УДК 336.7

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ[1]

Яшанова А.С.
студент
Финансовый университет при Правительстве Российской Федерации
Москва, Россия

Аннотация

В данной статье рассматриваются актуальные вопросы, связанные с обеспечением информационной безопасности банковских систем. Рассмотрены основные угрозы, с которыми сталкиваются банки, способы распространения вредоносных программ, а также выявлены методы защиты. Особое внимание уделяется важности постоянного мониторинга и анализу уязвимостей банковских систем для обеспечения их безопасности.

Ключевые слова: информационная безопасность, безопасность данных, защита информации, банковская система.

ENSURING INFORMATION SECURITY OF BANKING SYSTEMS

Yashanova A.S.
student
Financial University under the Government of the Russian Federation
Moscow, Russia

Abstract

This article discusses topical issues related to the information security of banking systems. The main threats faced by banks, the ways of malware distribution are

[1] Научный руководитель: к.э.н., доцент Александрова Л.С., доцент Департамента банковского дела и монетарного регулирования Финансового факультета Финансового университета при Правительстве РФ

considered, as well as protection methods are identified. Particular attention is paid to the importance of continuous monitoring and analysis of vulnerabilities of banking systems to ensure their security.

Keywords: information security, data security, information protection, banking system.

Современные российские банки собирают большое количество информации о клиентах. Это личные и паспортные данные, сведения о доходах и расходах, имущественном положении, наличии судимостей, долгов и активов. Данные сведения необходимы банку при анализе платежеспособности клиента, определении процентной ставки по ипотеке, оценки эффективности конкретного финансового продукта.

Однако эта информация представляет особую ценность и для мошенников, недобросовестных сотрудников, торгующих данными клиентов. Из-за нарушений безопасности могут произойти большие финансовые потери банка и утечка информации и в дальнейшем негативно отразится на клиентском доверии и репутации банка. В эпоху технологического прогресса, банкам нужно постоянно совершенствовать меры безопасности и следить за последними измерениями в области информационных технологий. Ведь в базах хранится и обрабатывается немалое количество важной информации. Для киберпреступников украсть эту информацию - главная цель. Поэтому тема безопасного обеспечения банковских систем сейчас весьма актуальна.

По данным обзора отчетности Центрального Банка РФ «Об инцидентах информационной безопасности при переводе денежных средств» за первый квартал 2023 года [2] мошенники, заполучившие персональные данные клиентов, смогли перевести без их согласия около 4,5 млрд рублей. Чаще всего преступления совершались с помощью онлайн-банкинга. Отчасти виной была низкая цифровая грамотность клиентов, так как они сами сообщили

мошенникам недостающую информацию. Однако не менее редки случаи утечки информации из-за недобросовестных действий сотрудников самого банка, либо же взлома базы данных.

Частота покушений на финансовые организации по итогам 2022 года снизилась на 16% в сравнении с 2021 годом. За последние несколько лет кибератаки на финансовую отрасль идут на спад и от числа всех кибернападений на организации сейчас составляет примерно 5%. Сетевые границы финансовых организаций лучше защищены, поэтому чаще всего мошенники используют методы социальной инженерии. Этот показатель достигает 47%.

Количество вредоносных программ, используемых в атаках:

- основную часть составляют загрузчики: в 59% атак используется ВПО
- шпионские программы: 18%
- криптографы: 18%
- банковские трояны: 12%

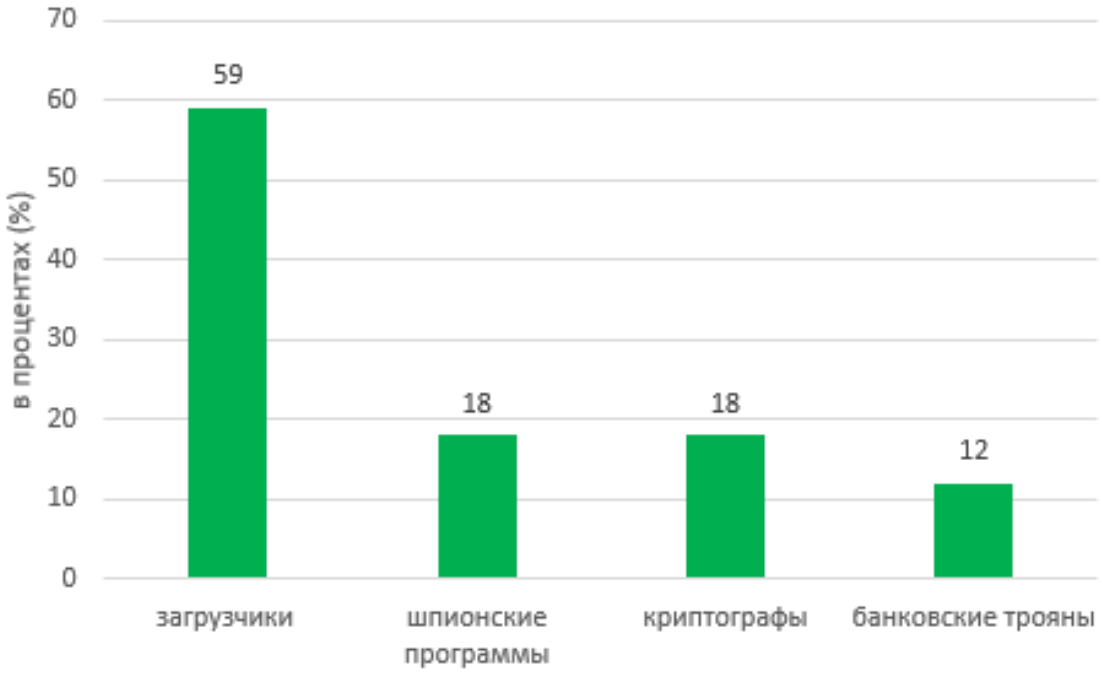

Рисунок 1. Количество вредоносных программ, используемых в атаках. Источник: составлено автором по данным [1]

Большая часть случаев распространения вредоносных программ осуществляется путем рассылки на электронную почту и составляет 56%.

В 2022 году, по сравнению с аналогичным периодом 2021 года, общий объем продаж доступа к банковским корпоративным сетям удвоился. В настоящее время плата за доступ колеблется от 250 до 30 000 долларов, цена зависит от организации и сетевых привилегий, полученных покупателем. Помимо этого, происходит поиск сотрудников банка, которые будут готовы передать мошенникам доступ к системе и конфиденциальной информации.

Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [6] является основным документом, регламентирующим требования к обеспечению информационной безопасности Российского банка. Он основывается на международных актах, ратифицированных в России, и нормах национального законодательства. Так, согласно данному стандарту, системы обеспечения информационной безопасности банка должна состоять из следующих этапов:

1. Разработки политики информационной безопасности. Каждый банк должен, основываясь на требованиях Центрального банка, разработать свои документы и стандарты, определяющие политику информационной безопасности. Помимо минимальных установленных законом предписаний можно разработать дополнительные меры.

2. Определение области действия системы обеспечения информационной безопасности. Банк определяет объекты охраны: систему базы данных, перечень охраняемых сведений, конкретные программы и сервисы для их обработки. По итогу данного этапа составляются документы и инструкции по защите данных объектов.

3. Обработка и оценка рисков информационной безопасности. Любой банк заинтересован в максимальной защите информации при минимальных затратах. Поэтому на данном этапе производится оценка рисков и

определяются наиболее проблемные задачи, на которые надо будет затратить наибольшее количество ресурсов.

4. Управление информационной безопасностью: комплекс мероприятий и институтов по поддержанию обеспечения системы информационной безопасности.

5. Контроль достижения целей системы информационной безопасности. На этом этапе вырабатываются критерии эффективности политики информационной безопасности. Их сравнивают с текущими результатами. Прогнозируется и определяется дальнейший вектор развития банка в этом направлении.

В настоящее время наиболее частными проблемами являются [4]:

- Совершенствование технологий и методов хакерских атак. Мошенники, как правило, в ответ на принятые банками меры обеспечения информационной безопасности придумывают способ их обойти.

- Сложность, комплексность и противоречивость норм национального и международного законодательства в сфере обеспечения информационной безопасности банков. Сейчас, в условиях санкций, российским банкам стало сложнее взаимодействовать с международным сообществом. Международным организациям практически невозможно дать оценку соблюдения российскими банками норм международного законодательства. Проблему усугубляет усложнившийся порядок обмена информацией между российскими и зарубежными банками. Стало сложнее получать информацию о преступлениях в банковской сфере.

- Утечки банковской тайны и сложности с наймом надежных сотрудников. В настоящее время нет ни одной системы найма сотрудников, позволяющей вычислить потенциального мошенника, человека, готового продать данные клиентов. Отсутствие уголовной и административной ответственности, опыт работы в банке и хорошая профессиональная характеристика не дают гарантий, что человек будет работать добросовестно.

Для этого в банках новому сотруднику редко сразу предоставляют доступ к важной внутренней информации. С момента найма на работу до доступа к информационной базе может пройти от нескольких недель до месяцев [3]. За это время руководство должно оценить, можно ли доверять сотруднику более ответственную работу. Но даже это не может быть надежной гарантией защиты от его недобросовестных действий, подкупа со стороны конкурентов.

- Сложность автоматизированной банковской системы, проблемы управления доступа к информации. На практике сотруднику банка часто приходится обращаться за помощью к техническому специалисту. Поэтому нужно принимать меры, чтобы внештатные сотрудники, технические работники и специалисты не имели доступа к охраняемым сведениям.

- Взаимодействие с интернетом и нейросетями. Современные технологии умного машинного обучения могут предоставить клиентам больше возможности: быстро проанализировать кредитную историю, предложить наиболее подходящий банковский продукт, указать на необходимость получения конкретных документов. При этом механизм их развития во многом не предсказуем и опасен. Искусственный интеллект должен быть прозрачен и развиваться только под четким контролем. Председатель Верховного суда России Вячеслав Лебедев допускает применения искусственного интеллекта для взыскания долгов по кредитам. Но для этого нужно обеспечить систему контроля и надзора за ним, разработать нормативно-правовое регулирование искусственного интеллекта в банковской сфере.

- Необходимость пересмотра нормативно-правового регулирования системы обеспечения информационной безопасности. Многие юристы отмечают, что Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» морально и технологически устарел. Технологии развиваются быстрее, чем контрольно-надзорные органы разрабатывают инструкции по их правомерному использованию.

Рисунок 2. Тенденции и главные события на рынке утечек ПДн, 2019-2022 гг [5]

Одной из нарастающих угроз является изменение операционной среды. Высокие скорости обмена информацией, развитие облачных сервисов, социальных сетей, искусственного интеллекта позволяют преступникам действовать быстрее, более непредсказуемо и незаметно. Расследование преступлений по раскрытию банковской тайны занимает много времени. Даже в случае успешного нахождения преступника по цифровому следу он успевает скрыться.

Это, в свою очередь, ведет к формированию квалифицированной среды хакеров - киберпреступников. Экосистема киберпреступности сплачивает непойманных мошенников и ведет к рецидиву преступлений. Поскольку многие из них можно сделать без личного участия, преступная группировка приобретает международный характер.

Современная система обеспечения информационной безопасности банков развивается, однако не успевает за научно - техническим прогрессов. Нейросети, новые способы мошенничества распространяются быстрее, чем банки разрабатывают меры реагирования. Государство, а тем более Центральный Банк, действуют еще медленнее. В результате страдают как сами банки, так и клиенты.

Главный документ по обеспечению информационной безопасности, Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» не отвечает требованиям современного банкинга. Он морально и технологически устарел. Следует пересматривать порядок и способы регулирования минимальных стандартов безопасности.

Для нормального функционирования банковской системы России ей нужно наладить взаимодействие с международными организациями и зарубежными банками. В настоящее время процесс обмена информацией между российскими и зарубежными банками усложнился, что привело к росту международной банковской преступности. Также нужно позволить российским банкам сотрудничать с международными организациями в сфере разработки норм, регулирующих информационную безопасность.

Помимо прямых финансовых потерь от утечки информации, взлома и мошенничества следует учитывать репутационные риски. По данным NPS-2023 [7], 18% клиентов не доверяют своему основному банку. Поэтому потери от ненадежной системы обеспечения информационной безопасности не ограничены прямыми финансовыми убытками.

Библиографический список:

1. Интерфакс: Доля кибератак на финотрасль в 2022 г. [Электронный ресурс]. – Режим доступа – URL: https://www.interfax.ru/digital/871910 (Дата обращения: 26.10.2023)

2. Официальный сайт Банка России [Электронный ресурс]. – Режим доступа – URL: https://cbr.ru/statistics/ib/review_1q_2023/ (Дата обращения: 26.10.2023)

3. Малофеев С.Н. Проблемы защиты информации в банковской сфере // Инновации и инвестиции. 2019. №12. URL:

https://cyberleninka.ru/article/n/problemy-zaschity-informatsii-v-bankovskoy-sfere (Дата обращения: 26.10.2023)

4. Полетаева К.А. Обеспечение информационной безопасности банковской системы // Скиф. 2018. №4 (20). [Электронный ресурс]. – Режим доступа – URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-bankovskoy-sistemy (Дата обращения: 26.10.2023)

5. Сбербанк. [Электронный ресурс]. – Режим доступа – URL: https://www.sberbank.ru/ru/person/kibrary/investigations/utechki-personalnykh-dannykh (Дата обращения: 27.10.2023)

6. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399)

7. NPS-2023. Лояльность пользователей розничных банковских услуг. [Электронный ресурс]. – Режим доступа – URL: https://nafi.ru/projects/finansy/nps-2023-loyalnost-polzovateley-roznichnykh-bankovskikh-uslug/ (Дата обращения: 27.10.2023)

Оригинальность 88%