**УДК 336.719.2**

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ**

**В ФИНАНСОВОЙ СФЕРЕ**

**Д.Р. Козлова**

***Аннотация.*** *В статье рассматриваются вопросы кибербезопасности в финансовой сфере, описываются основные решения, препятствующие осуществлению кибератак и мер, защищающих от киберугроз, приводятся аргументы важности кибербезопасности. Цель нашего исследования выявление актуальных проблем, формулирование понятия кибербезопасности и предложение решения проблем кибербезопасности в финансовой сфере. Были использованы следующие методы: изучение и анализ литературы по проблеме исследования; сравнение; обобщение. Результаты проведенного исследования показали, что распространенные киберугрозы в финансовом секторе постоянно развиваются и становятся все более сложными, чтобы опережать злоумышленников, важно понимать различные векторы направлений, которые они используют для проведения атак, именно поэтому приводится комплекс действий стратегического характера, направленный на защиту от нанесения экономического, технического или информационного ущерба вследствие угроз, совершаемых с помощью программно-технических средств, а также в результате ежедневной работы с информационными сетевыми технологиями.*

***Ключевые слова:*** *кибербезопасность, киберугрозы, информационные системы, информационная безопасность, кибер-риски, финансовый сектор, кибератака.*

**CURRENT CYBERSECURITY ISSUES**

**IN THE FINANCIAL SPHERE**

**D.R. Kozlova**

***Annotation.*** *The article discusses the issues of cybersecurity in the financial sphere, describes the main solutions that prevent the implementation of cyber-attacks and measures that protect against cyber threats, and provides arguments on the importance of cybersecurity. The purpose of our research is to identify current problems, formulate the concept of cybersecurity and propose solutions to cybersecurity problems in the financial sector. The following methods were used: study and analysis of the literature on the research problem; comparison; generalization. The results of the study showed that widespread cyber threats in the financial sector are constantly evolving and becoming more complex, in order to stay ahead of attackers, it is important to understand the various vectors of the directions they use to carry out attacks, which is why a set of strategic actions aimed at protecting against economic, technical or information damage due to threats made using software and hardware, as well as as a result of daily work with information network technologies is given.*

***Keywords:*** *cybersecurity, cyber threats, information systems, information security, cyber risks, financial sector, cyber-attack.*

За последнее десятилетие кибератаки стали популярными в финансовой сфере. Киберпреступники эволюционировали в технологиях, совершенствуя свои методы и навыки. Кибербезопасность не ограничивается какими-либо отраслями, связанными технологиями. Технологии имеют решающее значение в финансовой сфере, поскольку именно в ней совершают миллионы транзакций каждый день, и большинство из них выполняется на платформах цифровых платежей. Это делает финансовый сектор основной целью кибератак во всем мире.

Защита активов клиентов - одна из основных причин, почему кибербезопасность важна в финансовой сфере. Интернет захватывает мир, другие люди переходят на безналичный расчет, а действия, связанные с деньгами, осуществляются через сканеры кредитных карт и страницы онлайн-оплаты. В обоих случаях данные клиента могут быть получены или перенаправлены в любое место. Эти действия повлияют на клиентов и повредят бизнесу, им придется восстанавливать данные.

Более того, организации могут в конечном итоге заплатить хакерам сотни и тысячи долларов за разглашение информации, когда их данные будут взяты в заложники. Это повлияет на финансовый сектор экономически, а также на его репутацию, клиенты потеряют доверие к финансовому учреждению. В мире наблюдается волна оцифровки, поэтому необходимо повысить уровень своей кибербезопасности. Эти причины показывают, почему кибербезопасность важна для любого финансового учреждения [4].

В процессе исследования проанализированы работы, посвященные проблеме глобального развития киберпреступности, а также методам обеспечения кибербезопасности финансовых организайций. Весомый вклад в исследование данных вопросов внесли отечественные учёные: Номоков В.А., Тропина Т.Л., Чернова М.А., Семенко Г.В., Алпеев А.С., а также зарубежные: Leukfeldt E.R., Gable K.A., Boes S. [5]

Понятие кибербезопасности является относительно молодым, поэтому не имеет общепринятого определения.

Кибербезопасность обеспечивает защиту от возникновения убытков из-за действий злоумышленников, которые совершаются при помощи телекоммуникационных технологий, т.е. борется с проявлением кибер-рисков.

Согласно докладу «Управление рисками и кибербезопасность», подготовленному компанией Price water house Coopers (PwC), ключевыми аспектами кибербезопасности являются [2]:

1) определение уровня допустимого риска и пороговых значений ущерба;

2) определение приемлемого остаточного риска и лимитов принятия риска;

3) обеспечение методикой оценки рисков необходимой точности и финансовых значений оценки;

4) установление прозрачной связи бизнес-процессов и критичных активов;

5) распределение новых ролей и ответственности между компетентными специалистами;

6) определение допустимых сроков закрытия выявленных рисков;

7) определение ключевых индикаторов риска и установление порядка мониторинга рисков;

8) определение положения кибер-рисков в системе корпоративного управления рисками;

9) соответствие уровней принятия решений полномочиям лиц;

10) регулярное предоставление лицам, принимающим решения, достоверной отчетности о кибер-рисках.

Киберугрозы становятся все сложнее. Ежегодно выявляются сотни миллионов новых видов вредоносного ПО. Новые типы вредоносных программ могут избежать обнаружения традиционными антивирусами или даже работать без использования двоичных файлов (бесфайловые атаки).

Киберпреступления обычно не происходят в вакууме; они во многом распространены в природе. То есть киберпреступники обычно полагаются на других участников для совершения преступления. Будь то создатель вредоносного ПО, использующий даркнет для продажи кода, дистрибьютор нелегальных фармацевтических препаратов, использующий криптовалютных брокеров для хранения виртуальных денег на условном депонировании, или государственные субъекты угроз, полагающиеся на технологических субподрядчиков для кражи интеллектуальной собственности.

Киберпреступники используют различные векторы атак для проведения своих кибератак и постоянно ищут новые методы и приемы для достижения своих целей, избегая обнаружения и ареста.

Атаки становятся все более многослойными и включают сочетание сетевых методов, вредоносных программ и атак веб-приложений. Внутренние угрозы представляют собой растущую проблему, и внутренние атаки очень трудно отличить от законных действий пользователей. Злоумышленники также используют такие устройства, как мобильные телефоны, подключенные к сети устройства в офисе и дома, а также инфраструктуру Интернета вещей для проведения крупномасштабных атак.

Системы искусственного интеллекта (ИИ), основанные на алгоритмах машинного обучения, могут помочь обнаружить и устранить многие из этих новых угроз. Они способны анализировать гораздо больший объем данных, чем профессионалы в области безопасности человека, интеллектуально выявлять аномалии и подозрительное поведение и расследовать угрозы путем сопоставления множества точек данных. Системы безопасности с искусственным интеллектом несовершенны и требуют контроля, настройки со стороны человека, но становятся важной частью арсенала кибербезопасности в 21 веке.

С ростом числа угроз, с которыми сталкиваются организации как извне, так и изнутри, информационные системы становятся важной частью системы обеспечения безопасности. Чтобы быть эффективной, безопасность должна применяться на нескольких уровнях, включая уровни сети, облака, конечных точек и приложений.

Инструменты и методы информационной безопасности должны развиваться быстро, чтобы не отставать от новых и развивающихся киберугроз. Передовые технологии кибербезопасности используют машинное обучение, что позволяет организациям опережать киберугрозы. Это алгоритмы и системы, которые могут использовать данные из сетей и приложений для интеллектуального обнаружения, расследования и даже реагирования на киберугрозы.

Рассмотрим основные современные угрозы кибербезопасности на примере банковского сектора. Существует множество распространенных угроз кибербезопасности финансового сектора, в последнее время появилось несколько современных угроз:

1. Кража личных данных - получение чьих-либо финансовых данных без их ведома с целью совершения скрытых действий. Когда в банке обрабатывается конфиденциальная информация клиентов, то украденная информация банка обычно продается и покупается в темной сети незаконными организациями и другими киберпреступниками.
2. Спуфинг. Этот тип киберугроз является относительно новым, при котором кибератаки находят способ имитировать URL-адрес банка с помощью поддельного веб-сайта, который функционирует и выглядит точно так же. Если злоумышленники могут заставить клиента открыть и использовать поддельный веб-сайт вместо настоящего, клиент использует конфиденциальную информацию, такую как имя пользователя и пароль, думая, что они действуют на настоящем веб-сайте банка. Эта информация, представленная клиентом на поддельном веб-сайте, затем быстро берется хакерами для использования или продажи позже.
3. Небезопасные сторонние сервисы. Некоторые финансовые средства используют сторонние инструменты, такие как чат-боты и программное обеспечение для управления взаимоотношениями с клиентами, предлагаемые другими частными компаниями, для предоставления клиентам более качественных услуг. Однако, если эти сторонние компании не обладают кибербезопасностью, это может повлиять на ваш банк. Уровень интеграции таких сторонних инструментов с системными банковскими системами и с системами, которые хранят данные клиентов, необходимо тщательно проверять.

Количество кибератак в банковской сфере растет, приведем несколько способов минимизировать риск взлома.

Так как осуществлять вручную запрос каждой транзакции на предмет угроз нецелесообразно, поэтому банкам придется использовать решения по автоматизации процессов, чтобы автоматизировать все процессы мониторинга и сканирования, заблокировать и отфильтровать проникновение вредоносного трафика в сеть. Идеальное решение безопасности будет останавливать и пропускать прозрачные действия. Более того, эти киберрешения должны легко настраиваться и обновляться.

Необходимо информирование и обучение сотрудников по угрозам, с которыми обычно сталкиваются финансовые учреждения, для их предотвращения. Многие кибератаки нацелены на сотрудников и пытаются получить от них информацию, поэтому необходимо сообщить команде о таких действиях и о том, чего ожидать. Это особенно важно, поскольку многие кибератаки исходят от вирусов, которые проходят через эти вложения. Учреждениям также запретить своим сотрудникам делиться конфиденциальной информацией.

Кибератаки часто включают человеческий фактор, когда сотрудники, подрядчики или даже клиенты невольно участвуют в инцидентах. Эта проблема номер один для каждого руководителя высшего звена, в частности, мы наблюдаем растущую озабоченность человеческим фактором. Один щелчок по ссылке или загрузка может привести к дорогостоящей атаке программ-вымогателей или утечке данных, что может повлечь за собой репутационный ущерб и потерю данных.

Обучение и технологии могут помочь свести к минимуму человеческий фактор. Сотрудники - это первая линия безопасности и защиты. Человеческий фактор может повлиять на положение организации в области кибербезопасности, а зачастую и на ее репутацию. Те, кто хорошо обучен, могут значительно уменьшить воздействие нарушения или даже предотвратить его. Сотрудников следует рассматривать как часть группы по кибербезопасности, именно поэтому необходимы соответствующие инвестиции в их обучение и образование. То же самое относится и к высшему руководству, которое должно периодически репетировать сценарии, чтобы подготовиться к крупному киберинциденту и уметь своевременно отреагировать на него - создание устойчивости и планирование непрерывности бизнеса являются абсолютным ключом к снижению воздействия. Кибербезопасность идет вверх по цепочке [3].

Регулярно проверять все системы. Кибератаки всегда можно проследить до каких-то лазеек или незначительных уязвимостей во внутренних системах и настройках сети. Обращать внимание на все, например, на отсутствие правил безопасности, ошибки разработки, неправильно настроенные системы или устаревшие расширения. Оценка уязвимости может помочь выявить отстающую их инфраструктуру в разделе безопасности и исправить их. В то же время тесты на проникновение могут имитировать реальные кибератаки, чтобы проверить надежность системы безопасности.

Истинную цену киберпреступности сложно точно оценить. Финансовые потери из-за киберпреступности могут быть значительными, предприятия могут также пострадать от других катастрофических последствий в результате преступных кибератак, включая следующие:

1. Ущерб для восприятия инвестора после взлома системы безопасности может привести к падению стоимости компании.
2. Помимо потенциального падения цен на акции, предприятия могут столкнуться с повышенными затратами на заимствования и более сложным трудностям в привлечении дополнительного капитала в результате кибератаки.
3. Потеря конфиденциальных данных клиентов может привести к штрафам для компаний, которые не смогли защитить данные своих клиентов. Компании также могут быть привлечены к ответственности за утечку данных.
4. Поврежденная идентичность бренда и потеря репутации после кибератаки подрывают доверие клиентов к компании и способность этой компании хранить свои финансовые данные в безопасности. В результате кибератаки фирмы не только теряют текущих клиентов, но и теряют возможность привлекать новых.
5. Предприятия также могут понести прямые расходы в результате криминальной кибератаки, включая увеличение стоимости страховых взносов и затрат на найм компаний по кибербезопасности для реагирования на инциденты и их устранения, а также на связи с общественностью и другими услугами, связанных с атакой.

Таким образом, бурный рост информационных технологий в последнее десятилетие ускорил беспрецедентные экономические и социальные изменения. Наш практически неограниченный электронный доступ к информации и телекоммуникационным услугам глубоко и безвозвратно изменил наш образ жизни и образ мышления. Точно так же технический прогресс резко изменил способ, которым преступники осуществляют свою деятельность. Информационные технологии не только создали дополнительную платформу для совершения традиционных преступлений, но и проложили путь для новых и пагубных форм преступности, включая киберугрозы.

В заключение хотелось бы отметить, насколько важно обеспечивать кибербезопасность в современной экономике, ведь потери могут быть просто колоссальны. Борьба с киберпреступностью ведется на всех уровнях: международном, государственном, региональном, отраслевом и на уровне отдельно взятых субъектов (в частности, финансовых организаций) [1].

Финансовая сфера имеет так много возможностей повышения своей кибербезопасности, несмотря на уязвимости. Финансовые учреждения могут сосредоточиться на поиске решений по киберугрозам и внедрению этих решений в свои сети, одновременно внедряя новые технологии, которые могут обеспечить бесперебойный процесс деятельности.

**Список литературы**

1. Оценка кибер-рисков в банковском секторе (на примере ПАО «Сбербанк») |Вигриянова | 38.03.01 Экономика [Электронный ресурс] // URL: <https://vkr.urfu.ru/index.php/38_03_01/article/view/213101> (дата обращения 20.03.2021).
2. Доклад PWC: Управление рисками и кибербезопасность [Электронный ресурс] // URL: [http://files.runet-id.com/2017/csf17/07feb.csf17- 3.2--chaplygin.pdf](http://files.runet-id.com/2017/csf17/07feb.csf17-%203.2--chaplygin.pdf) (дата обращения 20.03.2021).
3. Проектирование кибербезопасности для финансового сектора. Livemint. [Электронный ресурс] // URL: https://www.livemint.com/ (дата обращения 20.03.2021)
4. Кибербезопасность в секторе банковских и финансовых услуг - угрозы IoT, потенциальные решения и блокчейн. Stoodnt. [Электронный ресурс] // URL: https://www.stoodnt.com/ (дата обращения 20.03.2021).
5. Шматкова, Л.П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы. Молодой ученый. 2016. № 28 (132). С. 720-723 [Электронный ресурс] // URL: [http://elibrary.ru/item.asp?id=27535415](https://mkgtu.antiplagiat.ru/report/go?to=CfDJ8HWXr_sBTqlBrk4QroCjqzMt1_6oFWxdFNEmGpxfPjg13kd1IyX5DAYVkqqL7xlDruH3OoO-tNkOwjkKsmmJGgErexo47fsIIBZ0csE0ZUNiQVfvOIhvDOSdoG6qoCYazx2jZapsPuU1d0mB4TvKYlaTXIYeju3Oeea8qughczKe&next=do). (дата обращения 20.03.2021).

**References**

1. Assessment cyber risks in the banking sector (on the example of PJSC "Sberbank") |Villanova | 38.03.01 Economics [Electronic resource] // URL: https://vkr.urfu.ru/index.php/38\_03\_01/article/view/213101 (accessed 20.03.2021).

2. PWC report: risk Management and cyber security [Electronic resource] // URL: http://files.runet-id.com/2017/csf17/07feb.csf17 - 3.2--chaplygin.pdf (accessed 20.03.2021).

3. The design of cybersecurity for the financial sector. Livemint. [Electronic resource] // URL: https://www.livemint.com / (accessed 20.03.2021)

4. Cybersecurity in the banking and financial services sector - IoT threats, potential solutions and blockchain. Stoodnt. [Electronic resource] // URL: https://www.stoodnt.com / (accessed 20.03.2021).

5. Shmatkova, L.P. International cooperation in combating cybercrime: state and prospects. A young scientist. 2016. No. 28 (132). pp. 720-723 [Electronic resource] // URL: http://elibrary.ru/item.asp?id=27535415 . (accessed 20.03.2021).

**Козлова Дарья Романовна**

Обучающаяся второго курса направления подготовки 10.03.01. Информационная безопасность ФГБОУ ВО «Майкопский государственный технологический университет».

E-mail: natali20052001@bk.ru

(Майкоп)

**Научный руководитель:** Козлова Наталья Шумафовна, кандидат философских наук, доцент кафедры информационной безопасности и прикладной информатики, ФГБОУ ВО «Майкопский государственный технологический университет»

**Kozlova Darya Romanovna**

Student of the 2rd year of training10.03.01. Information security of the Maykop State Technological University.

E-mail: natali20052001@bk.ru

(Maykop)

**Scientific advisor:**  Natalia Kozlova, PhD, Associate Professor of the Department of Information Security and Applied Informatics, Maykop State Technological University