ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕСОПАСНОСТИ БАНКОВ

А.Н. Юрцев, *студент*
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-4-4-142-145

Аннотация. *Наибольший интерес для киберпреступников представляет банковский сектор. Проблема развития киберпреступности является актуальной вследствие масштабов потерь, которые несут как сами кредитные учреждения по всему миру, так и клиенты банков. В статье показаны наиболее опасные направления кибератак – на саму платежную систему, на процессинговые центры и системы дистанционного банковского обслуживания клиентов, описаны методы, используемые киберпреступниками в достижении своих замыслов. Большое внимание уделено необходимости комплексного решения задач обеспечения информационной безопасности банковской системы, начиная с архитектуры банковской сети, антивирусного программного обеспечения и заканчивая внедрением систем идентификации и аутентификации как клиентов банка, так внутренних пользователей. Основной вывод заключается в том, что несмотря на определенную специфику информационных систем банковского сектора, для защиты информации во многом пригодны те же методы и средства, что используются для обычных организаций. Главное – подходить к построению системы безопасности максимально ответственно, так как цена ошибки в банковской сфере высока как для самой банка, так и для его клиентов.*

Ключевые слова: *информационная безопасность, кибератаки, мультивендорая защита, 3dsec-коды.*

Практически каждый клиент банка, особенно в настоящее время, подвергается огромному количеству звонков или получению СМС оповещений в отношении якобы совершаемых именно в настоящее время банковских операций или в отношении попыток оформления кредита. Информационная безопасность банковского сектора выдержала, но некоторые аспекты обеспечения безопасности требуют проработки. Наиболее опасными для кредитных учреждений являются атаки на саму платежную систему, в случае успешных хакерских атак банк несет значительные финансовые потери [1].

Еще одно опасное направление кибератак – целевые атаки на процессинговые центры кредитных организаций с выводом средств через сеть банкоматов, карточный процессинг или систему SWIFT. Это – заражение подсистемы управления банкоматами или самих банкоматов, с последующей подачей команды на выдачу наличных или взлом процессинга с последующим зачислением денежных сумм на полученные карты. Далее злоумышленники просто снимают в банкоматах наличные денежные купюры.

Также подвергаются многочисленным атакам системы дистанционного банковского обслуживания клиентов. Многими банками внедрены 3dsec- коды, с помощью которых клиент должен подтворить осуществление банковской операции. Учитывая это, злоумышленники используют различные методы непосредственного эмоционального воздействия на человека с целью выманить данную информацию и совершить незаконную банковскую операцию. Как следует из отчета ЦБ России, в 2022 г. было похищено мошенниками у клиентов банков 14,2 млрд руб., что на 4,29% больше, чем в 2021 году. Доля краж с помощью социальной инженерии выросла до 50,4% [2].

Также в последнее время распространяются:

- вымогательство и шантаж. Например, на общий e-mail банка приходит письмо с угрозой что вся компьютерная сеть зара-

жена вирусом или процессинг банка взломан и далее требуют перечислить определенную сумму на электронный кошелек. В большинстве случаев это чистый фейк;

- несанкционированный доступ к криптовалюте. С момента своего изобретения (2009 год) криптовалюта остается все еще новым явлением в современной действительности, за весь период существования криптовалюты в результате применения вредоносных программ, хакерских атак было совершено множество взломов криптобирж. К большому сожалению, существует не так много способов обеспечения кибербезопасности в данном сегменте банковской деятельности.

По данным признанного эксперта в области противодействия DDoS-атакам Qrator Labs, в 2022 году число хакерских атак на российские ИТ-системы увеличилось на 73%, из них около 13% пришлось на платёжные системы и почти 10% – на отечественные финучреждения и банки, увеличилась ориентировочно на 1000% и длительность этих атак. В «Лаборатории Касперского» заявили, что продолжительность одной хакерской атаки составила почти 60 суток.

Помимо внешних атак существуют – внутренние злонамеренные и незлонамеренные нарушители информационной безопасности банковской сферы.

Банком России с целью регулирования вопросов информационной безопасности вменена обязанность коммерческим банкам сообщать в режиме онлайн в течение трех часов с момента возникновения об инцидентах информационной безопасности в ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности, специальное структурное подразделение Банка России).

Подразделение регулятора разработало и утвердило основные принципы обеспечения информационной безопасности банковской системы: улучшение правового регулирования системы, в том числе уточнение действующих законодательных актов; обеспечение информационной безопасности и кибербезопасности информационной системы банков; обеспечение информационной безопасности и кибербезопасности ПО, используемого для защиты информационных активов и персональных данных клиентов; соблюдение правил информационной безопасности при разработке и внедрении технологий обработки данных, улучшение качества финансовых технологий; повышение доверия населения к финансовой системе в целом; использование возможностей международного сообщества.

Система обеспечения информационной безопасности банка должна: быть адекватной внутренним и внешним угрозам; включать все необходимые организационные и технические мероприятия и комплексно защищать системы электронных платежей, электронного документооборота и обслуживания платежных карт, банковские программные и программно-технические комплексы, системы удаленного обслуживания, сети связи; обеспечивать высокую производительность; быть надежной; быть способной получить и проанализировать данные о фактах атак и фактах реагирования на события безопасности.

Так как большая часть обрабатываемой в банке информации относятся к банковской тайне, задача обеспечения ее защиты может быть решена только путем построения сложной комплексной системы защиты. Аналогичная ситуация складывается и с защитой значительного объема персональных данных в соответствии с законом 152-ФЗ «О персональных данных».

Все решения по информационной безопасности, программные и технические средства, регулируются стандартами Банка России, обязательными для применения.

Все задачи информационной безопасности необходимо решать комплексно, начиная с архитектуры банковской сети.

Достаточно распространенным способом в решении информационной безопасности является создание нескольких изолированных, хорошо защищенных шлюзов (сетей). В системе создаются изолированные операционные сети и сеть с доступом к ресурсам Интернета, в отдельные сети выделяются банкоматы и терминалы – все это позволит избежать многих проблем, связанных с утечкой информации и рас-

пространением вируса. Для надежной связи между подразделениями и филиалами банка должны использоваться выделенные каналы связи с применением шифрования данных.

Основными специализированными программами безусловно являются антивирусные программы. При помощи современного антивируса можно решить многие задачи, включая защиту от несанкционированного подключения любых внешних устройств или установки программ. Интернет-шлюзы и почтовые системы целесообразно защитить эшелонированной мультивендорной защитой, в которой несколько различных слоёв систем защиты установлены по всей компьютерной системе.

Актуальной идеей обеспечения безопасности банковской сферы может стать система удаленной идентификации (ЕСИА) [4]. С 30 декабря 2021 года единая биометрическая система (далее – ЕБС) приобрела статус государственной информационной системы, что определило ее дальнейшее развитие для обеспечения обработки биометрических персональных данных с учетом взаимодействия с иными информационными системами. В настоящее время ЕБС включена в состав инфраструктуры, обеспечивающей информационно-технологическое взаимодействие действующих и создаваемых информационных систем, используемых для исполнения государственных и муниципальных функций в электронной форме.

Если государством будет обеспечено наличие единой централизованной доверенной системы идентификации и аутентификации граждан, то это существенно упростит для банков задачу идентификации клиентов, в том числе в рамках исполнения Закона 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и для продвижения своих продуктов и услуг, в том числе в регионах, где нет физического присутствия конкретной финансовой организации.

Кроме аутентификации и контроля действий клиентов банку необходимо аутентифицировать и внутренних пользователей, т.е. обеспечить двухфакторную аутентификацию, будь то электронные ключи (токены) или генераторы одноразовых паролей.

В отношении сотрудников банка можно отметить следующее, сотрудники могут быть не только авторами самых больших проблем в безопасности, но и стать самой надёжной защитой безопасности. Исход зависит от того, как их обучить. У любой компании однозначно должен быть документ, регламентирующий поведение сотрудников во время атак на информацию, данные и ИТ-инфраструктуру. Обучение сотрудников по вопросам информационной безопасности − это ключ к предотвращению несанкционированных проникновений и распространению угроз. Необходимо убедиться, что сотрудники знают, как защититься от различных распространенных угроз, какие тактики несанкционированных проникновений существуют, что делать в случае взлома и как правильно защищать данные клиентов банка. Это кризисный план действий, который согласован со всеми подразделениями, сотрудниками и менеджментом, который может быть издан как отдельным документом или входить как раздел «Политики Информационной безопасности», утвержденной правлением коммерческого банка и описывать типичные ситуации атаки и разъяснять, кто из сотрудников что и в какие сроки должен делать.

Заключение. Информационные системы банков имеют свою специфику, но для защиты информации во многом пригодны те же методы и средства, что используются для обычных организаций. Главное – подходить к построению системы безопасности максимально ответственно, так как цена ошибки в банковской сфере высока как для самой банка, так и для его клиентов.

Библиографический список

1. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014) // Центральный банк Российской Федерации. – [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/.
2. Годовой отчет Банка России 2022 / Утвержден Советом директоров Банка России 28.03.2023 // Официальный сайт Банка России. – [Электронный ресурс]. – Режим доступа: www.cbr.ru/2023/C75-102.
3. Скородумов А. Информационная безопасность в банковской сфере: время перемен. – [Электронный ресурс]. – Режим доступа: https://www.tbforum.ru/blog/informatsionnaya-bezopasnost-v-bankovskoy-sfere-vremya-peremen.
4. Удаленная идентификация // Центральный банк Российской Федерации. – [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/2023.

FEATURES OF INFORMATION SECURITY BY THE BANK

A.N. Yurtsev, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *The banking sector is of the greatest interest to cybercriminals. The problem of the development of cybercrime is urgent due to the scale of losses incurred by both credit institutions themselves around the world and bank customers. The article shows the most dangerous areas of cyber attacks – on the payment system itself, on processing centers and remote banking customer service systems, describes the methods used by cybercriminals in achieving their plans. Much attention is paid to the need for a comprehensive solution to the problems of ensuring the information security of the banking system, starting with the architecture of the banking network, antivirus software and ending with the introduction of identification and authentication systems for both bank customers and internal users. The main conclusion is that despite certain specifics of information systems of the banking sector, the same methods and means that are used for ordinary organizations are largely suitable for information protection. The main thing is to approach the construction of the security system as responsibly as possible, since the cost of an error in the banking sector is high both for the bank itself and for its customers.*

Keywords: *information security, cyberattacks, multi-vendor protection, 3dsec codes.*