ПОТЕРИ БАНКОВ ОТ КИБЕРПРЕСТУПНОСТИ

BANK LOSSES FROM CYBERCRIME

УДК 33

Приходько Алла Андреевна, студент, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации, г. Москва
Керопян Гоар Багратовна, студент, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации, г. Москва

Prikhodko A.A. alla28022001@mail.ru
Keropyan G.B. alla28022001@mail.ru

Аннотация

В рамках данной статьи был проведен анализ воздействия киберпреступности на банковскую сферу. Банковская сфера была рассмотрена с точки зрения уязвимости к кибератакам, особое влияние было уделено потерям клиентов банков, а также реакцией банка на эти потери. Показано, что сегодня банковская сфера остается уязвимой для киберпреступности, а все большее значение принимает метод социальной инженерии.

Annotation

This article analyzed the impact of cybercrime on the banking sector. The banking sector was examined in terms of vulnerability to cyberattacks, with a particular impact on the losses of bank customers and the bank's response to these losses. It is shown that today the banking sector remains vulnerable to cybercrime, and the method of social engineering is becoming increasingly important.

Ключевые слова: киберпреступность, банки, банковская сфера, социальный инжиниринг, кибербезопасность.

Keywords: cybercrime, banks, banking, social engineering, cybersecurity.

Введение

Сейчас мы живем в эпохе ИТ сообщества, в котором компьютеры и ИТ системы охватывают практически все основные сферы жизни современного человека и государства. Однако человечество, поставившее на службу ИТ и глобальные компьютерные сети, не предвидело возможности злоупотребления информационными технологиями. Сегодня люди, а также целые государства могут стать жертвами киберпреступников, действующих в ИТ пространстве. В этом случае безопасность тысяч пользователей может зависеть от множества злоумышленников. Величина преступлений, которые совершаются в киберпространстве, увеличивается прямо пропорционально количеству пользователей Интернета и, как оценивает Интерпол, росту преступности в целом. Киберпреступность - одна из глобальных угроз как для всего мирового сообщества, так и для России в частности, поэтому ее исследование сегодня особенно актуально. Цель работы заключается в анализе влияния киберпреступности на деятельность банковской сферы.

Потери банков от киберпреступности

Киберпреступность — это результат глобализации информационных и ИТ технологий и появления международных ИТ и компьютерных сетей. В результате киберпреступность растет быстрее, чем любой другой вид преступности. Например, киберпреступность в России за последние 7 лет выросла в 20 раз. [3]

Количество киберпреступлений увеличивается прямо пропорционально количеству пользователей Интернет сетей, и Интерпол считает, что темпы роста преступности в глобальном Интернете являются самыми высокими на планете. В результате государства прибегают к различным методам борьбы,

как, например, привлечение хакеров для борьбы с киберугрозами, в том числе и в банковской сфере.

В 2013 году, например, в Японии была предпринята успешная попытка привлечения «этичных» хакеров к борьбе с киберпреступностью в банковской сфере. Кроме того, полиция Японии начала связываться с образовательными учреждениями и ИТ-компаниями, чтобы заставить экспертов по киберпреступности работать вместе. Со своей стороны, Министерство обороны Японии объявило, что для создания новых способов киберзащиты оно начало собирать и анализировать информацию о компьютерных вирусах, что, в свою очередь, связано с установлением взаимодействия с непосредственными разработчиками вирусов [1].

Соединенные Штаты продолжают активную борьбу с киберпреступностью. Это основано на исследовании Zecurion Analytics, по отчетам которого финансирование этой области в США составляет около 7 миллиардов долларов США в год, а количество хакеров, работающих с государством, составляет около 9000 человек [1].

С января по август 2020 года количество краж банковских счетов составило 107,2 тысячи, что вдвое больше, чем за аналогичный период 2019 года. Об этом сообщили 14 октября 2020 года. По данным прокуратуры, подобные инциденты регистрировались в два и более раза у 35% испытуемых.

Они отмечают, что каждый пятый факт хищения в России связан с хищением денег со счетов граждан. За восемь месяцев 2020 года количество мошенничества, совершенного с использованием электронных платежных методов, увеличилось вдвое.

Всего зарегистрировано 20,8 тысячи таких преступлений, рост которых в разной степени наблюдается в 90% регионов. В абсолютном выражении их больше всего в Саратовской (2,2 тысячи) и Омской (1,7 тысячи) областях, говорится в отчете. В записях генерального прокурора не указано, сколько денег было украдено мошенниками.

Центробанк объявил о росте активности хакерских групп в 2020 году. Однако эффективность атак на банки по сравнению с 2019 годом не увеличилась. Они не ответили на вопрос об общем ущербе, который мошенники наносят клиентам банков и других финансовых сервисов. [4]

ЦБ сообщил, что в 2019 году мошенники похитили 6,4 млрд рублей у клиентов российских банков, а «средний чек» при хищении средств у граждан составил 10 000 рублей, сообщает FinCERT. В исследовании говорится, что большинство транзакций осуществляются без ведома клиента – некие физические лица совершают транзакции для оплаты в Интернете (транзакции CNP).

Однако, в 2019 году банками было возмещено только 15% украденных средств в пользу пострадавших – около 1 млрд. рублей. При этом Интернет-банки и мобильные приложения были взломаны около 160,8 тыс. раз, при этом общий ущерб составил 2,27 млрд руб., при этом 877 случаев в год связаны с похищением людей сотрудниками банка.

69% транзакций, осуществленных без согласия клиента, были выполнены с использованием методов социальной инженерии - из-за запроса клиента на проведение транзакции или с помощью недобросовестного злоупотребления доверием. Год назад доля этих операций достигла 97%.

Наибольшая доля в рамках социальной инженерии (88%) была зафиксирована в онлайн-банкинге: там клиенты утратили около 2,22 млрд рублей (в среднем 14 000 рублей за транзакцию), при это они смогли вернуть только каждый 14-й украденный рубль. Меньше всего подвергались атакам мошенников при использовании банкоматов и терминалов граждане - 40 000 случаев на сумму 525 млн рублей (сумма составила в среднем 13 000 рублей за транзакцию). При этом среди них только четверть времени держателей карт раскрывали конфиденциальную информацию самостоятельно, поэтому сумма, которая была возмещена банков составляет около 10%.

Учитывая высокую долю социальной инженерии в общем объеме транзакций, которые были совершены без согласия клиентов, банк России был

вынужден рассмотреть возможность изменения порядка возврата части или полной суммы похищенных средств согласно обзору FinCERT. [4]

Интернет-банкинг продолжает оставаться одним из ведущих способов заработка от киберпреступности. Банковские учреждения являются привлекательным местом для быстрого обогащения независимо от времени и технического прогресса. С одной стороны, электронные технологии снизили стоимость предоставляемых услуг; а если смотреть с иной стороны, то расширение использования этих технологий заметно увеличило различные возможности киберпреступников по осуществлению незаконных (мошеннических) операций.

Преступники обогащаются с помощью кибервымогательства, вымогательства и снятия средств с банковских счетов клиентов банков. Незаконный прием реквизитов личных данных клиентов банковской карты осуществляется злоумышленниками, когда держатель средств осуществляет разного рода финансовые операции посредством электронного банкинга с SIM-карт с мобильных телефонов.

Удаленный банкинг требует комплексной защиты от вирусных атак, а также фишинга и троянов, чтобы предотвратить конфискацию конфиденциальной информации и кражу паролей. Сегодня серьезному распространению киберпреступности в банковском секторе способствует использование банками устаревшего программного обеспечения и технологий, которым преступники не могут противостоять. Сложная экономическая ситуация в стране не побуждает банки вкладывать значительные средства в замену оборудования и установку современного качественного программного обеспечения. Банки вынуждены взвешивать риск и стоимость мер по повышению экономической безопасности.

В свою очередь, у производителей программного обеспечения нет юридического механизма ответственности перед своими клиентами. В некоторых случаях предлагаемые программные продукты имеют низкий

уровень устойчивости к хакерским атакам и не соответствуют требованиям безопасности.

Литература

1. Гундерич Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. №4 (15). [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti (дата обращения: 18.10.2020).
2. Лакомов А. С. Киберпреступность: современные тенденции // Академическая мысль. 2019. №2 (7). [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/kiberprestupnost-sovremennye-tendentsii (дата обращения: 18.10.2020).
3. Уровень киберпреступности в России вырос в 20 раз за последние 7 лет [Электронный ресурс] // URL: https://www.gazeta.ru/tech/ (дата обращения: 18.10.2020).
4. Потери банков от киберпреступности [Электронный ресурс] // URL: https://www.tadviser.ru/ (дата обращения: 18.10.2020).

Literature

1. Gunderich G.A. The state of cybercrime // Scientific Bulletin of Crimea. 2018. No. 4 (15). [Electronic resource] // URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti (date accessed: 18.10.2020).
2. Lakomov A.S. Cybercrime: modern trends // Academic thought. 2019. No. 2 (7). [Electronic resource] // URL: https://cyberleninka.ru/article/n/kiberprestupnost-sovremennye-tendentsii (date of access: 18.10.2020).
3. The level of cybercrime in Russia has grown 20 times over the past 7 years [Electronic resource] // URL: https://www.gazeta.ru/tech/ (date accessed: 18.10.2020).

4. Losses of banks from cybercrime [Electronic resource] // URL: https://www.tadviser.ru/ (date accessed: 18.10.2020).