Секция «Информационное общество, цифровая экономика и информационная безопасность»

Расследование мошенничества с использованием электронных средств платежа

Научный руководитель – Пушкарев Виктор Викторович

Копылова Александра Павловна

Студент (специалист)

Московский университет Министерства внутренних дел Российской Федерации, Факультет подготовки дознавателей, Москва, Россия

E-mail: kop-sa_2001@mail.ru

Развитие экономики России и внедрение новых информационных технологий в жизнедеятельность граждан позволило расширить площадку использования безналичных расчетов, осуществляемые с помощью электронных банковских карт.

Ежегодная статистика свидетельствует о том, что более половины всех зарегистрированных преступлений (53,5%) составляют хищения чужого имущества, из них более 12,7% составляют мошенничества. С каждым годом количество преступлений, связанных с хищением денежных средств с банковских платежных карт увеличиваются - материальный ущерб от хищений в 2018 году составил 563,1 млрд рублей, в 2019 году - 627,7 млрд рублей. В 2019 году совершенно более 257 тысяч мошенничеств, из них только 1/3 раскрытых. В 2019 году банки выплатили 935 млн руб., лицам, с чьих счетов были списаны денежные средства без их согласия, что составляет лишь 15% средств, которые были похищены со счетов банковских клиентов [1; 2].

Создание новых методов незаконного завладения чужого имущества связано с повешением уровня информатизации населения, расширением электронных форм платежа и появлением обширных торговых площадок в сети Интернет.

Наиболее распространенными способами совершения мошенничества с использованием электронных банковских карт в настоящее время являются:

1. Скимминг (от английского но skim — снимать, просматривать) [4]. Преступники устанавливают возле банкоматов, касс видеокамеры, ставят накладки на клавиатуру банкоматов, чтобы зафиксировать пин-код, а также устройства, которые фиксируют данные с магнитной полосы банковской карты в момент совершения операции с банковской картой. Все используемые устройства маскируются под элементы банкомата. Полученные данные переносят на поддельную пластиковую карту, с которой в дальнейшем снимаются денежные средства.

Так, в г. Белгороде с 29.11-02.12 С. и П. устанавливали на банкомате прямоугольную накладку из полимерного материала с аудиовидеорегистратором и накладку на картоприемник, предназначенная для негласного получения информации с магнитных полос пластиковых карт.

02.12. в 3 часа 50 минут в ходе осмотра места происшествия - вышеуказанного банкомата, сотрудниками полиции, было изъято неизвестное постороннее устройство с банкомата. Согласно показаниям сотрудника службы безопасности за период нахождения скриммингового оборудования на банкомате, им воспользовалось 272 человека, сумма на счетах этих граждан составила 3 млн. рублей. После установления данного факта, все банковские карты были заблокированы, незаконного списания денежных средств не произошло [3].

2. Фишинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — похищение персональных данных держателей карт, пин-кода и/или самой карты.

При фишинге создаются не действительные интернет сайты, при переходе на которые необходимо ввести данные банковской карты, после чего вся необходимая информация попадает к злоумышленникам. Располагая всей необходимой информацией, мошенники получают полный доступ к личному кабинету потерпевшего, по средствам которого могут распоряжаться денежными средствами, находящимися на всех счетах гражданина.

Так, братья Попелыши разработали копию оригинальной веб-страницы дистанционного банковского обслуживания банка «ВТБ» и разместили там телефонные номера, принадлежащие им. После чего используя вирус «Троянский конь», который после активации на зараженном компьютере изменял некоторые параметры, используемые в функционале "банк-клиент". Вследствие чего все обращения клиентов к официальному банковскому сайту перенаправлялись на сайт, который создали хакеры. И уже на нем вводили свои персональные данные - пароли и коды для осуществления денежных операций. Получив идентификационные данные, мошенники от имени клиентов направляли дистанционные распоряжения на перевод средств с их банковских счетов на свои собственные, после чего обналичивали деньги [3].

3. Фарминг, подразумевает установку вирусной программы, которая способствует распространению ложных сообщений, в которых содержится информация о несуществующем событии и для устранения негативных последствий которого, потерпевший должен перевести денежные средства мошенникам.

Так, М. отправлял смс на неизвестные номера с текстом: «Ваша банковская карта заблокирована, информация по телефону: <№»>. После чего, М., созванивался с потенциальными потерпевшими, выдавал себя за сотрудника службы безопасности банка «Сбербанк России», и сообщал им ложную информацию о том, что их банковская карта заблокирована и чтобы её разблокировать необходимо сообщить паспортные данные, номер банковской карты и CVC-код, затем используя полученные данные, получал полный доступ к личному кабинету владельца банковской карты [3].

Проанализировав судебно-следственную практику можно выделить ряд сложностей, которые возникают при расследовании преступления и выявление лиц, совершивших мошенничество с использованием электронных средств платежей:

- невозможность быстрого и своевременного доступа к информации по лицевому счету держателя банковской карты и о движении денежных средств. Для решения данной проблемы необходимо внести изменения в уголовно-процессуальное законодательство, которое регламентирует получение информации сотрудниками полиции и позволило бы им получать необходимые сведения в короткие сроки;

- затягивание предоставления запрашиваемой информации. Для расследования данных преступлений необходимо получение сведений от сторонних организаций, которые в свою очередь могут предоставлять информацию в течение недели, месяца. В связи с этим затягиваются сроки расследования преступлений и возникают ситуации, когда на момент установления необходимая информация уже удалена из базы данных. Необходимо разработать единые требования для сторонних организаций по предоставлению необходимой информации, которая имеет значения для расследования уголовного дела;

- высокая стоимость проведения компьютерных судебных экспертиз и нехватка экспертов, которые способны проводить данные экспертизы, что увеличивает продолжительность проведения экспертизы до 6 месяцев и влияет на загруженность экспертов. Стоимость проведения такой экспертизы во вневедомственных учреждениях составляет от 15 до 300 тыс. руб., что в большинстве случаев больше стоимости причиненного ущерба, который варьируется от 1 до
15 тыс. руб.

Также при расследовании мошенничеств с использованием электронных средств пла-

тежа возникают сложности в установлении места совершения и окончания преступления, сложности в осуществлении качественного исполнения поручений о производстве отдельных следственных действий в других субъектах Российской Федерации и правильное определение потерпевшего от преступления.

Так, например, 10.02.2017 г СЧ СУ УВД по ЦАО ГУ МВД России по г. Москве возбуждено уголовное дело по ч. 4 ст. 159 УК РФ по факту совершения неустановленными лицами из числа руководства и сотрудников офиса АКБ «Ланта-Банка» хищение денежных средств находящихся на счетах граждан Т., К., П., М. и иных лиц, с которыми банком были заключены договора срочного вклада. До ВУД, банком, в целях поддержания деловой репутации и доверия населения были возмещены в полном объеме похищенные средства гражданам указанных в постановлении о ВУД. В связи с тем, что в результате совершенного преступления, в конечном счете, вред понес банк, следователем было принято решение о признании потерпевшим Банка АКБ «Ланта-Банка». Между тем, умысел лиц совершивших хищение, был направлен на хищение денежных средств граждан, которым и был причинен преступлением вред. При таких обстоятельствах признать потерпевшими следовало граждан, и квалифицировать содеянное надлежало по ст. 159.3 УК РФ [3].

Только совокупность предпринятых мер для решения имеющихся трудностей в расследовании мошенничеств с использованием банковских карт, будет влиять на эффективность раскрытия данных преступлений.

Источники и литература

1) Статистика ФинЦЕРТа. [Электронный ресурс]. – URL: https://cbr.ru/statistics.
2) Судебная практика по уголовным делам. [Электронный ресурс]. – URL: https://sudact.ru/practice/sudebnaya-praktika-po-ugolovnym-delam.
3) Официальный сайт МВД России. [Электронный ресурс]. – URL: https://мвд.рф.
4) Пушкарев В.В. Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора: учебное пособие. - М., 2019.

Иллюстрации

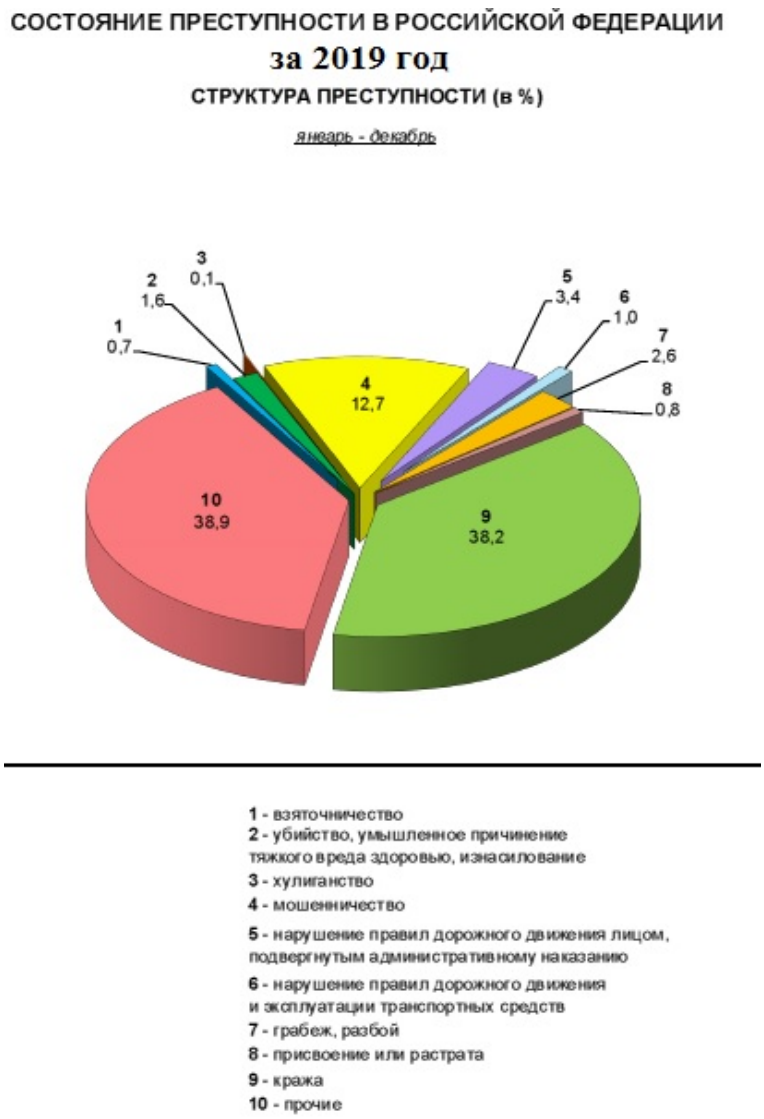

Рис. 1. Статистические данные о состоянии преступности в РФ за 2019 год