Сальмаер Т. Э.,
студентка 4 курса
Сибирского юридического института МВД России
Иваньков А. В.,
студент 4 курса
Сибирского юридического института МВД России

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОФИЛАКТИКА ХИЩЕНИЙ, ПРЕДУСМОТРЕННЫХ П. «Г» Ч. 3 СТ. 158 УК РФ.

В целях оптимизации уголовно-правового противодействия хищениям, совершаемым с использованием электронных систем расчета, законодателем был введен в действие 4 мая 2018 года такой квалифицирующий признак кражи как тайное хищение с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). До данного события хищение с банковских счетов оценивалось как неквалифицированная кража (при отсутствии иных квалифицирующих признаков данного преступления). Сейчас же это тяжкое преступление. Чем с точки зрения криминологической обусловленности вызвана необходимость установления такого вида хищения в качестве квалифицирующего признака? В пояснительной записке к законопроекту указывается следующее обоснование:

1. Рост числа хищений с использованием систем дистанционного банковского обслуживания, в 2014 году составляло 4 890, а в 2015 году – 32 578, то есть в 6,7 раза больше.

2. Увеличение объема операций с 1639,4 до 5126,5 миллионов рублей.

3. Потерпевшими часто становятся социально незащищенные слои населения (пенсионеры).

4. Невозможность привлечь за приготовление к преступлению.

5. Нарушение банковской тайны [1].

Стоит отметить, что хищения с использованием систем дистанционного банковского обслуживания являются лишь частью несанкционированных переводов денежных средств. Так, за то же 2015 г. ЦБ РФ зафиксировал 304154 несанкционированных транзакции. По данным ЦБ РФ за 2017 г. объем всех несанкционированных операций, совершенных с использованием платежных карт, эмитированных на территории Российской Федерации уменьшился, в 2017 г. составил 961,3 млн руб., а вот количество по сравнению с 2015 г. выросло до –317 178 [2]. Кроме того, хищения с банковского счета снижают доверие населения к банковской системе. Сказанное обуславливает повышенную общественную опасность краж с банковского счета, а равно в отношении электронных денежных средств.

Целесообразно проанализировать термины «банковский счет» и «электронные денежные средства». Так, В.А. Белов предлагает понимать под банковским счетом учетную единицу, применяемую в банковском деле с целью фиксации денежных требований одной стороны (клиента) к другой стороне (банку), возникающих из договора банковского счета, а также для учета банковских операций, предусмотренных для соответствующей категории счетов [3]. Иными словами, банковский счет – это не физическое место, где хранятся деньги, а документ, фиксирующий движение средств.

Говоря о понятии электронных денежных средств, Р.Э. Мирзоян отмечает, что электронные деньги – в широком смысле слова, рассматриваются как совокупность подсистем наличных (эмиссия осуществляется без открытия персональных счетов) и безналичных денег (эмиссия осуществляется с открытием персональных счетов) либо как система денежных расчетов посредством использования электронной техники.

В узком смысле, электронные деньги представляют подсистему наличных денег, выпускаемых в обращение банками или специализированными кредитными институтами. Здесь главное отличие – необязательность использования при платеже банковского счета, когда операция осуществляется от плательщика к получателю без участия банка [4].

По сути, электронные деньги – это деньги, которые существуют в компьютерных системах и доступны для транзакций через электронные системы. Их ценность поддерживается фиатной валютой и их можно обменять на физическую форму, однако использование часто более удобно в электронном виде. Строго говоря, «деньги на банковском счете» – это тоже своего рода «электронные деньги». Развитие систем платежей предусматривает варианты, когда эти самые деньги будут храниться не на банковских счетах, а на цифровых кошельках типа PayPal, WebMoney. При этом, хранятся именно деньги в эквиваленте, равном фиатной валюте. Например, тысяча рублей на PayPal означает, что человек оперирует суммой именно в одну тысячу рублей. С другой стороны активно развиваются криптовалюты.

Криптовалюта является цифровым активом предназначенным для работы в качестве средства обмена, который использует стойкую криптографию для обеспечения финансовых операций, управления созданием дополнительных блоков, и проверки передачи активов. Это своего рода альтернативная валюта, которая использует децентрализованный контроль [5].

Таким образом, не совсем ясно, что имел ввиду законодатель, разграничивая предмет хищения через призму п. «г» ч. 3 ст. 158 УК РФ.

При этом стоит отметить, что кражей будут считаться:

1) хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата;

2) когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети, а равно не создавались поддельные сайты [6].

В иных случаях хищение денежных средств будет считаться мошенничеством. При этом хищения вообще являются самым распространённым видом преступлений. По данным МВД РФ половину всех зарегистрированных преступлений (50,6%) в 2018 г. составляют хищения чужого имущества. Треть всех зарегистрированных преступлений – кражи [7]. К сожалению, в РФ не ведется статистики краж электронных денежных средств. Однако, как следует из отчета Norton только в США за 2017 г. люди потеряли в общей сложности 19,4 миллиарда долларов из-за действий хакеров, а по всему миру потери составили 172 млрд [8]. Учитывая, что в РФ провозглашен курс на увеличение числа электронных денег, можно предположить, что объемы хищений будут увеличиваться.

Если говорить о способах хищения, то их можно разделить на две большие группы:

1. Способы, не требующие особых навыков. Хищение с использованием данных, предоставленных потерпевшим. Пин-код, записанный на карте, легкий пароль от личного кабинета, украденная флешка с биткоинами. Например, в Канске двое подростков взяли у знакомого телефон, вошли с его помощью в «Сбербанка. Онлайн», откуда перевели деньги себе[9].

2. Способы, которые требуют специальной подготовки. Создание фишинговых сайтов, изготовление поддельной карты и т.д.

Рассмотрим более подробно способы из второй группы.

1. Скиминг. Фальшивый считыватель встроен в банкомат, который считывает и сохраняет всю информацию, указанную на магнитной полосе на карте. Эта информация позже используется хакерами для кражи денег.

2. Наложение пэдов. Преступники устанавливают поддельную клавиатуру на фактическую клавиатуру, чтобы украсть PIN-код.

3. Установка скрытых камер возле банкоматов. Эти шпионские камеры стратегически установлены таким образом, чтобы читать PIN-код

карточки. Поскольку они довольно маленькие по размеру, они обычно устанавливаются рядом с клавиатурой.

4. Захват карты. Специальный зажим, удерживает карту, когда человек вставляет ее в машину, карта извлекается позже.

5. Ведение журнала нажатия клавиш. Хакеры заставляют пользователей непреднамеренно загружать программное обеспечение, которое позволяет преступнику отслеживать свои ключевые штрихи и украсть пароли и данные [10].

6. Создание клонов банковских карт. Данные учетной записи копируются на пустые карточки, а затем используются для снятия денег или покупки товаров для продажи.

7. DDoS атака. Банковские грабители могут сбить систему видеонаблюдения и отключить аварийные сигналы, прежде чем они войдут в банк. Электронный эквивалент представляет собой распределенную атаку типа «отказ в обслуживании» (DDoS), в которой большие объемы сетевого трафика забивают системы банка, предоставляя преступникам необходимое им покрытие. В то время как ИТ-персонал банка пытается поднять свои серверы, преступники переходят на учетные записи пользователей» [11].

При этом, преступники часто комбинируют указанные способы. Например, Аверин В.А. осужден за то, что в группе лиц по предварительному сговору с ранее ему знакомыми установленными следствием лицами уголовное дело в отношении которого выделено в отдельное производство, находясь в неустановленном месте г. Тюмени, из корыстной заинтересованности совершил хищение чужого имущества - денежных средств с банковских счетов законных держателей карт, через банкоматы находящиеся на территории г. Тюмени, путем незаконного сбора сведений, составляющих банковскую тайну, неправомерного доступа к охраняемой законом компьютерной информации, на машинном носителе, в электронно-вычислительной машине (ЭВМ), повлекшей копирование информации, используя при этом специальное техническое устройство, заведомо приводящее к несанкционированному копированию информации, последующего нанесения полученной информации на магнитную полосу заготовок пластиковых карт и дальнейшего снятия денежных средств [12]. Как видим, группа использовала два метода – скиминг и создание клонов банковских карт.

Приведем следующий пример: Бонка Д.Ф., в неустановленные следствием время и месте, вступил с неустановленным лицом в предварительный преступный сговор, направленный на тайное хищение денежных средств, путем незаконного получения информации с магнитных полос пластиковых платежных карт. Действуя из корыстной заинтересованности, осуществляя реализацию общего преступного умысла по завладению денежными средствами банков, с целью создания условий для изъятия иму-

щества, он, Бонка Д.Ф., совместно с неустановленным следствием соучастником, в неустановленном следствием месте и время, приискали устройство для получения (перехвата) информации с магнитных полос пластиковых (в том числе платежных) карт, а также устройство для получения (перехвата) информации, вводимой пользователем посредством клавиатуры банкомата, в том числе пин-кодов банковских карт [13]. В данном случае использовалось наложение пэдов и создание клонов банковских карт.

Разумеется, это не все способы, к которым прибегают злоумышленники. Преступники придумывают различные методы, чтобы получить доступ к финансам. Например, в 2013 г. мужчина вошел в филиал Barclays в северном Лондоне и украл 1,3 миллиона фунтов стерлингов дистанционно. Он назвался ИТ-специалистом и установил коммутатор клавиатуры. Они обычно используются в центрах обработки данных для управления несколькими компьютерами с одного терминала, и, подключив его к маршрутизатору 3G, похититель смог удаленно получить доступ к машинам Barclays по сети сотового телефона. Так он перевел деньги на свои собственные счета [14]. Данный способ похож на наложение пэдов и в российском правовом поле был бы квалифицирован именно как кража с банковского счета.

Таким образом, личность преступника будет отличаться в зависимости от способа. В первой группе портрет преступника ничем не будет отличаться от типичного портрета обычного вора. Как показывает статистика, большинство лиц, совершающих хищения – среднестатистический портрет российского преступника – мужчина в возрасте от 30-49 лет, имеющий 9 классов образования, либо среднее профессиональное образование, без постоянного источника дохода [15, 16, с. 42-65]. Если же мы будем рассматривать личность преступника, использующего специальные навыки для хищения средств, то Д. Шиндер выделяет следующие общие признаки «киберпреступника»:

1) определенная степень технических знаний (от «сценаристов», которые используют вредоносный код других до талантливых хакеров);

2) пренебрежение законом или рационализацией в отношении того, почему конкретные законы являются недействительными или не должны применяться к ним;

3) высокая терпимость к риску или потребность в «острых ощущениях»;

4) наслаждается манипулированием, возможностью «перехитрить» других [17].

Какие профилактические меры могут предложить правоохранительные органы для уменьшения числа хищений электронных денежных средств? Федеральный закон от 23 июня 2016 году № 182-ФЗ «Об основах

системы профилактики правонарушений в Российской Федерации» устанавливает два вида профилактики:

1) общая;
2) индивидуальная.

На общем уровне осуществляется устранение причин и условий, способствовавших совершению преступления. Мы не будем подробно останавливаться на общих мерах профилактики хищений вообще, а укажем те меры, которые помогут предотвратить совершение хищений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ.

По большому счету, эффективными мерами будут разъяснения гражданам о простейших мерах безопасности:

1) немедленно позвонить в банк, если банкомат «съел» карту. Если ее не могут извлечь незамедлительно – заблокировать ее;
2) проверять наличие на банкоматах посторонних устройств;
3) не сообщать никому пин-код и пароль;
4) не использовать для пароля свои данные (имя, дату рождения и т.д.);
5) внимательно проверять сайт, на котором осуществляются покупки;
6) устанавливать на компьютеры и сотовые телефоны качественные антивирусы.

Разумеется, данная информация должна быть подана людям в удобном, доступном и ясном виде. Люди, не работающие с компьютером, вряд ли поймут, если им просто сказать про скиминг или наложение пэдов. Кроме того, информация о мерах безопасности часто располагается на сайтах МВД [18]. Однако, вряд ли пользователи карт будут тратить свое время, чтобы зайти на сайт МВД РФ и почитать о мерах предосторожности. На наш взгляд, более эффективным будет распространение этих сведений в популярных группах в соцсетях, в рекламе по телевидению или в рекламе в супермаркетах – там, где люди с большей вероятностью увидят/услышат сообщение.

Индивидуальная профилактика проводится в отношении двух категорий лиц:

1) тех, кто может совершить данное преступление;
2) лиц, которые стали или могут стать жертвами таких посягательств.

К сожалению, приходится констатировать, что действенных индивидуальных мер для первой группы нет. Это обусловлено тем, что нет определенного типажа лиц, совершающих данные преступления – это может быть высокообразованный специалист, ведущий примерный образ жизни и человек без образования и работы укравший банковскую карту с пин-кодом на ней. Единственный вариант воздействия, который можно предложить – публикация в СМИ о случаях, когда преступник был обнаружен

и понес наказание. Риск быть пойманным снизит преступные намерения лица.

Библиографический список:

1.Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)». URL: http://sozd.duma.gov.ru/bill/410960-7.

2.Обзор по несанкционированным переводам денежных средств за 2017 г. // URL: http://www.cbr.ru/statichtml/file/14435/survey_transfers_17.pdf.

3.Белов В.А. Энциклопедия юриста. URL: https://dic.academic.ru/dic.nsf/enc_law/156/%D0%91%D0%90%D0%9D%D0%9A%D0%9E%D0%92%D0%A1%D0%9A%D0%98%D0%99.

4.Мирзоян Р.Э. Финансово-правовая природа электронных денег // Вестник Адыгейского государственного университета. 2013. № 4. С.2

5. URL: https://capital.aliterax.com/ru/.

6.Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 г. Москва «О судебной практике по делам о мошенничестве, присвоении и растрате». URL: https://rg.ru/2017/12/11/sud-moshennichestv-dok.html.

7. Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2018 года. URL: https://xn--b1aew.xn--p1ai/reports/item/14696015/.

8. Fontes B. Hackers stole $172 billion from people in 2017. URL: https://www.technologyreview.com/the-download/610043/hackers-stole-172-billion-from-people-in-2017/.

9. В Канске двое подростков подозреваются в хищении денежных средств с банковской карты своего знакомого.URL: https://vk.com/wall-101909810_4835.

10. Виго М. 15 способов преступников украсть деньги с вашей дебетовой / кредитной карты. URL: https://www.gadgetsnow.com/slideshows/15-ways-criminals-steal-money-from-your-debit/credit-card/15-ways-criminals-steal-money-from-your-debit/credit-card/photolist/55414119.cms.

11. Арон Я. Пять способов ограбить банк, используя Интернет. URL: https://www.newscientist.com/article/dn24324-five-ways-to-rob-a-bank-using-the-internet/.

12. Приговор Ленинского районного суда г. Тюмени от 11.02.2015 г. по делу 1-169/2015.URL: https://bsr.sudrf.ru/bigs/showDocument.html#id=1d2d0eee6b05a05583a91b236b6e30d0&shard

13. Приговор Хорошевского районного суда г. Москвы от 29.07.2014 г. по делу 1-242/2014. URL: https://bsr.sudrf.ru/bigs/showDocument.html#id=880c8dd5b6dbb0c8ed2067f4518920c1&shard.

14. Арон Я. Пять способов ограбить банк, используя Интернет. URL: https://www.newscientist.com/article/dn24324-five-ways-to-rob-a-bank-using-the-internet/.

15. Портал правовой статистики. URL:http://crimestat.ru/.

16. Жукова Ю.В., Мальков С.М., Рудакова Е.Н., Ступина С.А., Тепляшин П.В., Токманцев Д.В., Федорова Е.А.Состояние преступности в Сибирском федеральном округе (2011-2016): аналитический обзор / Красноярск: СибЮИ МВД России, 2017.

17. Shinder D. Profiling and categorizing cybercriminals Profiling and categorizing cybercriminals Deb Shinder. URL: https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/.

18. Министерство внутренних дел Российской Федерации. Азбука безопасности: советы полиции. URL: https://61.мвд.рф/азбука-безопасности-советы-полиции/еженедельная рубрика-азбука-безопасности/item/9102403;
https://краснодар.23.мвд.рф/news/item/8064816/.