УДК 34
ББК 67
DOI **10.53039/2079-4401.2020.1.1.003**

Научная специальность: 12.00.12. Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность
Научный руководитель: Анна Андреевна Лебедева, доцент кафедры криминалистики ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации» кандидат юридических наук, подполковник юстиции

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ. ТЕНДЕНЦИИ И ОСОБЕННОСТИ РАССЛЕДОВАНИЯ

Г.С. Сабельникова *

Аннотация. Расследование преступлений, совершаемых посредством компьютерных технологий, уже не новая задача для правоохранительных органов. С каждым днем количество таких общественно опасных деяний увеличивается, а способы их реализации совершенствуются. Вместе с тем отметим, что сами по себе компьютерные технологии стали составной частью финансового механизма государства, в том числе и его банковского сектора. Личные данные клиентов банка, их денежные средства – потенциальные объекты для посягательства для так называемых киберпреступников. В связи с этим имеется необходимость рассмотрения отдельных аспектов расследования киберпреступлений в банковском секторе.

Ключевые слова: банки, банковская деятельность, киберпреступления, киберпреступность, расследование преступлений

CYBERCRIME IN THE BANKING SECTOR. TRENDS AND FEATURES OF THE INVESTIGATION

G.S. Sabelnikova *

Abstract. Investigation of the crimes committed with use of computer technologies is not new law enforcement agencies. Every day the number of crimes increases, and ways of their commission are improved. However, computer technologies – became an element of the financial mechanism of the state including its banking sector. Personal data of clients of bank, their money are potential objects for encroachment of cybercriminals. In this regard, there is a need of consideration of the separate moments of investigation of cybercrimes for the banking sector.

Keywords: banks, bank activity, cybercrime, cybercrime, investigation of crimes

Киберпреступность – реалии современного информационного мира. Как правило, совершение киберпреступлений направлено на получение материальной выгоды, поэтому объектами посягательства с точки зрения уголовного права является чужое имущество, в том числе денежные средства физических и юридических лиц, которые хранятся на банковских счетах.

Вместе с тем крупные транзакции, банковские счета с денежными накоплениями, персональные данные клиентов банка, а также недостаточно высокая степень защиты от кибератак, невнимательность клиентов способствуют развитию киберпреступности в банковской сфере.

Существует несколько вариантов определения киберпреступности. Согласно установленным рекомендациям ООН киберпреступность – это совершение любого преступления, направленного против конфиденциальности, целостности и доступности компьютерных данных или систем; преступления, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда; преступления, связанные с содержанием компьютерных данных [16].

Вместе с тем следует отметить, что это преступления, которые могут совершаться не только с помощью компьютера, но и мобильного устройства.

В настоящее время практически любое преступление может быть реализовано при помощи компьютера, информационно-телекоммуникационных технологий и сетей.

Так как сфера наших интересов находится в рамках финансового сектора экономики, будем рассматривать исключительно киберпреступления в банковской сфере.

Рассмотрим составы преступлений, предусмотренных Уголовным кодексом Российской Федерации [13] (далее – УК РФ), которые могут быть отнесены к киберпреступлениям в банковской сфере:

• п. «г», ч. 3 ст. 158 УК РФ – кража с банковского счета, а равно в отношении электронных средств;

• ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа;

**** Галина Сергеевна Сабельникова,***
студент 5 курса ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации»

**** Galina S. Sabelnikova,***
Student of the Moscow Academy of the Investigative Committee of the Russian Federation

• ст. 159.6 – мошенничество в сфере компьютерной информации;

• ст. 183 УК РФ – незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;

• ст. 187 УК РФ – неправомерный оборот средств платежей.

К рассматриваемой нами категории также следует отнести и составы преступлений, включенных в главу 28 Уголовного кодекса Российской Федерации, – «Преступления в сфере компьютерной информации» (ст. 272-274.1 УК РФ).

Согласно данным отчета об инцидентах информационной безопасности, при переводе денежных средств за I и II кварталы 2019-2020 гг. от 29 октября 2020, формируемого Банком России на основании документов отчетности, подаваемых кредитными организациями, доля возмещенных средств клиентам от операций, проведенных без их согласия с использованием электронного средства платежа, за 2019 год составила в сумме за оба квартала 47,1 трлн рублей, в 2020 году – 41,9 трлн рублей; объем операций по переводу денежных средств, совершенных без согласия клиентов, в первом квартале 2020 года вырос на 38 % по сравнению с первым кварталом 2019 года, а во втором квартале прирост составил 59 % [11].

Осуществление таких транзакций представляет собой виновно совершенное уголовно наказуемое общественно опасное деяние, квалифицируемое в соответствии с УК РФ. Преступления, связанные с проведением операций без согласия клиентов, совершаются с применением компьютерных технологий, часто совместно с использованием методов социальной инженерии [10].

Вопросы о киберпреступлениях в банковском секторе экономики стоят остро и в других государствах. Согласно исследованию, проведенному на международном уровне и опубликованному в 2019 году компанией «IntSights»1, занимающейся разведкой и выявлением киберугроз, более 25% атак вредоносного программного обеспечения направлено на банки и финансовые организации. По сравнению с 2018 годом количество случаев мошенничества с банковскими картами увеличилось и составляет 212% [15].

Таким образом, киберпреступность в банковской сфере представляет собой проблему не только национального, но и международного уровня.

В настоящее время имеется множество спорных вопросов при расследовании указанной категории преступлений.

Методика расследования преступлений, совершенных с помощью компьютерных технологий, в банковской сфере имеет свои особенности, обусловленные спецификой деятельности по обслуживанию клиентов, использованием специальных технологий, таких как система дистанционного банковского обслуживания, система искусственного интеллекта и др.

Например, в методику расследования входят способы совершения киберпреступлений в банковской сфере, которые будут охватывать типичные способы совершения компьютерных преступлений и способы хищения денежных средств с помощью специального оборудования. Заметим, что совершенствование системы защиты от киберугроз и кибератак в банковских организациях и наращивание опыта правоохранительных органов в расследовании подобных преступлений стимулируют на появление новых путей незаконного завладения денежными средствами преступниками.

Существуют следующие виды киберпреступлений в банковской сфере: преступления в системе дистанционного банковского обслуживания (далее – ДБО), подделка платежных карт, хищение денежных средств из банкомата [6].

Система дистанционного банковского обслуживания представляет собой технологию предоставления банковских услуг на основании распоряжений, передаваемых клиентом без его визита в банк, как правило, с использованием компьютерных или телефонных сетей [1,8].

На сегодняшний день используются следующие виды ДБО: технология «банк-клиент», интернет-банкинг, мобильный банкинг, с использованием внешних сервисов – банкоматов и устройств банковского самообслуживания [12].

В свою очередь, злоумышленники, используя систему ДБО, могут применять следующие способы для достижения преступной цели: использование вредоносных программ скрытого управления;

1 IntSights – платформа для анализа внешних угроз и защиты, созданная для нейтрализации киберугроз за пределами сети.

использование программ считывания пароля; применение программ удаленного доступа; создание так называемого зеркального сайта или сайта-двойника; перечисление денежных средств на электронные кошельки злоумышленникам, кроме того, используются такие схемы, как отправка ложной информации (проблема у родственника) и получение звонков, SMS-сообщений о том, что ваша карта заблокирована [1].

Именно такими способами воспользовались участники хакерской группы во главе с братьями Дмитрием и Евгением Попелышами. В период с марта 2013 по май 2015 года с помощью вредоносных программ «QHost»,«Patched.IB», «rpcss.dll» и др., обеспечивающих процесс хищения, группа осуществляла атаки на систему ДБО системообразующих российских банков, похитив таким образом более 12,5 млн рублей.

Следствием установлено, что осужденные «заражали» компьютеры пользователей вирусом, который перенаправлял клиента на поддельную (зеркальную страницу) банка, отличную от оригинала несколькими символами в адресной строке.

Затем под предлогом смены политики безопасности пользователи вводили данные банковской карты и код подтверждения со скретч-карты банка. Используя эти данные, преступники выводили деньги через настоящий сайт дистанционного банковского обслуживания (ДБО) [2].

В суд направлено 813 эпизодов преступной деятельности братьев Попелышей и их соучастников по признакам преступлений, предусмотренных ч. 2 ст. 273 УК РФ – Создание, использование и распространение вредоносных программ, ч. 3 ст. 272 УК РФ – Неправомерный доступ к компьютерной информации, ч. 4 ст. 159 УК РФ – Мошенничество в сфере компьютерной информации. В июле 2018 года участникам группы вынесен обвинительный приговор.

Совершение киберпреступлений в банковской сфере с использованием поддельных, украденных пластиковых карт включает в себя использование личных данных владельцев карт при помощи установки специальных устройств на банкоматы (например, так называемые «cookie», «скиммеры»), которые позволяют считывать информацию с платежных карт.

Среди мировых тенденций киберугроз в банковском секторе, как отмечает в своем исследовании Banking & Financial Services. Cyber Threat Landscape Report компания Intsights, можно выделить использование троянских программ (Adload, ATRAS, Emotet), а также уязвимостей протокола SS7.

Протокол SS7 (ОКС-7) был разработан еще в 1970-х годах и в настоящее время используется во всем мире для расчета биллинга сотовой связи и отправки текстовых сообщений. Несмотря на повсеместное использование, протокол обладает уязвимостями, которыми позволяют осуществить перехват SMS-сообщений и их перенаправление [7]. Указанным способом воспользовались злоумышленники в 2017 году, перенаправив денежные средства клиентов немецких банков на их собственные счета [17].

В феврале 2019 года жертвами киберпреступников, которые также использовали недостатки протокола SS7, стали клиенты Metro Bank в Великобритании. В связи с тем, что недостатки протокола устранить невозможно, специалисты рекомендовали банкам не использовать авторизацию клиентов через одноразовые SMS-пароли [9].

Не остаются в стороне такие способы, как внедрение вредоносных приложений на коммутатор банкоматов ATM, использование поддельных мобильных приложений, внедрение троянских программ в приложения банков на мобильных устройствах (так называемые «банковские трояны»), DDoS-атаки, инсайдерские лазейки (когда посягательство осуществляет сотрудник банка, обналичивая в итоге денежные средства клиентов), фишинг и фишинговые наборы (пакет программного обеспечения, которое облегчает копирование дизайна сайта и загрузки его на другой веб-сервер в качестве фишингового сайта [15].

Таким образом, денежные средства физических и юридических лиц являются объектами посягательства со стороны преступных лиц и группировок, занимающихся киберпреступлениями. Наблюдается рост статистики: в частности, основываясь на собранных данных за 2018 и 2019 год, следует отметить, что доля фишинговых атак на кредитные организации увеличилась с 21,7% до почти 30% [14], что связано с увеличением использования информационных технологий при совершении бан-

ковских операций, совершенствованием способов совершения киберпреступлений.

Необходимость в усилении борьбы с киберпреступлениями отметил Генеральный прокурор Российской Федерации Игорь Викторович Краснов в своем интервью от 17 июля 2020 года. Генеральный прокурор указал на то, что наблюдается ежегодный рост компьютерных атак, нацеленных на попытки взлома информационных систем государственных органов Российской Федерации, корпораций и банков [5].

Рассмотренные способы совершения киберпреступлений в банковской сфере актуализируют необходимость совершенствования методики расследования киберпреступлений в банковской сфере.

Литература:

1. Алексеров В.И., Колокольчикова О.Н., Василенко Л.В. Раскрытие преступлений в системе дистанционного банковского обслуживания: учебно-практическое пособие. – Домодедово: ВИПК МВД России. 2020. – 99 с.

2. Архив Московского городского суда, постановление об отказе в передаче кассационной жалобы для рассмотрения в судебном заседании суда кассационной инстанции № 4у/9-2730/19.

3. Братья по кибероружию. Хакеры-близнецы Дмитрий и Евгений Попелыши сели в тюрьму со второго раза. [Электронный ресурс]//GroupIB – URL: https://www.group-ib.ru/blog/brothers.

4. Варламова А. О. Английские заимствования в современном французском языке//Научный вестник Международного гуманитарного университет. – 2018-33(2) – С. 22-26.

5. Генпрокурор РФ потребовал усилить борьбу с киберпреступлениями коду [Электронный ресурс]// Медиагруппа «Звезда». – URL: https://tvzvezda.ru/news/vstrane_i_mire/content/20207171247-Q1YKB.html.

6. Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития// Вопросы инновационной экономики - 2016 - №6(1) – С.73-88.

7. Кража денег с банковских счетов путем перехвата кодов в SMS [Электронный ресурс]//Kaspersky Daily– URL: https://www.kaspersky.ru/blog/ss7-hacked/22218/.

8. Лебедева А.А. Хищение денежных средств со счетов платежных карт// Безопасность бизнеса, Юрист - 2018 - № 1 - С. 59-64.

9. Немецкие банки отказываются от поддержки авторизации по одноразовому SMS-коду [Электронный ресурс]//TADVISER. Государство. Бизнес. ИТ. – URL: https://www.tadviser.ru/index.php.

10. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год, [Электронный ресурс]//Банк России - URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf.

11. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. I и II кварталы 2019-2020 годов [Электронный ресурс]// Банк России – URL: https://www.cbr.ru/analytics/ib/review_1q_2q_2020/.

12. Системы дистанционного банковского обслуживания (рынок ДБО России) [Электронный ресурс]// TADVISER. Государство. Бизнес. ИТ. – URL: https://www.tadviser.ru/index.php.

13. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред 31.07.2020) // СПС «Консультант плюс».

14. Финансовые киберугрозы в 2019 году коду [Электронный ресурс]// Kaspersky Securelist. – URL: https://securelist.ru/financial-cyberthreats-in-2019/95792/.

15. Banking & Financial Services. Cyber Threat Landscape Report/ Intsights 2019.

16. Comprehensive Study on Cybercrime/ United Nation Office on Drugs and Crime (UNDOC), 2013, pp 6-11.

17. Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer [Электронный ресурс]// Süddeutsce Zeitung – URL: https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504.

18. What is the Origin of the Word «Cyber»? [Электронный ресурс]//Alpine securyty - URL: https://alpinesecurity.com/blog/what-is-the-origin-of-the-word-cyber.