УДК 336.719.2

Садыков Р. Ф.

студент

Байлов К. А.

студент

Sadikov Ruslan

student

Bailov Konstantin

student

Санкт-Петербургский Государственный Лесотехнический

Университет им. С.М. Кирова

АКТУАЛЬНОСТЬ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ.

Аннотация.

Рассмотрена и проанализирована важность обеспечения информационной безопасности банковских систем. Излагается авторский взгляд на проблемы данной области.

Annotation

Relevance and problems of providing information security of banking systems. Annotation. The importance of ensuring information security of banking systems is considered and analyzed. The author's view on the problems in this area is presented.

Ключевые слова: *Информация, информационная безопасность банков, защита информации.*

Key words: *Information, information security of banks, information protection. Information security in banking systems plays a critical role in protecting the confidentiality, integrity and availability of financial information.*

Информационная безопасность в банковских системах играет критически важную роль для защиты конфиденциальности, целостности и доступности финансовой информации.

Актуальность информационной безопасности в банковских системах подтверждается следующими аспектами:

1. Конфиденциальность данных: Банковские системы содержат конфиденциальную информацию о клиентах, включая персональные данные, финансовые счета, транзакции и другие чувствительные сведения. Защита этой информации от доступа несанкционированных лиц является критической задачей для обеспечения доверия клиентов и соответствия нормативным требованиям.
2. Целостность данных: Банковские системы должны обеспечивать целостность данных, чтобы предотвратить искажение или модификацию информации несанкционированными лицами. Целостность данных необходима для сохранения точности финансовой информации и идентификации несанкционированных изменений.
3. Непрерывность бизнес-процессов: Банкировская деятельность зависит от непрерывности и доступности систем. Нарушения информационной безопасности, такие как кибератаки или вирусные атаки, могут привести к простоям или временной недоступности банковских услуг, что приводит к финансовым потерям и утрате клиентского доверия.
4. Соответствие нормативным требованиям: Банковские институты обязаны соблюдать строгие нормы безопасности и конфиденциальности, установленные компетентными органами и законодательством. Нарушение

нормативных требований может привести к финансовым штрафам, утрате лицензии или судебным преследованиям.

5. Защита от киберугроз: Банковские системы являются привлекательной целью для киберпреступников, которые стремятся получить доступ к финансовым ресурсам и скрыть свою активность. Защита от мошенничества, вредоносных программ и других киберугроз является необходимой для минимизации рисков финансовых потерь и сохранения репутации банка.

6. Защита от внутренних угроз: Банковские системы также нуждаются в защите от внутренних угроз, таких как несанкционированный доступ к данным со стороны сотрудников, конфликты интересов и злоупотребление привилегиями доступа. Эффективные механизмы аутентификации, авторизации и мониторинга должны быть введены, чтобы уменьшить подобные угрозы.

В информационной безопасности банков можно выделить несколько основных проблем:

1. Финансовые мошенничества: банки сталкиваются с угрозой мошенничества и кражи денег. К таким проблемам относятся фишинг, вредоносные программы, кража идентификационных данных клиентов и прочие финансовые атаки.

2. Компрометация данных клиентов: хакеры могут пытаться получить доступ к личной информации клиентов, такой как имена, адреса, номера социального страхования, номера кредитных карт и другие данные. Кража такой информации может привести к финансовым потерям и нанести серьезный ущерб репутации банка.

3. Недостаточная защита данных: банки могут столкнуться с проблемой слабой защиты данных, что может привести к утечке конфиденциальной информации или несанкционированному доступу к системам. Недостаточное обновление программного и аппаратного обеспечения,

уязвимости в системах и отсутствие механизмов обнаружения инцидентов также являются проблемами.

4. Социальная инженерия: хакеры могут использовать методы социальной инженерии для обмана сотрудников банка и получения несанкционированного доступа к системам или информации. Например, они могут представиться важным сотрудником банка и попросить отправить им конфиденциальную информацию.

5. Внутренние угрозы: иногда угрозы информационной безопасности могут исходить от сотрудников банка, намеренно или ненамеренно нарушающих политику безопасности. Недостаточное обучение сотрудников может способствовать подобным инцидентам.

6. Соответствие требованиям регуляторов: банки должны соблюдать строгие нормы безопасности и требования регуляторов в отношении защиты данных. Несоблюдение требований может повлечь за собой штрафы и снижение доверия со стороны клиентов.

Говоря об информационной безопасности банковской сферы невозможно не вспомнить о “Carbank”.

Вирус carbank является вредоносной программой, которая злоупотребляет финансовыми данными пользователей. Он предназначен для кражи информации о банковских счетах и кредитных карт, а также для осуществления незаконных финансовых транзакций.

Он занимает особое место в этой сфере, предполагаемый ущерб оценивается в 1 миллиард долларов. Можно сказать, что с момента начала активности этого вируса можно говорить о новой эпохе цифровых преступлений, в которой мошенники стали красть деньги не у клиентов, а у самих банков. Вирус затронул более 100 организаций. Первые случаи были обнаружены в конце 2013 года, однако пик активности вируса пришелся на середину 2014 года. Считается, что в половине случаев мошенникам удавалось выводить до 10 миллионов долларов из одного банка.

Еще можно вспомнить несколько известных хакерских атак на банки, которые оставили глубокий след в истории кибербезопасности.

Некоторые из них включают:

1. Центральный банк Бангладеш, 2016 год: Киберпреступники взломали серверы банка и украли около 81 миллиона долларов. Они использовали уязвимость в программном обеспечении, чтобы перевести деньги на различные банковские счета в разных странах. Попытка перевести еще 850 миллионов долларов была блокирована.
2. JP Morgan Chase, 2014 год: Группа киберпреступников смогла взломать серверы банка JP Morgan Chase и получить доступ к личной информации около 76 миллионов клиентов. Эта кибератака была одной из самых масштабных атак на банки когда-либо зафиксированных.
3. Тайваньский банк Far Eastern, 2015 год: Киберпреступники использовали вредоносное программное обеспечение, чтобы получить доступ к хранилищам данных и системам платежей банка. Они украли около 60 миллионов долларов.
4. Banco del Austro, 2015 год: Киберпреступники использовали фальшивые банковские карты и уязвимости в программном обеспечении банка, чтобы перевести более 12 миллионов долларов на счета в разных странах.
5. Банк Банг MetBank, 2019 год: Киберпреступники использовали фишинговые атаки и социальную инженерию, чтобы получить доступ к учетным записям сотрудников банка и информации о клиентах. После этого они смогли проникнуть в систему банка и провести кибератаку на около 1,6 миллиона долларов.

Это только некоторые известные примеры хакерских атак на банки. Все эти инциденты высветили важность кибербезопасности и заставили банки усилить свои меры защиты, чтобы предотвратить подобные атаки в будущем.

Изучив и проведя анализ всего сказанного выше, мы можем сделать вывод, что очень важно обеспечивать высокий уровень информационной безопасности в банковской сфере. Вмешательство злоумышленников в системы банков может привести к серьезным финансовым и репутационным последствиям как для банков, так и для их клиентов.

Банки должны активно вкладывать ресурсы в защиту своих информационных систем и клиентских данных. Необходимо установить и поддерживать современные системы безопасности, такие как фаерволы, антивирусы, межсетевые экраны и системы интра-сетевого обнаружения атак. Регулярное обновление и мониторинг этих систем является важным аспектом обеспечения безопасности.

Важным моментом также является обучение сотрудников банков вопросам информационной безопасности. Персонал должен быть осведомлен о возможных угрозах, методах атак, а также о процедурах предотвращения и реагирования на инциденты безопасности. Регулярные тренинги и тестирование знаний должны быть проведены, чтобы поддерживать высокую культуру безопасности среди сотрудников.

Взаимодействие с клиентами также требует особого внимания в плане информационной безопасности. Банки должны убедиться, что клиенты имеют доступ к безопасным каналам коммуникации и что их личные данные хранятся и передаются в безопасном режиме. Необходимо обеспечить двухфакторную аутентификацию и другие современные методы защиты для доступа клиентов к своим аккаунтам и выполнения финансовых операций.

В целом, адекватная информационная безопасность является неотъемлемой частью работы банка и его отношения с клиентами. Безопасность должна быть приоритетом для всех участников банковской сферы, чтобы защитить конфиденциальность и целостность данных, а также сохранить доверие клиентов и сохранить репутацию банка.

Использованные источники:

1. Марданов Р.Х., Ильин И.В. Стандарты информационной безопасности в банковской системе // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 7. С. 55–60.
2. Приходько А.А., Керопян Г.Б. Потери банков от киберпреступности // StudNet. 2020. №12.
3. Особенности обеспечения информационной безопасности в банковской системе
[Электронный ресурс]. – Режим доступа: http://www.antimalware.ru/analytics/Technology_Analysis/Features_information_security_in_the_banking_syst
em.
4. Сипратов, Р. О. Оценка рисков информационной безопасности кредитно-финансовой сферы и пути их снижения / Р. О. Сипратов // Актуальные вопросы современной экономики. — 2021. — № 2. — С. 369–375

References used

1. Mardanov R.Kh., Ilyin I.V. Information security standards in the banking system // Vestnik Ufimsky
State Aviation Technical University. 2013. T. 17. No. 7. pp. 55–60.
2. Prikhodko A.A., Keropyan G.B. Bank losses from cybercrime // StudNet. 2020. No. 12.
3. Features of ensuring information security in the banking system [Electronic resource]. – Access mode: http://www.antimalware.ru/analytics/Technology_Analysis/Features_information_security_in_the_banking_syst
em.
4. Sipratov, R. O. Assessing the risks of information security in the credit and

financial sphere and ways to reduce them / R. O. Sipratov // Current issues of modern economics. — 2021. — No. 2. — P. 369–375