УДК 338.43 DOI: 10.14451/1.234.279

Проблемы кибербезопасности в финансовом секторе цифровой экономики

© 2024 **Миргородская Марина Геннадьевна**
Кандидат экономических наук, доцент, заведующий кафедрой финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: mgm2502@mail.ru

© 2024 **Котова Ирина Борисовна**
Магистрант кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: kotova.08@yandex.ru

© 2024 **Аничкина Ольга Александровна**
Кандидат экономических наук, доцент кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: F-1980@yandex.ru

© 2024 **Целуйко Георгий Андреевич**
Аспирант кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: georgytseluyko@gmail.com

Ключевые слова: кибербезопасность, цифровая экономика, кибератаки, защита данных, финансовый сектор, утечка данных, персональные данные, информационная безопасность.

В цифровую эпоху финансовый сектор является важной мишенью для киберугроз из-за его экономической важности и конфиденциального характера обрабатываемых им данных. Появление интернет-банков, цифровых платежей и различных инноваций в области финансовых технологий изменило представление об удобстве и доступности для клиентов по всему миру. Однако эта цифровая трансформация также открыла новые уязвимости, которыми охотно пользуются киберпреступники. Сейчас, более чем когда-либо, защита цифровых активов — это не просто техническая проблема, а фундаментальная бизнес-проблема, которая может повлиять на доверие клиентов и корпоративную репутацию, именно поэтому тема данной статьи является актуальной. В статье рассматриваются текущие угрозы и риски, с которыми сталкиваются финансовые учреждения в цифровой экономике; роль человеческого фактора в уязвимости систем финансового сектора; меры предосторожности и защиты данных, которые могут быть приняты финансовыми компаниями; перечисляются основные методы и технологии, используемые злоумышленниками

для совершения кибератак на финансовые организации. В качестве вывода перечислены основные ключевые компоненты, которые должны быть частью любой надежной стратегии финансовой кибербезопасности.

В современных реалиях цифровые финансовые активы стали иметь такую же или даже большую ценность, чем физические активы, защита этих цифровых активов — от данных клиентов до стратегической финансовой информации — является колоссальной задачей, требующей многостороннего подхода. Финансовые учреждения должны сделать все, чтобы их меры кибербезопасности были надежными, масштабируемыми и способными противостоять постоянно меняющемуся ландшафту киберугроз и кибератак.

Основой законодательного регулирования Интернета в России является Конституция РФ [5]. Свободный доступ к информации гарантируется законом № 149-ФЗ «Об информации, информационных технологиях и защите информации» [11]. Доктриной информационной безопасности Российской Федерации, принятой Указом Президента от 5 декабря 2016 года, также определяются принципы регулирования этой области [8].

Стандарт ISO/IEC 27032:2012 определяет кибербезопасность как защиту от угроз в интернете и других сетях. Это включает защиту персональных данных, защиту от взлома и обеспечение доступности информации в любое время. Данный Стандарт объединяет разные аспекты безопасности, такие как безопасность приложений, сетевая безопасность, безопасность в интернете и безопасность ключевых систем информационной инфраструктуры. Все эти аспекты связаны между собой и работают вместе для обеспечения безопасности в киберпространстве (рис. 1) [14].

В соответствии с Концепцией Стратегии кибербезопасности Российской Федерации, кибербезопасность означает обеспечение защиты всех элементов киберпространства от угроз и злонамеренных действий. Киберпространство представляет собой окружающую среду, включающую сетевые каналы связи Интернета и других сетей, техническую инфраструктуру для их функционирования, а также различные формы человеческой деятельности, осуществляемые через них. Информационное пространство, в свою очередь, включает в себя всю информационную деятельность человечества [4]. Резюмируя, можно сказать, что киберпространство является безграничной, сложной средой и охватывает виртуальную сферу, в которой происходят цифровые взаимодействия, транзакции и коммуникации, что в свою очередь усложняет создание эффективной системы безопасности для него.

Актуальность обеспечения безопасности киберпространства обусловлена многочисленными киберугрозами и кибератаками, но перед тем, как перечислить и разобраться с основными их видами, следует пояснить, что из себя представляют данные термины. Киберугроза представляет собой угрозу потери данных или нарушения работы информационной системы в результате кибератаки. Кибератака — это преднамеренная попытка нарушить систему или же получить несанкционированный доступ к программному обеспечению, цифровым устройствам, чтобы причинить моральный или же физический ущерб в виде хищения конфиденциальных данных с целью их дальнейшей эксплуатации для извлечения некой выгоды.

Таким образом, если некий субъект (в виде определенного лица, объекта или явления) не проявит бдительность и воспользуется существующими уязвимостями, то потенциальная угроза перерастет в кибератаку, представляющую собой попытку проникновения в информационную систему и оказывающую негативное влияние на кибербезопасность.

Рис. 1. Связь между кибербезопасностью и другими видами безопасности.

Спектр киберугроз в финансовом секторе огромен и постоянно расширяется. Глобальный переход к цифровым финансовым услугам способствует регулярному появлению новых видов кибератак [9]. Ниже перечислены основные из них, которые активно применяются злоумышленниками на сегодняшний день:

1. Фишинговые атаки. Данные атаки проводятся в основном с помощью электронных писем, которые, как представляется, исходят из официальных источников, таких как банки, интернет-магазины и др., и запрашивают конфиденциальную информацию, такую как пароль от учетной записи, данные дебетовых и кредитных карт.
2. Атаки «Человек посередине» (Man-in-the-middle). Особенность данной кибератаки заключается в том, что злоумышленник перехватывает коммуникацию между пользователем и информационной системой, то есть при данной атаке, потенциальная жертва не догадывается о том, что в настоящий момент подвергается кибератаке. Стоит отметить, что данные атаки проводятся в основном при использовании общедоступных незащищенных сетей Wi-Fi или через скомпрометированные сетевые устройства.
3. Внедрение SQL-кода или же SQL-инъекции. Вид кибератаки, при котором злоумышленник, воспользовавшись уязвимостями веб-приложения, информационной системы выполняет вредоносные SQL-команды во внутренней базе данных. Манипулируя определенными запросами, он получает доступ к конфиденциальным данным и имеет возможность изменять, удалять или же выполнять административные команды. Данные атаки, как, впрочем, и большое число атак, выполняются с целью хищения конфиденциальной информации, внедрения вредоносного программного обеспечения (ПО) или нарушения безопасности всей системы.
4. Социальная инженерия (СИ). Атаки СИ направлены на психологическое давление, манипулирование пользователями с целью разглашения конфиденциальной информации и выполнения действий, ставящих под угрозу безопасность системы. Среди распространенных тактик СИ можно выделить использование предлогов, фишинг, кибербуллинг и слежку.
5. Захват учетной записи (Account takeover — ATO). Данный вид кибератаки подразумевает полный контроль над учетной записью пользователя в сети Интернет, а также над соответствующими авторизациями — паролями и конфиденциальной информацией. Целью данной атаки является совершение несанкционированных действий (в основном, совершение покупок разного размера) от имени пользователя данного аккаунта.
6. Скимминг. Данная кибератака направлена на сбор данных с кредитных и дебетовых карт с помощью установки вредоносных устройств на платежные терминалы, банкоматы и системы торговых точек. Скиммеры могут получить от платежных карт такую информацию, как номер карты, срок действия и CVV-код.
7. Атаки программ-вымогателей. Данные программы являются вредоносными, они блоки-

руют устройство или шифруют его содержание, вымогая деньги у жертв. За некую плату злоумышленники обещают восстановить доступ к зараженным устройствам и данным. Финансовые учреждения часто становятся мишенями для таких кибератак, поскольку хранят данные конфиденциального характера, так, например, информация о клиентах, финансовые отчеты и детали транзакций. Атаки программ-вымогателей распространяются через фишинговые письма, о которых ранее упоминалось, вредоносные веб-страницы и уязвимости информационной системы учреждения. Данные атаки чреваты большими финансовыми потерями и репутационным ущербом.

8. Инсайдерские угрозы. Данные угрозы, а в следствие и атаки, результат небрежных, а иногда и целенаправленных действий отдельных лиц внутри организации. Целью таких атак может быть хищение конфиденциальных данных клиентов в личных целях, если действия были преднамеренными, но в случае, если действия непреднамеренные, то сотрудники просто становятся жертвами фишинговых атак, и не зная об этом, разглашают конфиденциальную информацию.
9. DDoS атаки. Целью применения данного вида кибератак является выведение из строя серверов организации через одновременную отправку множества запросов на сервер, пока он не будет перегружен, отсюда и название «Отказ в обслуживании» (Distributed Denial of Service — DDoS). Часто злоумышленники могут потребовать деньги взамен на остановку вредоносных действий.
10. Компрометация корпоративной почты (Business Email Compromise — BEC). Атаки BEC, направленные на сотрудников финансовых учреждений, обманом заставляют их совершать несанкционированные транзакции, раскрывать конфиденциальную корпоративную информацию. Также преступник выдает себя за лицо, которому жертва доверяет, и просит переводить определенные средства. Стоит отметить, что при проведении данной кибератаки злоумышленники часто пользуются фишинговыми письмами.
11. Спуфинг. Данный вид кибератак является относительно новым, при котором злоумышленники создают поддельные веб-сайты, отражающие URL-адрес организации. Пользователи, не замечая разницу, могут воспользоваться данным сайтом, тем самым раскрывая свои конфиденциальные данные.
12. Эксплойты. Эксплойты представляют собой программный код, написанный злоумышленниками с целью использования уязвимостей в компьютерных системах, веб-приложениях или приложениях для получения несанкционированного доступа, установки вредоносного ПО или кражи конфиденциальной информации.
13. Постоянная серьезная угроза (advanced persistent threat — APT).
    APT — это целевая кибератака повышенной сложности, особенностью которой является то, что злоумышленник имеет доступ к сети в течение продолжительного времени. Эти кибератаки направлены на получение такой информации, как финансовые данные, бизнес-стратегии, которую в будущем преступник может использовать с целью шпионажа и вымогательства.

Не стоит недооценивать человеческий фактор при оценке уровня кибербезопасности, поскольку сотрудники служат в качестве основной защиты киберпространства организации. Хорошо обученные сотрудники могут оперативно реагировать на киберугрозу, тем самым предотвращая ее превращение в потенциальную киберататку, из этого следует, что необходимо выделять средства на их обучение, а также аналогичные мероприятия целесообразно будет провести для высшего руководства, которое должно планировать алгоритм по предотвращению киберинцидентов, ведь разработка надежной стратегии по борьбе с кибератаками может минимизировать последствия и обеспечить непрерывную работу организации.

Параллельно внедрению новых информаци-

онных технологий с целью повышения качества жизни появляются новые виды кибератак, а в условиях глобализации и интеграционных процессов борьба с киберпреступностью и вовсе становится сложной задачей.

Ниже перечислены основные проблемы, которые могут способствовать развитию киберпреступности [3, с. 8]:

- киберпреступники постоянно разрабатывают и внедряют новые вредоносные программы и методы взлома для использования уязвимостей в сетях и системах;
- слабая кибербезопасность организаций, которая связана с использованием необновлённого программного обеспечения и ненадежных паролей;
- низкая просвещенность о киберугрозах среди отдельных лиц и сотрудников организации могут привести к тому, что они станут жертвами, например, фишинга или других распространенных кибератак;
- огромные объемы конфиденциальных данных, которые хранятся в сети Интернет, делают их особенно привлекательными для злоумышленников, стремящихся украсть данные с целью шантажа и вымогательства;
- несовершенство нормативно-правовой базы также может сыграть на руку злоумышленникам, которые безусловно воспользуются этим;
- необходимость экспертов для создания надлежащей защиты от киберугроз;
- глобальный характер киберугроз, поскольку, как ранее выяснили, киберпространство является безграничной средой, процесс определения местонахождения злоумышленника, откуда была проведена кибератака и последующее судебное преследование правонарушителя, становится задачей нетривиальной;
- нехватка квалифицированных специалистов по кибербезопасности;
- утаивание фактов о совершенных кибератаках с целью сохранения репутации.

В современных реалиях, где цифровизация успешно протекает в каждой сфере, финансовый сектор не является исключением и вопрос о значении кибербезопасности априори становится актуальным.

Защита данных клиентов, владельцев цифровых активов, которые идут наравне с физическими активами, является одной из важных задач для финансовых учреждений, в чьих базах данных хранится информация о конфиденциальных данных клиентов, проведенных транзакциях и др. Утечка этих данных может иметь серьезные последствия как для самого учреждения, так и для клиента.

Стоит также отметить про важность сохранения доверия клиентов и репутации, поскольку слабая защита от киберугроз с легкостью может спровоцировать кибератаку, что в свою очередь отрицательно скажется на отношениях клиента и финансового учреждения, на восстановление которых нужно будет потратить годы [12, с. 12].

Согласно отчету Группы Компаний (ГК) InfoWatch, объем персональных данных, которые оказались в общем доступе в 2023 году выросли на 60%, составив — 1,12 млрд записей по сравнению с 2022 годом (тогда это число составило 702 млн). В 2023 году утечка баз данных увеличилась, с такой проблемой столкнулись 95 основных баз данных российских компаний, что на 28% больше, чем в 2022 году. В отчете также указывается, что 80% и более утечек с данными — это следствие кибератак, при этом каждая десятая утечка была связана с действиями сотрудников. Стоит отметить, что данный показатель в 2023 году снизился на 45%, однако опрос проведенный также ГК InfoWatch, показал, что 35% представителей компаний считают, что утечка по неосторожности сотрудника одна из наиболее актуальных угроз [2]. Результатом таких утечек могут быть финансовые потери, штрафы регулирующих органов из-за нарушения закона по персональным данным (152-ФЗ), затраты на устранение последствий [10].

Таким образом, учитывая все вышеизложенное, обеспечение высокой защиты от кибератак является важной задачей для финансового сектора, но стоит также отметить, что это довольно

ресурсозатратный процесс и в рамках данного процесса учреждения сталкиваются со множеством препятствий, так, например, управлением устаревшими системами и проблемой опережения быстроразвивающихся киберугроз. Поскольку определенное количество финансовых учреждений работают на устаревших системах, то возникает такая проблема, как несовместимость с современными мерами безопасности, также данные системы могут иметь неизвестные уязвимости, которые трудно устранить, что в свою очередь делает их легкой мишенью для злоумышленников. При принятия решении о модернизации данных систем, стоит учитывать, что процесс будет занимать много времени и требовать немалых затрат.

Также не стоит недооценивать злоумышленников, которые с развитием новых технологий регулярно находят инновационные решения для придумывания новых способов осуществления кибератак. Такие быстро меняющиеся способы взлома системы безопасности требуют постоянной бдительности, периодических обновлений системы и проведения нужных обучающих мероприятий для просвещённости сотрудников в данной области.

Следует также отметить про нормативные ограничения, поскольку в каждой стране действуют определенные законы защиты данных и кибербезопасности, следовательно, международные учреждения должны обеспечивать соблюдение всех этих законов. Разработка комплексных мероприятий по защите данных от киберугроз имеет ключевое значение в финансовом секторе [6].

Таким образом, перечислим те ключевые компоненты, которые должны являться частью стратегии по кибербезопасности:

1. Внедрение межсетевого экрана (брандмауэр), который выполняет функцию проверки и фильтрации данных, поступающих из интернета; внедрение безопасного веб-шлюза, он служит в качестве кибер-барьера или контрольной точки, которая не позволяет неавторизованному трафику проникнуть в систему организации; использование единых конфигураций для всех систем и ПО.
2. Проведение аудитов и оценки рисков на ИТ-инфраструктуры на регулярной основе, что позволит выявить уязвимости заблаговременно и принять необходимые меры.
3. Периодическое обновление и исправление информационной системы, поскольку устаревшие системы особенно подвержены кибератакам.
4. Создание четкого плана реагирования на инциденты позволит оперативно реагировать на угрозу.
5. Шифрование данных при передаче с помощью двухфакторной или многофакторной аутентификации, что обеспечит дополнительную защиту от киберугроз.

Стоит также отметить о важности знающего и бдительного персонала, который является одним из наиболее эффективных средств защиты от киберугроз. Регулярное обучение на первоклассных курсах по кибербезопасности может помочь сотрудникам выявлять потенциальные угрозы и реагировать на них, снижая риск успешных атак. Согласно результатам опроса Группы Компаний InfoWatch, в условиях ухудшающейся тенденции к утечке конфиденциальной информации в 2023 году 59% организаций провели фундаментальное обучение сотрудников информационной безопасности и гигиене. Кроме того, 27% интегрировали системы предотвращения вторжений и еще 17% внедрили системы DLP (предотвращения потери данных) для защиты от утечек конфиденциальных данных в корпоративной сети.

Если взглянуть в будущее, становится ясно, что кибербезопасность в финансовом секторе по-прежнему будет оставаться насущной проблемой. Однако благодаря новым достижениям и появляющимся технологиям отрасль готова решать эти проблемы более эффективно.

Искусственный интеллект (ИИ) и машинное обучение (МО) — две технологии с огромными перспективами для кибербезопасности. Они могут обнаруживать аномальное поведение или

закономерности, указывающие на кибератаку, часто распознавая эти признаки раньше, чем аналитики-люди. Кроме того, они могут помочь в автоматизации реагирования на угрозы более низкого уровня, освобождая персонал по кибербезопасности для того, чтобы сосредоточиться на более сложных проблемах.

Технология блокчейн, известная своей безопасной и прозрачной природой, также может быть использована для повышения кибербезопасности. Она может помочь в поддержании безопасных, неизменяемых записей транзакций, тем самым уменьшая возможности для мошенничества. Более того, ее применение при проверке личности может значительно улучшить процессы аутентификации пользователей [13].

Роль регулирующих органов также будет иметь решающее значение в формировании будущего кибербезопасности в финансовом секторе. Стандарты регулирования должны идти в ногу с технологическими достижениями, обеспечивая безопасное и ответственное внедрение новых технологий.

После рассмотрения ситуации с кибербезопасностью в финансовом секторе стало очевидно, что защита цифровых активов является важнейшей задачей. Финансовые учреждения находятся на переднем крае цифровой экономики, защищая не только денежные активы, но и конфиденциальные персональные данные, которые при неправильном обращении или компрометации могут иметь далеко идущие последствия.

Таким образом, стремительный прогресс информационных технологий в последние десятилетия привел к глубоким преобразованиям как в экономике, так и в обществе. Практически неограниченный доступ к электронной информации и телекоммуникационным услугам фундаментально и навсегда изменил наш образ жизни и мыслительные процессы. Кроме того, развитие технологий значительно изменило то, как преступники осуществляют незаконную деятельность. Информационные технологии не только расширили возможности для совершения традиционных преступлений в Интернет-пространстве, но и привнесли новые и рискованные формы преступного поведения, включая киберугрозы.

Библиографический список

1. Банки утаивают каждую пятую успешную кибератаку. — URL: https://www.securitylab.ru/news/489810.php (дата обр. 12.03.2024).
2. ГК InfoWatch, Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г.: Аналитический отчет. — Экспертно-Аналитический центр InfoWatch, 2023. — 17 с.
3. *Дерюгин Р. А.* Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. — 2019. — № 2.
4. *Козырь Н. С.*, *Оганесян Л. Л.* Экономические аспекты информационной безопасности : учебник и практикум для вузов. — М. : Юрайт, 2024. — 131 с.
5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) / Собрание законодательства РФ. — 04.08.2014, № 31. – ст. 24.
6. Концепция стратегии кибербезопасности Российской Федерации. — URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обр. 12.03.2024).
7. *Номоконов В. А.* Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. — 2013. — 5 (10).
8. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
9. Управление рисками информационной безопасности [Текст]: учебное пособие для вузов / А. П. Курило [и др.]. — 2-е изд. — М. : Горячая линия – Телеком, 2015. — 130 с.
10. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. *Чернова Г. В.* Страхование и управление рисками : учебник для бакалавров / под ред. Г. В. Черновой. — 2-е изд. — М. : Юрайт, 2017. — 767 с.
13. *Boes S.*, *Leukfeldt E. R.* Fighting cybercrime: joint effort // Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. — Cincinnati : Springer, 2016. — P. 185–205.
14. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.