждение и похитили денежные средства, либо не верят в силы правоохранительных органов, так как знают, что данная категория преступлений практически остается нераскрытой[3].

Совсем иным образом дела обстоят с вниманием общественности к уголовным делам расследуемым по фактам кражи в данной сфере, так как они

---

[1] Поддубный И. В. К вопросу об использовании фигурантами информационно-коммуникационных технологий в целях сокрытия хищений с банковских счетов граждан // Вестник Удмуртского университета. Серия «Экономика и право». 2020. № 3. С. 424 – 430.

[2] Полянская Е. П., Никоноров А. А. Информационное взаимодействие следователя со службами негосударственных организаций и подразделениями правоохранительных органов как основа успешного расследования преступлений в сфере высоких технологий // Вестник экономической безопасности. 2021. № 1. С. 49 – 51.

[3] Егоров Н. Н. Криминалистика: учебник и практикум для вузов, 3-е изд., испр. и доп. / Н. Н. Егоров, Е. П. Ищенко. М.: Издательство Юрайт, 2022. С. 75.

обладают широким общественным резонансом, и общественность наблюдает за ходом расследования данных уголовных дел[1].

Ход и результаты расследования уголовных дел по данным кражам (квалифицируемым по пункту «г» части третьей статьи 158 УК РФ), которые получили большое общественное внимание, однозначно попадают в статистический учет. Также отдельно ведется статистическое наблюдение по данным о личности преступника, по немногочисленным уголовным делам, которые удалось раскрыть и в последующем направить их в суд[2].

Основные способы совершения и сокрытия преступных действий при совершении кражи, совершенной с использованием информационно-телекоммуникационных систем:

– способы, которые связаны с получением удаленного доступа к компьютерным средствам;

– способы, которые связанны с непосредственным доступом к компьютерным средствам и системам;

– комбинированные способы, сочетающие в себе первые два способа совершения кражи.

Способы, которые связаны с прямым непосредственным воздействием лица на информационную систему заключаются в том, что требуют предварительной подготовки для преступника, так как необходимо знать, где хранится нужная информация (программное обеспечение, файлы, приложения), и как получить к ней доступ и совершить кражу денежных средств, как сокрыть следы преступных действий.

Данные способы требуют наличия у преступника знаний и навыков в информационных технологиях, в подборе паролей, или иных способов взлома защищенных устройств, аккаунтов, приложений.

---

[1] Дерюгин Р. А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46 – 49.

[2] Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. № 1. С. 152 – 157.

Для успеха в совершении преступления и сокрытии следов преступных действий, как правило, преступники используют свое должностное положение. Они чаще всего являются сотрудниками организации, специализирующимися в ремонте и отладке информационных систем, иных электронно-вычислительных устройств. Не редки случаи когда преступления совершают лица, которые являются работниками организаций, которые предоставляют услуги по ремонту и отладке компьютерного оборудования на возмездной основе[1].

Примером применения данного способа могут являться преступные действия гр. П. В дежурную часть ОМВД России по Мелеузовскому району поступило заявление от гр. С. директора ООО «Сладкий сон» по факту кражи денежных средств с банковского счета предприятия на общую сумму 570 000 рублей совершенного неустановленным лицом, находившемся в неустановленном месте, которое причинило ООО «Сладкий сон» имущественный ущерб в крупном размере. Опрошенный по данному факту гр. С. пояснил, что двумя неделями ранее в помещении бухгалтерии неизвестное лицо по договору с ИП А. осуществляло ремонт и отладку компьютерного оборудования. Иные работники организации, в том числе и бухгалтеры пояснили, что краж они не совершали, ряд бухгалтеров сказали, что лицо мужского пола, которое ремонтировало компьютеры в помещении бухгалтерии спрашивало их о расположении бухгалтерских файлов и программного обеспечения, ремонтировало компьютеры дольше обычного, ссылаясь на сложность программного кода отладки в командной строке[2].

Следователем было вынесено постановление о возбуждении уголовного дела № 00001, а также дано поручение сотрудникам отдела уголовного розыска, об установлении неизвестного лица, которое осуществляло ремонт и отладку компьютеров в ООО «Сладкий сон» и проверки его на причастность к совершению преступления.

---

[1] Криминалистика: учебник и практикум для вузов, 3-е изд., перераб. и доп. / Н. П. Яблоков. М.: Издательство Юрайт, 2022. С 135 – 136.

[2] Уголовное дело № 00001 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 219 л.

Сотрудники уголовного розыска оперативным путем установили местонахождение неизвестного лица, которым оказался гр. П. компьютерный мастер (IT специалист), работающий в ИП А.

П. в ходе опроса дал показания о том, что он не совершал кражу денежных средств из банковского счета ООО «Сладкий сон», когда занимался ремонтом компьютеров.

Также он пояснил, что обнаружил в файловой системе компьютера вредоносное программное обеспечение, которое могло похитить финансовую информацию с данного компьютера, данное вредоносное программное обеспечение он устранил, о чем сказал главному бухгалтеру.

Таким образом, в данном случае присутствует ситуация неочевидности совершения преступления, так как преступные действия были совершены удаленно с использованием вредоносного программного обеспечения, для выяснения того, какая именно программа использовалась и кто ее внедрил следователь назначил судебную компьютерно – техническую экспертизу, по итогам которой была определена конкретная вредоносная программа, относящаяся к троянским коням, но путей внедрения данной программы в ходе проведенной экспертизы установить не удалось[1].

Комбинированные способы и средства, в которых активно используются как получение удаленного доступа к информационной системе банковского онлайн сервиса, так и непосредственное воздействие[2].

В соответствии с ч. 1 ст. 64 Федерального закона Российской Федерации от 7 июля 2003 г. № 126-ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений,

---

[1] Колиев В. В., Шахкелдов Ф. Г. Методика раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Право и практика. 2021. № 1. С. 92 – 95.

[2] Криминалистика в 3 ч. Часть 1 : учебник для вузов, 2-е изд., испр. и доп. / Л. Я. Драпкин [и др.]. М.: Издательство Юрайт, 2022. С. 128.

изображений, звуков, видео- или иных сообщений пользователей услугами связи в течение трех лет с момента окончания осуществления таких действий[1].

Также существует проблема незащищенности клиентов банка в судебных разбирательствах с организацией банка, по поводу незащищенности личных кабинетов банковских онлайн сервисов.

Если проанализировать судебные решения за последние 6-7 лет по спорам между банками и клиентами о хищениях денег через интернет – банк, посредством дистанционного банковского обслуживания (далее – ДБО), собирается интересная статистика.

Суды, как правило, встают на сторону банка. Дело в том, что клиенту крайне сложно доказать, что именно действия или бездействия банка привели к хищению денежных средств[2].

В случаях если сам клиент банка не выполняет элементарных требований безопасности, то решение суда однозначно будет не в пользу клиента банка, но если же клиент осуществлял все необходимые действия, то доказать это очень сложно, так как суд обычно занимает позицию организации банка, как имеющей больший вес и средства по сравнению с клиентом-физическим лицом.

Согласно статье 393 ГК РФ для взыскания понесенных убытков клиент должен представить суду доказательства, подтверждающие нарушение банком принятых по договору обязательств, а также доказать причинную связь между понесенными убытками и неисполнением или ненадлежащим исполнением обязательств.

В этом и заключается проблема, так как вся информация о действиях клиента и операциях, происходящих в системе, имеется лишь у банка, а истребование данной информации практически невозможно без соответствующей санкции суда.

---

[1] О связи: федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2003 г. // Собрании законодательства Российской Федерации. 2003 г. № 28. ст. 2895.

[2] Гриб Г. В., Тюнис И. О. Криминалистика и цифровые технологии // Российский следователь. № 9, 2019. С. 99 – 105.

Получается, что клиент может лишь осуществить техническую экспертизу, которая лишь покажет, что на момент совершения финансовых операций присутствовала вредоносная программа, а в данной ситуации суд сразу отказывает в рассмотрении искового заявления в связи с отсутствием вины банка. Многие специалисты говорят о незащищенности клиентов в условиях договора банка, так как в данном договоре чаще всего все риски по использованию средств дистанционного банкинга лежат на клиенте, а не на стороне банка[1].

У оперативных сотрудников существуют возможности установить организацию сотовой связи, к которой относится абонентский номер, с которого преступники совершали свои действия, посредством обращения и применения информации справочных интернет-ресурсов, таких как «www.spravportal.ru», «www.phonenum.info»[2].

Также в данных ресурсах отображается информация о том, менялся ли оператор при сохранении самого абонентского номера.

В виде таблицы, как правила, предоставляются сведения об абонентах (владельцах абонентских номеров, которые использовались при совершении преступления), соединениях абонентов и (или) абонентских устройств с привязкой к приемопередающим базовым станциям.

Такие данные, должны подвергаться тщательному анализу, подтверждению их в открытых официальных источниках и реестрах, которые помогают в установлении как места совершения вызова от имени оконечного устройства, также они могут предоставить информацию о марке и модели данного устройства, их Ip – адресе, если преступник совершал преступление посредством подключения к сети Интернет, а также при использованиями ими услуг Ip телефонии. Такие данные предоставляют криминалистически

---

[1] Ищенко П. П. Актуальные проблемы судебно-экспертного обеспечения расследования организованной преступной деятельности // Пролог: журнал о праве. 2019. № 4. С. 40 – 45.

[2] Криминалистика в 5 т. Том 5. Методика расследования преступлений : учебник для вузов / И. В. Александров [и др.]. М.: Издательство Юрайт, 2022. С. 63 – 64.

значимую информацию оперативным подразделениям, дают направление для производства оперативно – розыскных мероприятий, следственных действий и иных процессуальных действий. Позволит осуществить запрос в организацию предоставившую преступнику услуги связи, для получения детальной информации о личности преступника и его месте жительства, месте размещения ЭВМ, что даст возможность в последующем планировать производство обысков по данному адресу.

В целях установления местонахождения лица, совершившего преступные действия, в первую очередь, необходимо совершить определенные действия, проанализировав также имеющуюся информацию о способе совершения хищения денежных средств, а также установления вида финансово-платежной системы и счета, на который были отправлены денежные средства[1].

При выяснении обстоятельства о том, что денежные средства со счета потерпевшего похищены неустановленным лицом посредством выхода в сеть Интернет и использования банковского онлайн сервиса с IP – адресов определенного диапазона (с точным посекундным временем), возможно самостоятельно установить компанию-провайдер, предоставившую тот или иной IP – адрес.

Это возможно сделать через справочные интернет-ресурсы (сервисы) «www.Xinit.ru», «www.reg.ru», «www.whois-service.ru», «www.2ip.ru» (в случае необходимости открыть вкладку «IP – LOOKUP»): нужно указать IP – адрес, содержащийся в ответе банка при предоставлении сведений о движении денежных средств по счетам, при этом использовать вкладку «Проверить».

В случае обращения к справочному интернет-ресурсу «www.Xinit.ru» для установления компании-провайдера по IP – адресу необходимо на главной странице сайта открыть вкладку «Продвинутый WHOIS-сервис», в строке «Доменное имя или IP – адрес» указать данные об IP – адресе, предоставленные

[1] Богомолова А. Г. Тактические особенности взаимодействия следователя с общественностью в современных условиях в ходе расследования преступления // Криминалистика: вчера, сегодня, завтра. 2021. № 3. С. 62 – 68.

в сведениях кредитной организации, нажать «Запросить информацию», после чего справочным интернет - ресурсом будет выведена информация о компании-провайдере, использующей интересующие IP – адреса.

Как правило, информация предоставляется в сочетании английских и русских слов с указанием компании-провайдера, ее юридического и фактического адресов, контактного номера телефона (факса)[1].

Полученную через данные справочные интернет – ресурсы информацию можно скопировать посредством производства скриншота с целью приобщения к материалам проверки или уголовного дела, составив соответствующий рапорт на приобщение[2].

После установления компании-провайдера необходимо направить запрос о предоставлении сведений, кому, в какое время (дата, час, минута, секунда) был предоставлен IP – адрес, номер TCP/UDP - порта, указанные в ответе кредитной организации, о местонахождении абонента, использующего данный IP-адрес, дате регистрации договора предоставления услуг связи в сети Интернет, а также о том, с кем заключен договор (ФИО, дата рождения, место регистрации, паспортные данные), информации о логине, пароле, при помощи которых осуществляется доступ клиента в сеть Интернет, о MAC – адресе устройства, с которого осуществлялся выход в сеть Интернет в момент совершения преступления[3].

На данном этапе у оперативных сотрудников возникают трудности в понимании того, что такое MAC-адрес устройства, какое он имеет доказательственное значение в определении места совершения преступления, как его можно определить у телефона, планшета, ноутбука, стационарного компьютера, Wi-Fi роутера.

---

[1] Криминалистическая методика: учебное пособие для вузов / И. В. Александров [и др.]; под редакцией Л. Я. Драпкина. М.: Издательство Юрайт, 2022. С. 158 – 159.

[2] Егоров В. А. Недостатки правового регулирования организации расследования мошенничества, совершенного с использованием средств связи // Юридическая наука и правоохранительная практика. 2018. № 2. С. 125 – 135.

[3] Там же. № 2. С. 125 – 135.

MAC – адрес (англ. Media Access Control -управление доступом к среде, также Hardware Address) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Интернет (Ethernet)[1].

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь шестибайтный номер (MAC – адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации при появлении в сети нового компьютера (или другого устройства, способного работать в сети). Его еще называют «Физический адрес» (MAC – адрес – это уникальный номер сетевой карты компьютера).

Знание MAC-адреса позволяет оперативным подразделениям осуществлять установление конкретного местоположения, при обладании определенными познаниями в сфере информационно-телекоммуникационных технологий. Также оперативным подразделениям необходимо знать, что все устройства, которые подключаются к сети интернет обладают данным идентификатором. Также нужно обладать пониманием, что MAC – адрес должен состоять из шестибайтного номера, который должен прошиваться в сетевой карте при ее изготовлении[2].

Сведения о MAC – адресе легко установить при условии, что злоумышленники совершают действия на территории нашего государства, пользуясь примитивными техническими средствами, не используя средств сокрытия своих преступных действий, или пользуясь устаревшими средствами, которые на данный момент устраняются различными защитными алгоритмами при использовании программного обеспечения того или иного банковского онлайн сервиса.

---

[1] Гаврилин Ю. В., Реент Я. Р. Обеспечение начальником территориального органа МВД России на районном уровне раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2021. № 4. С. 94 – 98.

[2] Там же. С. 94 – 98.

Таким образом, установление способа совершения преступления является одной из важнейших задач при расследовании преступлений в сфере информационно-телекоммуникационных технологий, так как способ совершения преступления является одним из основных обстоятельств, подлежащих выяснению, а также способ совершения преступления сильно влияет на квалификацию состава преступления[1].

В большинстве случаев хищения, которые совершаются с использованием информационно-телекоммуникационных технологий следователи квалифицируют как кража, а именно пункт «г» часть 3 статьи 158 УК РФ: «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств», либо как «Мошенничество с использованием электронных средств платежа» по статье 159.3 УК РФ[2].

В заключение данного параграфа необходимо отметить, что способов совершения преступлений данного вида множество. Как правило они подразделяются на сопряженные с удаленным доступом, а также способы сопряженные с непосредственным доступом к информационно-телекоммуникационной системе.

§ 2. Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования

На первоначальном этапе расследования данной категории уголовных дел, в зависимости от обстановки выделяются следующие типичные следственные ситуации:

– подозреваемый задержан при попытке произвести перевод денежных средств, оплату, снятие денежных средств с использованием банковских онлайн сервисов;

---

[1] Криминалистическая методика: учебное пособие для вузов / А. Г. Филиппов [и др.]. М.: Издательство Юрайт, 2022. С. 281.

[2] Иванова О. М., Иванов М. Г. Проблема квалификации «бесконтактных» хищений на стадии возбуждения уголовных дел // Вестник РУК. 2021. № 3. С. 123 – 125.

– поступила информация или заявление о незаконном использовании банковской карты или же банковских онлайн сервисов от держателя банковской карты в связи с похищением у него денежных средств, лицо совершившее хищение не установлено, но есть информация, связанная с номером его телефона, информации с социальных сетей и так далее[1];

– поступила информация или заявление о незаконном использовании банковской карты или же банковских онлайн сервисов от держателя банковской карты в связи с похищением у него денежных средств, лицо совершившее хищение не установлено, информация о лице отсутствует, в связи с использованием злоумышленником средств сокрытия своих преступных действий;

– поводом для возбуждения уголовного дела послужили результаты проведения оперативно-розыскных мероприятий, при проведении которых были выявлены факты хищения денежных средств с использованием банковских онлайн сервисов и иных средств платежей, подозреваемый установлен[2].

При расследовании данных категорий уголовных дел, касательно сущности совершенного преступления отрабатываются следственные версии. Существуют рекомендации следователям в расследовании данных преступлений на первоначальном этапе.

Для установления местонахождения электронно-вычислительного устройства с которого получался удаленный доступ, технических средств, которые использовались в процессе хищения денежных средств следователю (дознавателю) необходимо совершись следующие действия:

– получить сведения о поступивших звонках и СМС-сообщениях путем запроса детализации абонентских действий (с какого номера в

[1] Егоров В. А. Недостатки правового регулирования организации расследования мошенничества, совершенного с использованием средств связи // Юридическая наука и правоохранительная практика. 2018. № 2. С. 125 – 135.

[2] Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98 – 106.

действительности совершались вызовы и оправлялись СМС – сообщения и в какое время), данные о финансовых операциях в отделении банка, легче всего предложить потерпевшему самостоятельно запросить информацию об абонентских соединениях и совершенных финансовых операциях, так как клиенту от оператора связи и банка ответ на запрос приходит гораздо быстрее[1].

Владельцами таких платежных систем, как RBK money, WebMoney, Деньги@mail.ru, Money Mail являются юридические лица, которые расположенные на территории Российской Федерации. В свою очередь владельцами платежных систем PayPal, Liberty Reserved и многих других сервисов являются юридические лица, которые зарегистрированы и находятся за пределами России, а на территории Российской Федерации у данных организаций в некоторых случаях имеются лишь филиалы и представительства, которые не обладают полномочиями предоставления каких-либо функций, а выполняют лишь отдельные функции данного юридического лица[2].

– направление в организацию-провайдер, которой принадлежит интересующий ip-адрес, запроса о предоставлении информации об абоненте, который работал в сети «Интернет» во время совершения операций с похищенными электронными денежными средствами.

Такой запрос необходимо направлять на имя руководителя организации-провайдера. В ответе на запрос обычно указываются следующие сведения об абоненте: фамилия, имя, отчество; номер договора о предоставлении услуги доступа в сеть «Интернет»; фактический адрес (город, улица, дом, квартира); иные сведения в рамках запроса.

Полученные из компании-провайдера сведения укажут, что именно с компьютерной техники данного абонента, находящейся по конкретному адресу, осуществлялись онлайн-транзакции.

---

[1] Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98 – 106.

[2] Кучин О. С., Гаврилин Ю. В. Тенденции и проблемы в развитии современной российской криминалистики // Академическая мысль. 2020. № 4 . С. 85 – 89.

По мнению авторов, местом окончания рассматриваемых видов преступлений является место нахождения оборудования (компьютерной техники, средств мобильной связи), с которого преступник осуществляет администрирование виртуального счета электронной платежной системы (открытие виртуального счета, переводы виртуальных денежных средств и т. д.), то есть получает реальную возможность распоряжения или фактически распоряжается похищенными денежными средствами[1].

Временем окончания преступления целесообразно считать совершение преступного действия, а именно момент в который денежные средства поступили на виртуальный счет в электронной платежной системе или на банковский счет, принадлежащий злоумышленникам, их пособникам или иным лицам, в последующем которые путем обмана или уговоров перечислят денежные средства преступникам[2].

Важное значение имеет также установление должностным лицом, осуществляющим расследование данного преступления информации о собственниках объектов недвижимости, где находится электронно-вычислительная техника – орудие преступления. Данное действие необходимо для того, чтобы в кратчайшие сроки после возбуждения уголовного дела принять решение о производстве обысков в жилищах граждан либо в иных объектах недвижимости, далее осуществить уведомление данного лица о производстве следственных действий на территории недвижимого имущества, которая является его собственностью[3].

Проведение в установленном уголовно-процессуальным законом порядке с участием специалиста изъятия электронно-вычислительной техники, явившейся орудием совершения преступления. Данное действие следует

[1] Миронова А. В. Оказание международной правовой помощи в получении электронных доказательств // Вестник Московского университета МВД России. 2020. № 3. С. 78 – 80.

[2] Гаврилин Ю. В. Участие негосударственных организаций в выявлении, раскрытии и расследовании преступлений // Академическая мысль. 2018. № 3. С. 26 – 29.

[3] Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98 – 106.

проводить как можно скорее после принятия решения о возбуждении уголовного дела в целях исключения утраты следов совершенного преступления. При этом необходимо обеспечить неизменность состояния указанной техники на момент изъятия, так как, например, ее включение может привести к потере или модификации важной с точки зрения доказывания информации.

Также рекомендуется следовать разработанным в криминалистике указаниям о способах упаковки такой техники. Нарушение этого требования тоже может привести к потере или изменению важной с точки зрения доказывания информации или вызвать сомнения в части ее неизменности[1].

Проведение в установленном законом порядке осмотра изъятой техники и содержащейся в ней информации. Для доступности восприятия доказательств интересующие сведения можно оформить приложением к протоколу осмотра, например таблицей либо схемой. Анализ судебно-следственной практики свидетельствует о том, что осмотр изъятой в ходе расследования техники является одним из основных доказательств по уголовным делам о хищениях электронных денежных средств.

Назначение компьютерно-технической судебной экспертизы для исследования изъятой электронно-вычислительной техники, по результатам которой может быть восстановлена практически любая ранее удаленная с носителей информация (файлы, папки, базы данных и др.). Далее действовать из сложившейся следственной ситуации[2].

При обнаружении преступных действий, особенно на ранних стадиях, необходимо помнить, что хищения денежных средств со счета могут происходить неоднократно. В целях предупреждения данных случаев потерпевшим лицам рекомендуется в первую очередь предпринять меры по

---

[1] Кондратьев Ю. А., Сафонов О. М. Особенности толкования термина «компьютерные технологии» для целей уголовно-правового регулирования // Конвенционные начала в уголовном праве: материалы Международной научно-практической конференции. М.: РПА Минюста России. С. 165 – 168.

[2] Каиргалиева Д. Ж. Проблемы предупреждения преступлений с использованием сети интернет // Вестник магистратуры. 2019. № 9-2. С. 113 – 115.

блокировке своих аккаунтов в банковских онлайн сервисах или же блокировке банковских карт, с последующим перевыпуском данных карт.

Таким образом все действия, которые могут быть совершены дистанционно или при использовании устройств банкоматов невозможны к выполнению, а все операции в период перевыпуска банковской карты, могут быть совершены при обращении клиентом банка к сотрудникам ближайшего отделения банка лично с предъявлением документа, удостоверяющего личность (как правило, паспорт гражданина РФ или паспорт гражданства иностранного государства)[1].

Министерство внутренних дел Российской Федерации (далее – МВД РФ) на своем официальном сайте рекомендует лицам, потерпевшим от преступлений данного вида, а также лицам, на банковские счета которых оказываются попытки воздействия со стороны злоумышленников в данных ситуациях разрешать все проблемы, связанные с выполнением финансовых операции непосредственно в банковских отделениях банка при личном обращении к сотрудникам банка[2].

Необходимо помнить, что преступники чаще всего обладают навыками психологии и активно их используют при совершении преступлений. Нельзя при таких ситуациях сразу бросаться выполнять действия или требования лиц, звонящих с подозрительных номеров, или как в вышеописанном случае, когда звонок совершается с якобы официального номера обслуживающего банка, но на самом деле с номера, замаскированного аппаратными средствами.

Категорически запрещается сообщать сведения о своем местоположении или иной информации, которая может быть использована преступниками. Ни в коем случае нельзя сообщать различные коды подтверждения, которые могут

---

[1] Косарев К. В. Отдельные вопросы раскрытия и расследования мошенничеств, совершаемых с использованием мобильных телефонов // Закон и право. 2019. № 9. С. 129 – 130.

[2] Темиралиев Т. С., Омаров Е. А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения // Вестник Института законодательства и правовой информации Республики Казахстан. 2019. № 1. С. 93 – 99.

быть присланы по СМС- сообщению в ходе телефонного разговора, также при отсылке данных кодов подтверждения снизу текстом, в большинстве случаев лица предупреждаются о том, что данные коды подтверждения должен знать лишь данное лицо, а также о том, что данные коды подтверждения нельзя никому сообщать, даже сотруднику банка.

При наличии возможности позвонить со второго телефона, обязательно путем самостоятельного набора с клавиатуры телефона официального номера банка или же экстренных служб, органов полиции, не прерывая при этом общения с звонящим[1].

Данный звонок осуществляется с целью сообщить, что лицу совершается звонок, с конкретного номера, требуется совершение конкретных действий или же запрашивается какая-либо информация. В данной ситуации сотрудники банка могут проверить данную информации и сообщить рекомендуемые действия, а экстренные службы и органы полиции сориентируют в недопущении хищения денежных средств[2].

Если появились подозрения о том, что по телефонному разговору совершается кража, необходимо исключить слова подтверждения или отрицания, также можно сообщить звонящему что его якобы плохо слышно, данный прием позволит выиграть время для обдумывания дельнейших действий, и запоминания голоса звонящего лица и номера телефона, с которого осуществляется вызов[3].

Рекомендуется сохранять (не удалять) номера телефонов, с которых осуществлялись вызовы, в записной книжке или истории звонков в телефоне, а также необходимо записать точную дату и время совершения звонков. Для установления точного номера телефона, в случаях если при звонке на

[1] Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / С. В. Зуев. М.: Издательство Юрайт, 2022. С. 19 – 21.

[2] Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98 – 106.

[3] Каиргалиева Д. Ж. Проблемы предупреждения преступлений с использованием сети интернет // Вестник магистратуры. 2019. № 9-2. С. 113 – 115.

мобильном устройстве номер телефона не определился, то можно осуществить заказ детализации всех звонков и сообщений, в которых будут отображены реальные номера с которых совершались те или иные действия[1].

Детализацию всех действий, совершенных с абонентского номера телефона той или иной организации сотовой связи, как правило можно заказать через мобильное приложение оператора сотовой связи. В данных приложения характерно присутствие инструментов, позволяющих совершить заказ данной детализации.

Следует заявлять обо всех случаях в органы полиции совершения данных действий, будь то удачная попытка хищения денежных средств или же при неудавшейся попытке похитить денежные средства. При сообщении данной информации необходимо указывать все номера телефонов, звонивших или отправлявших СМС – сообщения, информацию о лицах, связывавшихся посредством использования электронной почты или же социальных сетей. Необходимо оповестить близких лиц и окружение о данных действиях, в целях недопущения воздействия уже на них[2].

В случае же если хищение денежных средств уже совершено необходимо сообщить данную информацию в полицию, оператору сотовой связи, в организацию банка.

При сообщении информации оператору сотовой связи и организации банка, есть возможность узнать о том, что вероятно данный случай хищения денежных средств не единственный, следовательно, и установить иные случаи хищения денежных средств, также возможно удастся вычислить злоумышленников.

---

[1] Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды Академии управления МВД России. 2018. № 4. С. 48 – 51.

[2] Косарев К. В. Отдельные вопросы раскрытия и расследования мошенничеств, совершаемых с использованием мобильных телефонов // Закон и право. 2019. № 9. С. 129 – 130.

§ 3. Проблемы, возникающие в ходе расследования краж, совершенных с использованием информационно-телекоммуникационных систем и пути их решения (по материалам территориального органа внутренних дел)

При расследовании краж, совершаемых с использованием информационно-телекоммуникационных систем возникают проблемы различного рода. К ним можно отнести низкий уровень подготовленности и профессиональности как следователей, так и сотрудников оперативных подразделений, в связи с чем данные преступления не раскрываются и не расследуются.

Также к проблемам можно отнести отсутствие в ряде случаев содействия расследованию со стороны организаций и подразделений, которые предоставляют услуги связи, являются провайдерами или владельцами интернет ресурсов[1].

Одной из проблем в расследовании данного вида преступлений является невозможность отслеживать следы преступной деятельности в информационной среде, что связано с использованием преступниками различных систем и сервисов, программного и аппаратного обеспечения, которые позволяют скрыть действия преступника[2].

К данным системам и сервисам относятся:

1) VPN – виртуальная частная сеть, которая позволяет пользователю сети интернет подключаться к данной сети зашифровано и конфиденциально, обходить локальную информационную систему и ее ограничения. При использовании данного сервиса действия, которые совершает пользователь, как правило, отображаются как действия, совершаемые через IP – адрес

[1] Шевко Н. Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки Казанского юридического института МВД России. 2016. № 1. С. 13 – 16.

[2] Климова Я. А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. № 4. С. 128 – 132.

используемой виртуальной частной сети, а их расположение в основном находится в иностранных государствах по всему миру[1].

В ходе расследования уголовного дела № 00002 по факту кражи совершенной дистанционным способом, путем взлома аккаунта социальной сети «В Контакте» принадлежащего А. был осуществлен запрос в ООО «В Контакте» о предоставлении сведений о подключении к аккаунту А. В ответе на запрос ООО «В Контакте» предоставили сведения о всех подключениях за запрошенный период, среди которых имелся IP – адрес не принадлежащий А. В открытых источниках таких как 2ip.ru и другие, данный IP – адрес располагался в Гвинейской Республике. Возник вопрос в том, кто является владельцем данного IP – адреса. Из открытых источников в сети интернет оперативным путем было установлено, что данный IP – адрес используется Гвинейской организацией для предоставления VPN (виртуальная частная сеть) соединения[2].

Данный случай иллюстрирует о сложности установления лица, причастного к совершению преступления, так как по запросам, направляемым в зарубежные страны о предоставлении информации об Ip – адресе лица, который пользовался услугами VPN, ответы от исполнителей приходят неполноценные, либо не приходят вовсе.

Относительно недавно появился новый аппаратно-программный комплекс, который позволяет злоумышленникам маскировать свой номер под видом другого номера телефона в целях совершения мошеннических действий посредством совершения вызовов, отправки СМС-сообщений. При этом чаще всего данным вызовам предшествуют действия по получению несанкционированного доступа в личные кабинеты клиентов банка через приложения банков, обычно способом подбора ПИН – кодов, необходимых для получения доступа, также злоумышленники должны располагать сведениями о

---

[1] Степанова М. А., Царёв Е. В. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий // Вестник БелЮИ МВД России. 2021. № 1. С. 12 – 16.

[2] Уголовное дело № 00002 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 193 л.

самой банковской карте (номер карты, имя держателя карты, срок действия карты, защитный трехзначный код на обратной стороне карты) или логин личного кабинета банковского онлайн сервиса[1].

В последующем для совершения аунтификации (входа) в личный кабинет преступникам необходимо получить защитный код для подтверждения входа, который как правило приходит на номер телефона самого держателя карты или же номер телефона, привязанный к личному кабинету банковского онлайн сервиса. Для получения данного кода преступники совершают телефонный звонок под видом официального номера банка (на примере банка ПАО «Сбербанк», злоумышленники маскируют свой номер под официальный номер банка: 900) и узнают данный код.

Также если для доступа к личному кабинету банковского онлайн сервиса вышеуказанный код не нужен, для перевода денежных средств со стороннего устройства необходимо подтверждение данного перевода, с помощью кода подтверждения или же устного подтверждения, также через телефонный звонок. Для получения данного подтверждения осуществляется телефонный звонок с маскировкой своего номера телефона, под номер телефона банка и преступникам необходимо услышать и записать слово «Да» сказанное держателем карты. Получить слово подтверждения достаточно просто, представившись сотрудником банка с первых слов общения можно спросить, например: «Это Иванов Иван Иванович?», далее клиент банка отвечает: «Да».

В последующем конечно злоумышленники могут спросить действительно ли он совершают данную операцию, если не совершают, то посоветуют заблокировать банковскую карту, но блокировка карты не поможет, денежные средства на этот момент уже похищены. В данных случаях рекомендуется при общении избегать слов «да» или «нет», иных слов подтверждения. Следует помнить, что, как правило, сотрудники банка с официального номера никогда сами никогда не звонят, или же звонят с официальных телефонов

[1] Васильков Е. Д. Электронные носители информации в уголовном судопроизводстве // StudNet. 2021. № 6. С. 1825 – 1833.

подразделений банка, информацию о которых можно узнать на официальном сайте подразделения банка в сети Интернет. Также особое внимание следует обращать на особенности проведения следственных действий, которые являются наиболее часто производимыми по данной категории уголовных дел[1].

После этого преступники, пользуясь тем или иным банковским онлайн сервисом, перечисляет денежные средства со счета или сразу всех счетов потерпевшего посредством перевода по номеру карты или по номеру телефона, привязанному к данному сервису, также переводы осуществляются на счета электронных кошельков (виртуальных кошельков) платежных систем (Qiwi, WebMoney и т.п.)[2].

Одним из способов совершения хищения является воздействие преступником через телефонный разговор на потерпевшего с использованием манипуляций, психологических воздействий. Чаще всего потерпевший под диктовку, находясь в заблуждении перечисляет денежные средства сам со своего счета на банковские счета преступника, чаще всего под предлогом исправления ошибок в системе, либо подключает услугу к номеру телефона, принадлежащего преступнику, а далее совершается перевод денежных средств.

Бывают ситуации, когда преступники воздействуют на лица, которым принадлежат банковские онлайн сервисы, через социальные сети или через электронную почту. Злоумышленники в процессе общения выясняют необходимые им данные, тем самым получая доступ к личным кабинетам владельцев. Чаще всего данные действия совершаются путем рассылки различных сообщений и уведомлений о том, что адресант якобы победил в каком-либо розыгрыше или лотереи и для перевода им всего лишь необходимо сообщить данные о банковской карте, после ввода владельцем карты данных ему сообщают о необходимости ввода кода подтверждения, отправленного ему

---

[1] Рязанова Е. Н. Правовые аспекты определения места совершения и момента окончания хищения денежных средств с использованием информационно-коммуникационных технологий // Юридическая наука. 2021. № 10. С. 91 – 93.

[2] Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды Академии управления МВД России. 2018. № 4. С. 48 – 51.

системой по СМС – сообщению. Иногда, находясь в заблуждении, владельцы карт могут установить на свое устройство, будь то компьютер или телефонное устройство, якобы в целях, достижение которых как связано с выполнением финансовых операций, так и не связанных с ними.

В случае, когда лицо устанавливает программное обеспечение не с лицензионных сайтов, либо, когда для расширения своих полномочий посредством получения Root-доступа пользователь устанавливает программное обеспечение, и чаще всего данные программы содержат в своих файлах вредоносные программы или полностью являются ими, но лишь замаскированными под официальное программное обеспечение. Позже данные вредоносные средства получают доступ к данным или к действиям связанными с денежными средствами пользователя[1].

После получения внешнего (удаленного) доступа к устройству, совершаются операции на заранее подысканном электронно-вычислительном устройстве, оснащенным доступом к информационно-телекоммуникационной сети Интернет.

При этом совершенные операции самой системой банка распознаются как действия истинного владельца банковской карты. В последнее время набирает популярность один из способов совершения преступления, по которому преступники получают доступ к личному кабинету банковского онлайн сервиса посредством осуществления одного из вышеуказанного способа, далее перечисляют денежные средства на счета абонентских номеров сим-карт, в последующем преступники отправляют СМС-сообщение на номер телефона сим-карты где сообщают о том, что им якобы по ошибке отправили денежные средства на счет и просят их вернуть переводом на номер банковской карты, интернет кошельки («QIWI», «Web money» и т.д.).

[1] Рясов А. А., Жигалова Г. Г., Аветисян А. Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // МНКО. 2018. № 4. С. 72 – 74.

Тем самым лицо, которому были отправлены денежные средства на счет абонентского номера сим-карты не подозревает, что своими действиями фактически способствует совершению преступления, также рискуя стать сообщником, если не будет доказано, что данное лицо осуществляло свои действии в состоянии добровольного заблуждения[1].

В правоприменительной практике местом преступления в силу того, что лиц, совершающих данные преступления, а также их место их расположения установить очень сложно, выбирают место расположения (жительства) потерпевшего.

Так в ходе расследования уголовного дела № 00003 по факту кражи денежных средств неустановленным лицом путем перевода денежных средств с банковской карты потерпевшей П., данные которой были похищены путем обмана, под предлогом помощи в получении выплаты за лечение от COVID – 19, местом предварительного следствия было место жительства потерпевшего, а именно город Мелеуз[2].

С целью установления места выхода телефона (абонентского устройства) в эфир необходимо своевременно подготовить материалы о разрешении получения в компании сотовой связи информации о соединениях между абонентами и (или) абонентскими устройствами с привязкой к приемопередающим базовым станциям[3].

Также при существовании угрозы уничтожения вещественных доказательств, необходимо предварительно, путем направления запросов в ЖЭУ, Росреестр, в организацию, обеспечивающую электропитание данного

---

[1] Косарев К. В. Отдельные вопросы раскрытия и расследования мошенничеств, совершаемых с использованием мобильных телефонов // Закон и право. 2019. № 9. С. 129 – 130.

[2] Уголовное дело № 00003 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 156 л.

[3] Аветисян А. Д., Рясов А. А. Особенности работы следователя с объектами – носителями электронной информации при раскрытии и расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 3. С. 109 – 112.

помещения, а также в организацию, предоставляющую доступ к Интернет соединению (Интернет – провайдер), для того чтобы выяснить соответственно, план схему данного помещения организации или учреждения, схему электропитания, чтобы в последующем не допустить отключения компьютеров от питания, изучить линию оптоволоконной сети, которая обеспечивает соединение компьютеров как внутри помещения, так и их взаимодействие с глобальной сетью[1].

К тому же таким образом можно выяснить, какой компьютер является главным в сети, так как вся важная информация, в том числе бухгалтерская, может храниться на памяти данного устройства.

Как известно из положений дисциплины противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий информация может также храниться в оперативно – запоминающем устройстве (далее – ОЗУ), свойства которого является стирание информации из памяти ОЗУ при выключении устройства от сети электропитания[2].

Также существует проблема, которая связана увеличением количества дропов, предоставляющих свои банковские карты преступникам, среди специалистов в области юриспруденции есть мнение, что данных дропов необходимо привлекать к юридической ответственности, за безразличное отношение к тому факту, что их банковская карта, которую они сами добровольно передают в руки преступникам, может быть использована в преступных целях.

Так ряд ученых предлагает привлекать данных лиц в качестве пособников в совершении преступления, то есть квалифицировать данные действия по основной статье вменяемого деяния со ссылкой на часть 5 статьи 33 УК РФ.

---

[1] Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды Академии управления МВД России. 2018. № 4. С. 48 – 51.

[2] Косарев К. В. Отдельные вопросы раскрытия и расследования мошенничеств, совершаемых с использованием мобильных телефонов // Закон и право. 2019. № 9. С. 129 – 130.

Данная точка зрения является не вполне правильной, так как существуют проблемы с доказыванием факта пособничества в совершении именно данного эпизода преступной деятельности. Трудно доказать, что именно та банковская карта, которую передал «дроп» в преступное пользование использовалась для совершения конкретного перевода денежных средств добытых преступным путем, что это именно те денежные средства, которые были похищены у гражданина Иванова[1].

Сложно доказывать факт, что дропу заведомо было известно о преступных намерениях использования его банковской карты, так как дроп может сказать, что его обманули и под иным благовидным предлогом попросили помочь открыть банковскую карту.

Часто «дропы» говорят, что сам приискатель «дропов» не говорит о его преступных намерениях, что они сами не спрашивают о целях данной сделки, а в данном случае на лицо именно сделка, пусть и не совсем законная, так как лицу предлагается на возмездной основе оформить на себя банковскую карту и передать ее иному лицу. Что «дропы», а как правило это студенты, при виде пяти тысячной купюры, которую предлагают ему за совершение данных действий, без раздумий идут оформлять банковскую карту, так как у студентов лишних денег не бывает[2].

Часть исследователей данного вопроса предлагают ввести ответственность за данное деяние в рамках административного законодательства в качестве отдельного состава административного правонарушения.

На практике данный вопрос решается очень просто, «дропов» привлекают к уголовной ответственности за соучастие в легализации (отмывании)

---

[1] Шапиро Л. Г. Основные направления развития криминалистической методики в условиях цифровизации и глобализации преступности // Вестник СГЮА. 2021. № 6. С. 224–226.

[2] Рясов А. А., Жигалова Г. Г., Аветисян А. Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // МНКО. 2018. № 4. С. 72–74.

денежных средств добытых преступным путем. Так существует реальная судебная практика привлечения «дропов» по определенной части (пункту) статьи 174 УК РФ со ссылкой на часть пятую статьи 33 УК РФ.

На практике складывается такая картина, что в общественно – опасном деянии, которое совершают «дропы», лучше всего усматривать не пособничество в совершении мошенничества, а пособничество в совершении легализации (отмывании) денежных средств, добытых преступным путем. Так сложилось потому, что доказательную базу можно собрать лишь по причастности дропов к пособничеству в совершении отмывания денежных средств, когда они передают члену организованной преступной группы свою банковскую карту для совершения преступных действий.

Таким образом, в данном параграфе были рассмотрены основные проблемы, которые могут возникнуть на различных досудебных этапах уголовного процесса у следователя при расследовании уголовных дел по кражам, совершенным с использованием информационно-телекоммуникационных систем. В данном параграфе были предложены наиболее эффективные с точки зрения правоприменительной практики способы решения данных проблем.

ЗАКЛЮЧЕНИЕ

В дипломной работе были рассмотрены основные понятия, касающиеся исследуемого вида преступлений, статистические данные за 2021 год о количестве преступлениях, совершаемых с использованием информационно-телекоммуникационных систем. Сформулированы динамические показатели роста по сравнению 2020 годом, выявлены основные причины изменения количественных и качественных показателей. Кроме того, автором изучены количественные показатели числа пользователей различных популярных банковских онлайн-сервисов, рассмотрены способы совершения преступных действий с использованием разнообразных программно-технических средств, а также способы сокрытия следов преступлений в информационно-технической среде.

В первой и второй главах исследования, в целом рассмотрены криминалистические особенности установления тех или иных обстоятельств, имеющих значение для раскрытия и расследования краж с использованием информационно-телекоммуникационных систем. В работе отражены некоторые проблемы, возникающие при раскрытии и расследовании указанного вида преступлений, сформулированы рекомендации по проведению следственных и иных действий и мероприятий на первоначальном этапе расследования.

Исходя из данных исследования, следует сделать вывод, что расследование краж, совершенных с использованием информационно-телекоммуникационных систем требует значительного совершенствования в методах действий сотрудников правоохранительных действий. Немаловажное значение здесь имеет стремительный темп совершенствования механизма преступной деятельности, возрастающий групповой характер этих преступлений[1].

[1] Балашов Д. Н. Криминалистика: учебник для вузов / Д. Н. Балашов, Н. М. Балашов, С. В. Маликов. М.: ИНФРА-М, 2019. С. 124 – 126.

Современное развитие компьютерных технологий сопровождается непрерывным ростом преступлений, совершенных с использованием информационно-телекоммуникационных систем, что подтверждено официальной статистикой и научными исследованиями, как в России, так и за границей.

В рамках данной дипломной работы нами были решены поставленные цели и достигнут задачи исследования. Сформулирован понятийный аппарат исследования, изучена историческая составляющая использования интернет-технологий в преступных целях, рассмотрены основные способы совершения краж с использованием информационно-телекоммуникационных систем, изучены организационно тактические особенности отдельных следственных действий на первоначальном этапе расследования; выявлены некоторые проблемы расследования указанного вида преступлений и сформулированы рекомендации по их разрешению.

Учитывая эту глобальную негативную тенденцию в области правовой борьбы с преступностью в сети Интернет, необходимы решительные меры по противодействию и профилактике данного вида преступлений криминалистического и уголовно-правового характера. Принимая во внимание всепроникающее внедрение Интернет во все сферы жизнедеятельности общества, представляется, что проблема преступности в сети Интернет, являясь одной из главных составляющих Информационной безопасности РФ, относится к актуальным, своевременным, имеющим теоретическое и практическое значение[1].

[1] Рясов А. А., Жигалова Г. Г., Аветисян А. Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // Мир науки, культуры, образования. 2018. № 4. С. 72 – 74.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправке к Конституции Российской Федерации от 4 июля 2020 г. № 1-ФКЗ // Собрание законодательства Российской Федерации. 2020. № 44. ст. 2358.

2. Уголовный кодекс Российской Федерации: федеральный закон Российской Федерации от 13 июня 1996. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25, ст.2954.

3. Уголовно – процессуальный кодекс Российской Федерации: федеральный закон Российской Федерации от 18 декабря 2001. № 174-ФЗ // Собрании законодательства Российской Федерации. 2001. № 52. ст. 4921.

4. Гражданский кодекс Российской Федерации. Часть вторая: федеральный закон Российской Федерации от 26 января 1996 г. № 14-ФЗ // Собрании законодательства Российской Федерации. 1996. № 5. ст. 410.

5. Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации 2006. № 31. ст. 3448.

6. О связи: федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2003 г. // Собрании законодательства Российской Федерации. 2003 г. № 28. ст. 2895.

7. Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов: инструкция Банка России от 30 мая 2014 года № 153–И // Вестник Банка России № 60. 2014.

8. Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Банка России от 24.12.2004 № 266-П // Вестник Банка России № 17. 2005.

II. Учебная, научная литература и иные материалы:

1. Аветисян А. Д., Рясов А. А. Особенности работы следователя с объектами – носителями электронной информации при раскрытии и расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 3. С. 109–112.

2. Анучина О. В., Анучин А. П. О некоторых процессуальных средствах изучения личности разыскиваемого подозреваемого (обвиняемого) в информационно-коммуникационной среде // Политика и общество. 2021. № 3. С. 3–7.

3. Балашов Д. Н. Криминалистика: учебник для вузов / Д. Н. Балашов, Н. М. Балашов, С. В. Маликов. М.: ИНФРА-М, 2019. 503 с.

4. Богомолова А. Г. Тактические особенности взаимодействия следователя с общественностью в современных условиях в ходе расследования преступления // Криминалистика: вчера, сегодня, завтра. 2021. № 3. С. 62–68.

5. Васильков Е. Д. Электронные носители информации в уголовном судопроизводстве // StudNet. 2021. № 6. С. 1825–1833.

6. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды Академии управления МВД России. 2018. № 4. С. 48–51.

7. Гаврилин Ю. В. Участие негосударственных организаций в выявлении, раскрытии и расследовании преступлений // Академическая мысль. 2018. № 3. С. 26–29.

8. Гаврилин Ю. В., Реент Я. Р. Обеспечение начальником территориального органа МВД России на районном уровне раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2021. № 4. С. 94–98.

9. Гриб Г. В., Тюнис И. О. Криминалистика и цифровые технологии // Российский следователь. 2019. № 9. С. 99–105.

10. Дерюгин Р. А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46–49.

11. Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. № 1. С. 152–157.

12. Егоров В. А. Недостатки правового регулирования организации расследования мошенничества, совершенного с использованием средств связи // Юридическая наука и правоохранительная практика. 2018. № 2. С. 125–135.

13. Егоров Н. Н. Криминалистика: учебник и практикум для вузов, 3-е изд., испр. и доп. / Н. Н. Егоров, Е. П. Ищенко. М.: Издательство Юрайт, 2022. 1018 с.

14. Егоров Н. Н. Криминалистика: учебник и практикум для вузов, 2-е изд., испр. и доп. / Н. Н. Егоров, Е. П. Ищенко. М.: Издательство Юрайт, 2020. 613 с.

15. Зубакина Ю. К. Интернет-банкинг как современная форма банковского обслуживания // Молодой ученый. 2019. № 22. С. 79 – 84.

16. Иванова О. М., Иванов М. Г. Проблема квалификации «бесконтактных» хищений на стадии возбуждения уголовных дел // Вестник РУК. 2021. № 3. С. 123–125.

17. Ищенко П. П. Актуальные проблемы судебно-экспертного обеспечения расследования организованной преступной деятельности // Пролог: журнал о праве. 2019. № 4. С. 40–45.

18. Каиргалиева Д. Ж. Проблемы предупреждения преступлений с использованием сети интернет // Вестник магистратуры. 2019. № 9-2. С. 113–115.

19. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

20. Климова Я. А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. № 4. С. 128–132.

21. Колиев В. В., Шахкелдов Ф. Г. Методика раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Право и практика. 2021. № 1. С. 92–95.

22. Кондратьев Ю. А., Сафонов О. М. Особенности толкования термина «компьютерные технологии» для целей уголовно – правового регулирования // Конвенционные начала в уголовном праве: материалы Международной научно-практической конференции. М.: РПА Минюста России. С. 165–168.

23. Косарев К. В. Отдельные вопросы раскрытия и расследования мошенничеств, совершаемых с использованием мобильных телефонов // Закон и право. 2019. № 9. С. 129 – 130.

24. Криминалистика в 3 ч. Часть 1 : учебник для вузов, 2-е изд., испр. и доп. / Л. Я. Драпкин [и др.]. М.: Издательство Юрайт, 2022. 246 с.

25. Криминалистика в 5 т. Том 5. Методика расследования преступлений : учебник для вузов / И. В. Александров [и др.]. М.: Издательство Юрайт, 2022. 242 с.

26. Криминалистика: тактика и методика: учебник для вузов / И. В. Александров. М.: Издательство Юрайт, 2022. 313 с.

27. Криминалистика: учебник для вузов / Белкин Р. С., Корухов Ю. Г., Российская Е. Р. М.: Издательство НОРМА. 2021. 990 с.

28. Криминалистика: учебник и практикум для вузов, 3-е изд., перераб. и доп. / Н. П. Яблоков. М.: Издательство Юрайт, 2022. 239 с.

29. Криминалистическая методика: учебное пособие для вузов / А. Г. Филиппов [и др.]. М.: Издательство Юрайт, 2022. 338 с.

30. Криминалистическая методика: учебное пособие для вузов / И. В. Александров [и др.]; под редакцией Л. Я. Драпкина. М.: Издательство Юрайт, 2022. 386 с.

31. Кучин О. С., Гаврилин Ю. В. Тенденции и проблемы в развитии современной российской криминалистики // Академическая мысль. 2020. № 4. С. 85–89.

32. Миронова А. В. Оказание международной правовой помощи в получении электронных доказательств // Вестник Московского университета МВД России. 2020. № 3. С. 78–80.

33. Морар И. О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? // Российский следователь. 2018, № 13. С. 34–38.

34. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2019. № 1. С. 45–55.

35. Першин А. Н. Документированная коммуникация как социальный след преступной деятельности // Психопедагогика в правоохранительных органах. 2015. № 4. С. 73–76.

36. Поддубный И. В. К вопросу об использовании фигурантами информационно-коммуникационных технологий в целях сокрытия хищений с банковских счетов граждан // Вестник Удмуртского университета. Серия «Экономика и право». 2020. № 3. С. 424–430.

37. Полянская Е. П., Никоноров А. А. Информационное взаимодействие следователя со службами негосударственных организаций и подразделениями правоохранительных органов как основа успешного расследования преступлений в сфере высоких технологий // Вестник экономической безопасности. 2021. № 1. С. 49–51.

38. Разъяснения Роскомнадзора по вопросу лицензирования деятельности провайдеров хостинга от 20 августа 2016 года // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и

массовых коммуникаций. URL: https://rkn.gov.ru/it/control/p852 (дата обращения: 09.01.2022).

39. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / С. В. Зуев. М.: Издательство Юрайт, 2022. 243 с.

40. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. С. 37–45.

41. Рязанова Е. Н. Правовые аспекты определения места совершения и момента окончания хищения денежных средств с использованием информационно-коммуникационных технологий // Юридическая наука. 2021. № 10. С. 91–93.

42. Рясов А. А., Жигалова Г. Г., Аветисян А. Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // Мир науки, культуры, образования. 2018. № 4. С. 72–74.

43. Состояние преступности в России за январь-октябрь 2021 года / Официальный сайт МВД России URL: https://mvd.ru. 2021.

44. Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно–Сибирского института МВД России. 2014. № 1. С. 16–20.

45. Степанова М. А., Царёв Е. В. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий // Вестник БелЮИ МВД России. 2021. № 1. С. 12–16.

46. Темиралиев Т. С., Омаров Е. А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения // Вестник Института законодательства и правовой информации Республики Казахстан. 2019. № 1. С. 93–99.

50

47. Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2015. № 3. С. 127–132.

48. Шапиро Л. Г. Основные направления развития криминалистической методики в условиях цифровизации и глобализации преступности // Вестник СГЮА. 2021. № 6. С. 22–226.

49. Шевко Н. Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки Казанского юридического института МВД России. 2016. № 1. С. 13–16.

50. Яджин Н. В., Егоров В. А. Некоторые особенности получения сведений, содержащихся в базах данных операторов связи, в целях раскрытия и расследования преступлений // Юридическая наука и правоохранительная практика. 2020. № 2. С. 98–106.

III. Эмпирические материалы:

1. Уголовное дело № 00001 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 219 л.

2. Уголовное дело № 00002 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 193 л.

3. Уголовное дело № 00003 // Арх. ОМВД РФ по Мелеузовскому району РБ. Оп. 1. 156 л.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

Л. Н. Назаров