УДК 336.719

Артамонова В.А.

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ
ABOUT INFORMATION SECURITY IN THE BANKING SECTOR

Филиал «Протвино» государственного университета «Дубна»
Секция «Социальные и гуманитарные науки»

Автор: Артамонова Виктория Алексеевна, студентка 3 курса направления «Информатика и вычислительная техника» филиала «Протвино» государственного университета «Дубна».

Научный руководитель: Захарова Лидия Ивановна, кандидат экономических наук, доцент кафедры информационных технологий филиала «Протвино» государственного университета «Дубна».

Author: Artamonova Victoria Alekseevna, 3rd year student of the direction «Informatics and computer engineering» of the branch «Protvino» state University «Dubna».

Scientific adviser: Zakharova Lidiya Ivanovna, candidate of economics sciences, associate professor of the department of information technology of the branch «Protvino» state University «Dubna».

Аннотация

В статье исследуются важность информационной безопасности в банковской сфере, основные виды угроз деятельности банков, приводятся проблемы информбезопасности и возможность их решения в настоящее время.

Abstract

The article explores the importance of information security in the banking sector, the main types of threats to the activities of banks, the problems of information security and the possibility of solving them at the present time.

Ключевые слова: банковские услуги, информационные технологии, кибер-атака, кибер-преступления, информационная безопасность.

Keywords: banking services, information technology, cyber attack, cyber crime, information security.

Статья, посвященная исследованию информационной безопасности в банковской сфере, является на сегодня достаточно актуальной, т.к. касается финансового жизнеобеспечения не только организаций, но и граждан.

Объект исследования – информбезопасность, предмет – эта безопасность в банковской среде.

Цель исследования – наметить пути решения проблем, связанных с повышением банковской информбезопасности. Для достижения цели необходимо решить задачи:

- показать актуальность и серьезность темы исследования;
- рассмотреть виды угроз информбезопасности и проникнуть в историю проблемы;
- оценить современное состояние банковской информбезопасности и отметить пути ее повышения.

Теперь, когда любой человек, имея доступ к средствам передачи информации и обладающий определённым набором знаний, может получить информацию предприятия для использования её в своих личных целях. В настоящее время, время

«информационного» общества, невозможно ведение успешного бизнеса без грамотно построенной системы информационной безопасности. Из этого следует, что становится недостаточным обеспечение физической охраны информации, а также материалов и иных ценностей, крайне важных для бизнеса. Особенно это касается финансово-банковской сферы

Благодаря своей специфической роли, со времени своего появления они всегда притягивали преступников. Банки в современном мире находятся в особой опасности, так как, имея непосредственный доступ к денежным средствам, становятся целью кибер-преступников. Поэтому обеспечение информационной безопасности банка является первостепенной задачей предпринимателя и неотъемлемой частью системы, гарантирующей безопасность банковского бизнеса.

Параллельно с процессами автоматизации и компьютеризации банковской системы растет проблема обеспечения защиты информации. Информация внутри банка перемещается огромными потоками, а основная часть данных подлежит обязательной конфиденциальности. Как показывают последние исследования, утечка хотя бы 20% информации, представляющих коммерческую тайну, в большинстве случаев приводит к разорению кредитной организации.

Действительно, банковская система как никакая другая подвержена опасности, так как в ней в первую очередь внедряются новейшие информационные технологии. Это происходит, во-первых, ради увеличения количества предоставляемых банком услуг, во-вторых, для повышения качества этих услуг. У клиентов банков появилось огромное количество преимуществ использования предлагаемых банком услуг, а самим кредитно-финансовым организациям становится все тяжелее конкурировать на рынке банковских услуг. В современном мире действует масса банков, которые используют в своей деятельности весь спектр возможных информационных технологий.

Отрицательные последствия из-за сбоев в работе отдельных банковских организаций приводят к стремительному развитию системного кризиса платежной системы России, а также наносят ущерб интересам клиентов и собственников. В случае наступления инцидента информационной безопасности значительно возрастает результирующий риск и возможность нанесения ущерба организациям банковской сферы [2,18]. Поэтому для организаций банковской системы угрозы информационным активам, то есть угрозы информационной безопасности, представляют реальную опасность (рис. 1).

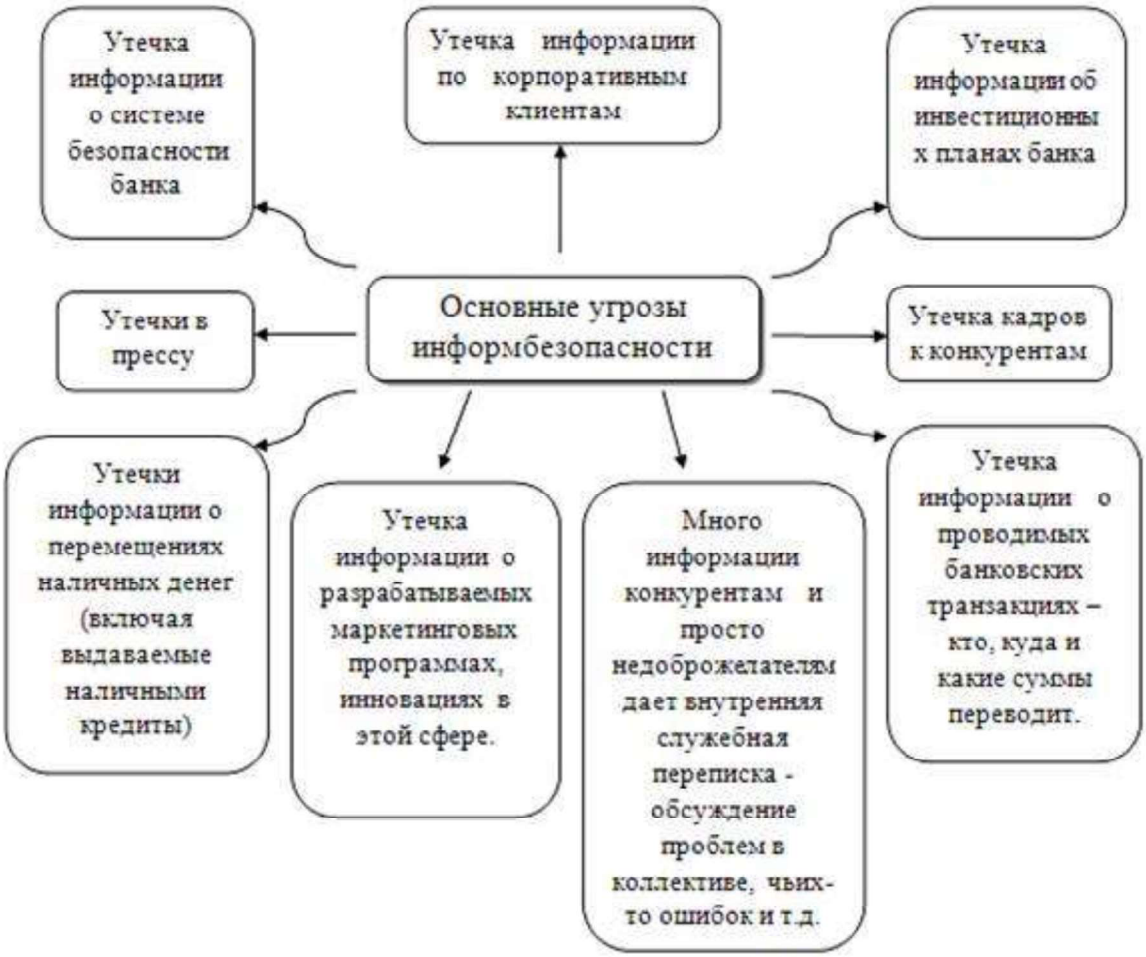

Рисунок 1. Основные угрозы информбезопасности

Существуют, как известно, два аспекта, выделяющих банки из круга остальных коммерческих систем:

1. Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д.

2. Она затрагивает интересы большого количества организаций и отдельных лиц.

Поэтому информационная безопасность банка — критически важное условие его существования.

Следует отметить, что со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Так, еще в XVIII веке недоброжелатели известного Джакомо Казановы опубликовали закрытые данные о движении средств по его счету в одном из парижских банков. Из этой информации следовало, что организованная Казановой государственная лотерея приносила доход не только казне, но и (в не меньших масштабах) ему лично [1, с.4].

Кроме того, в августе 1995 г. в Великобритании был арестован 24-летний российский математик Владимир Левин, который при помощи своего домашнего компьютера в Петербурге сумел проникнуть в банковскую систему одного из крупнейших американских банков Citibank и похитить $2,8 млн. В 1994 году Владимир

Левин вместе с приятелем сумел подобрать ключи к системе банковской защиты Citibank и попытался снять с его счетов крупные суммы. Служба безопасности Citibank выяснила, что у банка пытались похитить $2,8 млн., но контролирующие системы вовремя это обнаружили и заблокировали счета. Украсть же удалось лишь $400 тысяч.

В настоящее время в России особенно остро стоит вопрос обеспечения безопасности банковской информации. По данным службы Сбербанка только за 2017 год были зафиксированы свыше 60 тысячи попыток несанкционированных списаний денежных средств со счетов, ущерб от которых приравнивается к 7 млрд. рублей, а за период 2017-2018 гг. установлено свыше 70 критических ситуаций, которые могли нарушить систему работы банка.

По всей России, по сравнению с прошлыми годами число инцидентов связанных с информационной безопасностью банков возросло в 14 раз, а за 2018 год по всей стране зафиксировано свыше 50 тысяч кибер-преступлений, что, по мнению многих экспертов, весьма заниженный показатель.

Банки РФ несут существенные финансовые потери. В марте 2016 года на Металлинвест банк хакерами были совершены атаки, ущерб от которых оценивался в 667 млн. рублей. Позже, украденные средства удалось заблокировать в других банках, часть удалось вернуть. В том же году со счета Русского международного банка было похищено 508 млн. рублей. Исходя из отчетности банка, из похищенных денежных средств удалось вернуть 336 млн. рублей,28 млн. рублей заблокировали на счетах других банков, однако108 млн. рублей злоумышленникам удалось списать со счетов.

Российские банки оказались под особой угрозой в 2017 году, когда количество кибер-атак увеличилось еще в несколько раз. Усложняет ситуацию то, что появляются новые штампы вирусов, так называемые вирусы-вымогатели, которые блокируют работу не только банков, но и крупнейших организаций, таких как Nivea, Mars, Maerks и другие. Некоторые банки, на время пика кибер-атак прекращали свою деятельность, например «Хоум кредит банк» принял решение, в превентивном порядке провести проверку безопасности систем информационной безопасности. На то время отделения банка работали, проверке подверглись интернет-протоколы и сам сайт банка. После всех атак, такие крупные банки как Альфа-банк и Сбербанк России заявили, что атак на их сервисы не было зафиксировано.

Практика показывает, что популярным механизмом киберхищения является фишинг (от англ. – phishing), который заключается в рассылке электронных писем владельцам денежных средств о том, что они якобы стали победителями в какой-либо акции. Если владелец переходит по ссылке, отраженной в этом письме, данные его банковской карты (электронного кошелька) отсылаются злоумышленникам. Далее денежные средства потерпевшего без его ведома перемещаются на счета, подконтрольные хакерам».

Каковы же причины таких преступлений?

Основная из них — возросший уровень доверия к автоматизированным системам обработки информации. Им доверяют самую ответственную работу, от качества которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, движениями самолетов и поездов, выполняют финансовые операции, обрабатывают секретную информацию.

Не менее важная причина - рост киберпреступности как индустрии: «Сейчас вход на этот рынок доступен практически любому: научиться писать вирусы, взламывать сайты или почту можно по статьям в интернете».

Третья – преступления в сфере высоких технологий являются сложными для расследования, они требуют специальных знаний, опыта и ресурсов со стороны сотрудников правоохранительных органов. Существенная часть бытовых киберпреступлений (взлом социальных сетей или мессенджеров, вирусные атаки на домашние компьютеры) просто не фиксируется.

Четвертая – низкий уровень защищенности: граждане имеют минимальные знания о компьютерной гигиене и правилах безопасной работы в интернете, это делает их легкой добычей для киберпреступников».

Конечно, в последние десятилетия в Российской Федерации были реализованы практические меры по повышению уровня информационной безопасности банковской сферы. Скоординированными усилиями законодателей, Правительства РФ и Банка России была сформирована система нормативно-правового и организационного обеспечения банковской безопасности, а также осуществлялись практические мероприятия, которые совершенствовали меры безопасности в самих банках. Уровень банковской безопасности в современной России не соответствует объективным потребностям, и состояние защиты банков от преступных посягательств оставляет желать лучшего [1,6].

Библиографический список

1. Внуков А.А. Защита информации в банковских системах: учеб.пособие для бакалавриата и магистратуры / А.А. Внуков. – 2-е изд., испр. И доп. – М.: Издательство Юрайт, 2019. – 246 с.
2. Ефанова Е.А. Информационная безопасность банковской сферы в Российской Федерации // Молодежный научный форум: Общественные и экономические науки: электр. сб. ст. по мат. XLIX междунар. студ. науч.-практ. конф. № 9(49). URL: https://nauchforum.ru/archive/MNF_social/9(49).pdf (дата обращения: 08.10.2019)
3. Карпунова А.А. Проблемы обеспечения информационной безопасности в банковской сфере Российской Федерации и пути их решения // Научное сообщество студентов XXI столетия. Экономические науки: сб. ст. по мат. IV междунар. студ. науч.-практ. конф. № 4. URL: http://sibac.info/archive/economy/4.pdf (дата обращения: 20.10.2019)

УДК 004.92

Артамонова В.А., Михалюк Е.Ю.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ЗАМЕЧАТЕЛЬНЫХ КРИВЫХ МАТЕМАТИКИ В СРЕДЕ РАЗРАБОТКИ MICROSOFT VISUAL STUDIO 2019

PROGRAM REALIZATION REMARKABLE MATH CURVES IN THE VISUAL STUDIO 2019 DEVELOPMENT ENVIRONMENT

Филиал «Протвино» государственного университета «Дубна»

Секция «Информационные технологии»