СОВРЕМЕННЫЕ ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ БАНКОВСКИХ ДАННЫХ

MODERN PROBLEMS OF CRIMINAL LAW PROTECTION OF BANK DATA

УДК 343.7

Ефимова Екатерина Александровна, магистрант, Владимирский юридический институт ФСИН России, г. Владимир

Семенов Сергей Александрович, доцент кафедры публично - правовых дисциплин, Владимирский юридический институт ФСИН России, г. Владимир

Semenov S.S. kurlak09@rambler.ru

Efimova E.A. eaefimova@yandex.ru

Аннотация. В статье рассматриваются вопросы, связанные современными проблемами уголовно-правовой охраны банковский данных, приведены статистических данные. Итогом проведенного исследования стало утверждение направлений по борьбе с посягательствами на банковские данные.

Annotation. The article deals with issues related to modern problems of criminal law protection of personal data, provides statistical data. The result of the study was the approval of directions for combating encroachments on bank data.

Ключевые слова: банковская тайна, персональные данные, кредитные организации, уголовная охрана банковских данных, мошенничество, электронные системы оплаты.

Keywords: bank secrecy, personal data, credit organizations, criminal protection of bank data, fraud, electronic payment systems.

В настоящее время банки стали уделять повышенное внимание защите оборудования, которое в свою очередь обеспечивает операции по банковским картам. Например, появляются соответствующие банковские автоматы, где имеются различные системы защиты персональных данных владельца карты, во избежание того, что ими могут воспользоваться злоумышленники. Также следует констатировать то что, когда владельцу банковской карты приходит одноразовый пароль для подтверждения соответствующей операции, это свидетельствует о том, что принимаются соответствующие меры защиты со стороны банков.

Однако, все вышеперечисленные меры и способы осуществления банковских операций, онлайн транзакций не обеспечивают необходимой защиты от хищений с банковских карт и иных платежных документов, так по данным компаний «Информзащита»: «число интернет краж с банковских карт на 2020 год составило 300 тыс., а объем ущерба 1,05 млрд. рублей, годом ранее преступники скомпрометировали 267 тыс. банковских карт, общий ущерб составил 1,08 млрд. рублей [3].«Хищения с помощью онлайн приложений и через Интернет составляют 90% всех хищений с банковских карт, второе место занимают скимминги, оффлайн хищения, хищения из банкоматов, подделка пластиковых банковских карт»[1]. Рост хищений денежных средств граждан с банковских карт определяет низкую оценку эффективности работы российской банковской системы. «По данным ассоциации European ATM SecurityTeam (EAST), Россия входит в число стран, чья банкоматная сеть используется для снятия наличных с карт путем утечки данных» [2].

В рамках рассмотрения социальной обусловленности борьбы с хищениями с банковского счета, а также в отношении электронных банковских карт, также целесообразно рассмотреть актуальные проблемы борьбы с такими преступлениями в целом.

Итак, Федеральный закон РФ от 23 апреля 2018 г. N 111 -ФЗ внес существенные изменения, а именно: части 3 ст. 158 и ст. 159.6 УК РФ были дополнены новым квалифицирующим признаком совершения хищения с

банковского счета, в том числе в отношении электронных денежных средств. В результате введения в части 3 ст. 158 и ст.159.6 УК РФ указанного квалифицирующего признака тайное хищение безналичных денежных средств, стало считаться тяжким преступлением во всех случаях, даже тогда, когда размер похищенного не превышает 2 500 руб. В числе основных характерных признаков такого преступления можно назвать следующие:

1) повышенная степень общественной опасности;

2) преступление международного характера;

3) обладает транснациональным характер;

4) связано с посягательством на право собственности человека;

5) наводит страх и ужас обществу;

6) вносит беспорядки и смуту;

7) вносит угрозу стабильности в мире;

8) нуждается в повышенном внимании со стороны всех государств мирового сообщества.

Соответственно, поскольку хищения с банковского счета и в отношении электронных банковских систем посягают на право собственности граждан, российским уголовным законодательством введены и действуют меры уголовной ответственности за указанные преступления.

Анализ материалов уголовных дел, связанных с хищением денежных средств со счетов банковских карт посредством хищения, показал, что преступность такого рода процветает и набирает серьезные обороты.

Говоря о проблемах правового регулирования денежных средств как предмета хищения, важно обратить внимание на следующие аспекты.

Денежные средства для того, чтобы они стали объектом уголовно-правовой охраны, должны находиться в чужой собственности, быть не досягаемы для неопределенного круга лица. Есть некоторые разночтения среди авторов в доктрине касаемо того, какую правовую природу приобретают денежные средства после зачисления их на расчетный счет клиента в банке.

В связи с развитием информационных технологий, а также внедрением

современной рыночной экономики, ориентированной на компьютеризацию, финансовый рынок в настоящее время становится востребованным и быстрорастущим. В частности, данное явление обусловлено развитием банковской системы, расширением спектра представляемых кредитными организациями услуг. По данным Федеральной службы государственной статистики, рынок безналичного ритейла составил: «в 2018 году - 1,0356 триллиона рублей; в 2019 году - 1,172 триллиона рублей; за 2020 год - при приросте от 13-19 % составит 1,32-1,39 триллионов рублей [5].

Что касается дифференцированной уголовной ответственности за хищения с банковских счетов, необходимо отметить в настоящее время значительное число граждан используют различные приложения на своих мобильных устройствах.

Соответственно, приложение обеспечено доступом к банковскому счету гражданина. Основная часть покупок происходит при помощи приложений на телефонах и иных современных гаджетах.

Кредитные организации в целях упрощения пользования их услугами предоставляют клиенту доступ к соответствующему приложению, где клиент может оперативно осуществлять все операции без посещения банков. Безусловно, это является значительным плюсом для клиентов.

Во-первых, экономия времени клиента, что, несомненно, весомый аргумент. Гражданин не стоит в очереди в банке, не тратит время на дорогу, очереди и так далее.

Во-вторых, это несомненный плюс для кредитных организаций. Можно путем уменьшения издержек на содержание штата работников банковского сектора, усилить финансовые вложения в разработку новых приложений для клиентов для того, чтобы максимально пользоваться всеми банковскими продуктами. Тем самым происходит финансовая активность клиентов.

Также важно сказать о том, что в последние годы возрос спрос у граждан применять бесконтактную оплату.

Известны следующие технологии бесконтактной оплаты:

1. Apple Pay;
2. Samsung Pay;
3. Pay Pal.

Именно посредством мобильных приложений происходит бесконтактная оплата. Мобильный телефон становится средством для того, чтобы осуществить бесконтактную оплату.

Однако введение законодателем новых уголовных норм не решает проблему утечки персональных данных клиентов кредитных организаций, которые в последующем могут быть использованы для хищения и мошеннических действий.

По данным экспертно-аналитического центра ГК InfoWatch, за 2020 год в мире обнаружено 202 утечки конфиденциальной информации из банков, финансовых и страховых компаний, что повлекло компрометацию 486 млн. записей персональных данных и платежной информации.

В России число утечек в финансовом сегменте выросло на 36,5% - с 52 до 71 и привело к утечкам 13,4 млн. записей пользовательских данных, сообщили в InfoWatch 29 января 2021 года.

По сравнению с 2019 годом количество утечек, появившихся в открытом доступе, снизилось на 7,3% в глобальном масштабе. В исследовании отмечается, что такое снижение, вероятнее всего связано с влиянием пандемии, поэтому публичные сообщения об утечках «ушли» в серую зону и остались незамеченными.

По данным отчета, процент утечек данных, произошедших по вине сотрудников пострадавших предприятий, в России значительно выше, чем по миру в целом – 82% в России против 51% в мире. Думается, что этот показатель не говорит об отличиях России в сфере защиты данных, а лишь о толковании утечки. Дело в том, что во многих западных странах (США, Великобритания, Канаде и др.) закон предусматривает обязательную публикацию факта утечки данных со стороны самой компании, допустившей утечку. Естественно, компании хотели бы представить это так, что в утечке виновны не они, а некие

«сторонние хакеры» [4]. Тогда как в России такого требования нет. При этом на практике найти виновных в такой утечке персональных данных из кредитной организации, как правило, не представляется возможным.

При этом, считаем, что необходимо принимать жесткие правовые меры защиты банковских данных.

Следует сформировать основные направления борьбы с исследуемой преступностью, а именно:

1. необходимо совершать профилактическую деятельность, направленную на предупреждение совершения данных преступлений. Проводить комплексное изучение причин и условий, которые стали толчком для совершения того или иного преступления данной направленности.

2. непосредственная борьба с преступлениями данной категории. Здесь в числе основополагающих задач: выявлять, предупреждать, пресекать, раскрывать и расследовать такого рода преступные действия;

3. минимизировать и (или) ликвидировать последствия каких-либо проявлений такой преступной деятельности, а также другие направления.

Так же необходимо на законодательном уровне предусмотреть уголовную и административную ответственность субъектов, которые проявили халатность в своей профессиональной деятельности, в результате чего произошла утечка банковских данных. При этом квалифицировать тяжесть правонарушения необходимо от установленного размера ущерба.

Литература

1. Архипов А.В. Проблемы применения норм УК РФ, устанавливающих ответственность за хищение денежных средств с банковского счета // Российская юстиция. - 2020. -N 4. - С. 18 - 20.
2. Крашенинников С.В., Куприянов Е.И. Особенности рассмотрения сообщения о преступлении по факту хищения денежных средств со счетов банковских карт посредством использования электронных платежных систем // Российский следователь. - 2017. - N 18. - С. 33 - 35.
3. Состояние преступности [стат. данные] // Официальный сайт МВД РФ.

URL:http://мвд.рф/reports/item/1609734/ (дата обращения: 17.03.2021)

4. Утечки данных из банков России // [Электронный ресурс]https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России (дата обращения 10.04.2021)
5. Цифровая грамотность россиян: исследование 2020 - НАФИ [Электронный ресурс]. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (дата обращения: 11.04.2021).

Literature

1. Arkhipov A.V. Problems of applying the norms of the Criminal Code of the Russian Federation establishing responsibility for the theft of funds from a bank account // Russian justice. - 2020. - N 4. - p. 18-20.
2. Krasheninnikov S. V., Kupriyanov E. I. Features of consideration of a report on a crime on the fact of embezzlement of funds from bank card accounts through the use of electronic payment systems // A Russian investigator. - 2017. - N 18. - P. 33-35.
3. The state of crime [statistical data] / / Official website of the Ministry of Internal Affairs of the Russian Federation. URL:http://мвд.рф/reports/item/1609734/ (accessed 17.03.2021)
4. Data leaks from Russian banks / / [Electronic resource]http://www.tadviser.ru/index.php/Статья:Leaked_date_iz_banks_Russia (accessed 10.04.2021)
5. Digital literacy of Russians: research 2020 - NAFI [Electronic resource]. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (accessed 11.04.2021).