ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 33

УПРАВЛЕНИЕ РИСКАМИ В ФИНАНСОВОЙ СФЕРЕ, ВКЛЮЧАЯ КИБЕРБЕЗОПАСНОСТЬ, РИСКИ ВЗЛОМА И ФИНАНСОВЫЕ МОШЕННИЧЕСТВА

Семенюк Яна Васильевна [1],
Студент 3 курса УрГУПС, г. Екатеринбург, РФ,
semenyuck.iana@gmail.com

Аннотация

Управление рисками в финансовой сфере помогает предотвратить негативные последствия, связанные с потерей денег и нарушением конфиденциальности данных клиентов, что является достаточно частой проблемой в наши дни.

Ключевые слова: безопасность, мошенничество, кибербезопасность в финансовой сфере, кибератаки в финансовой сфере, электронный платежи, банковские системы.

FINANCIAL RISK MANAGEMENT, INCLUDING CYBERSECURITY, HACKING RISKS AND FINANCIAL FRAUD

Yana V. Semenyuk [2],
3rd year student of USUPS,
semenyuck.iana@gmail.com,
Yekaterinburg, Russia

ABSTRACT

Risk management in the financial sector helps to prevent the negative consequences associated with the loss of money and violation of the confidentiality of customer data, which is a fairly common problem these days.

Keywords: security, fraud, cybersecurity in the financial sector, cyber attacks in the financial sector, electronic payments, banking systems.

[1] Научный руководитель: Колышев Андрей Сергеевич. Преподаватель кафедры «Экономика транспорта», УрГУПС, г. Екатеринбург, РФ, ASKolyishev@bk.ru

[2] Scientific supervisor: Andrey S. Kolyshev, Lecturer of the Department "Economics of Transport", USUPS, ASKolyishev@bk.ru, Yekaterinburg, Russia

Риски, связанные с кибербезопасностью в финансовой сфере, могут быть крайне высокими, так как финансовые организации обрабатывают большие объемы чувствительной информации, включая данные о клиентах, финансовые транзакции и конфиденциальные документы. Нарушение безопасности данных может привести к утечке конфиденциальной информации, финансовым потерям, нарушению репутации компании и негативному влиянию на отношения с клиентами.

Одним из основных рисков является кибератака, которая может привести к нарушению целостности, конфиденциальности и доступности данных. Киберпреступники могут использовать различные методы, такие как фишинг, вредоносное программное обеспечение, DDoS-атаки и социальную инженерию, чтобы получить несанкционированный доступ к системам и данным финансовых организаций.

Другим риском является внутренняя угроза, связанная с неправомерными действиями работников или подрядчиков. Несоблюдение правил безопасности, утечка паролей или злоупотребление полномочиями могут привести к компрометации данных и нарушению безопасности.

Также существует риск отказа системы или программного обеспечения, который может привести к потере данных и прерыванию бизнес-процессов. Недостаточная защита от вирусов и других угроз может также привести к серьезным последствиям.

Для снижения рисков связанных с кибербезопасностью в финансовой сфере необходимо применять меры защиты, такие как шифрование данных, многофакторная аутентификация, мониторинг активности пользователей и обучение персонала правилам безопасности. Также важно иметь планы действий в случае кибератаки или других инцидентов, чтобы быстро реагировать и минимизировать ущерб [1, с. 173].

Целью данного исследования является анализ методов управления рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества, а также разработка рекомендаций по повышению эффективности управления рисками в данной области.

Для достижения данной цели были поставлены следующие задачи:

1. Изучение существующих подходов к управлению рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества.
2. Анализ применения различных технологий и методов защиты информации в управлении рисками.
3. Разработка рекомендаций по повышению эффективности управления рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества.

Для исследования темы "Управление рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества" использовались следующие методы: анализ научных статей и публикаций по теме, были проанализированы кейс-стади из прошлого, связанные с рисками в финансовой сфере.

Существует несколько подходов к управлению рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества:

1. Оценка рисков: Финансовые организации должны проводить оценку рисков, чтобы определить потенциальные угрозы и уязвимости своих систем и процессов. Оценка рисков позволяет организациям разработать стратегии по снижению рисков и улучшению безопасности.

2. Превентивные меры: Финансовые организации должны применять превентивные меры для защиты своих систем и данных от кибератак. Это может включать в себя шифрование данных, многофакторную аутентификацию, мониторинг активности пользователей и обучение персонала правилам безопасности.

3. Реагирование на инциденты: Финансовые организации должны иметь планы действий в случае кибератаки или других инцидентов, чтобы быстро реагировать и минимизировать ущерб. Это может включать в себя четкие процедуры по уведомлению клиентов и регуляторов, а также восстановление данных и систем.

4. Сотрудничество с другими организациями: Финансовые организации должны сотрудничать с другими организациями, такими как правительственные органы, регуляторы и другие финансовые организации, для обмена информацией о потенциальных угрозах и уязвимостях.

5. Обучение персонала: Финансовые организации должны обучать свой персонал правилам безопасности и проводить регулярные тренинги по обнаружению и предотвращению кибератак и финансовых мошенничеств.

Существует множество технологий и методов защиты информации, которые могут использоваться для управления рисками в финансовой сфере. Некоторые из них включают в себя [2]:

1. Шифрование данных: Шифрование данных является одним из наиболее эффективных методов защиты информации. Оно позволяет скрыть данные от неавторизованного доступа, используя математические алгоритмы для преобразования их в нечитаемый вид.

2. Многофакторная аутентификация: Многофакторная аутентификация требует от пользователей предоставления нескольких форм идентификации для получения доступа к системе. Это может включать в себя пароль, пин-код, отпечаток пальца или другие формы биометрической идентификации.

3. Мониторинг активности пользователей: Мониторинг активности пользователей позволяет выявлять необычную активность в системе, которая может указывать на кибератаку или другой инцидент безопасности.

4. Программное обеспечение для обнаружения вторжений: Программное обеспечение для обнаружения вторжений использует алгоритмы машинного обучения для выявления необычной активности в системе, которая может указывать на кибератаку или другой инцидент безопасности.

5. Физические меры безопасности: Физические меры безопасности, такие как видеонаблюдение, контроль доступа и биометрическая идентификация, могут быть использованы для защиты физических объектов, таких как серверные комнаты и хранилища данных.

6. Облачные технологии: Облачные технологии могут предоставлять более безопасное хранение данных и обеспечивать доступ к ним только авторизованным пользователям.

7. Обучение персонала: Обучение персонала правилам безопасности и проведение регулярных тренингов по обнаружению и предотвращению кибератак и финансовых мошенничеств является одним из наиболее эффективных методов защиты информации.

Для повышения эффективности управления рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества, можно рекомендовать следующие меры [3]:

1. Разработка стратегии безопасности: Разработка стратегии безопасности позволит определить основные риски и угрозы, а также выбрать соответствующие методы защиты информации.

2. Регулярное обновление программного обеспечения: Регулярное обновление программного обеспечения позволит устранять уязвимости и предотвращать кибератаки.

3. Внедрение системы мониторинга безопасности: Внедрение системы мониторинга безопасности позволит оперативно выявлять и предотвращать инциденты безопасности.

4. Создание команды по безопасности: Создание команды по безопасности позволит эффективно реагировать на инциденты безопасности и проводить регулярные аудиты системы безопасности.

5. Обучение персонала: Обучение персонала правилам безопасности и проведение регулярных тренингов по обнаружению и предотвращению кибератак и финансовых мошенничеств является одним из наиболее эффективных методов защиты информации.

6. Регулярное проведение тестирования на проникновение: Регулярное проведение тестирования на проникновение позволит выявлять уязвимости в системе безопасности и устранять их до того, как они будут использованы злоумышленниками.

7. Внедрение методов шифрования данных: Внедрение методов шифрования данных позволит защитить данные от неавторизованного доступа и предотвратить утечку конфиденциальной информации.

8. Регулярное проведение анализа рисков: Регулярное проведение анализа рисков позволит определить новые угрозы и риски и принять соответствующие меры по их предотвращению.

Таким образом, управление рисками в финансовой сфере, включая кибербезопасность, риски взлома и финансовые мошенничества, является важной задачей для любой организации, занимающейся финансовой деятельностью. Реализация соответствующих мер позволит снизить риски и обеспечить безопасность финансовой деятельности.

Список литературы:

1. Звягин Л.С. Комплексная оценка безопасности функционирования моделей экономических систем // Экономика и управление: проблемы, решения. 2017. Т. 4. № 1. С. 18-25.
2. Рекомендации в области стандартизации Банка России (РС БР ИББС 2.5-2014) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» от 01.06.2014.
3. Пупенцова С., Колотов В. Экономическая безопасность и защита информации в эпоху цифровизации // Экономика и управление: научно-практический журнал. 2020. № 6. С. 172-177.

References:

1. Zvyagin L.S. Comprehensive assessment of the safety of the functioning of models of economic systems // Economics and management: problems, solutions. 2017. Vol. 4. No. 1. pp. 18-25.
2. Recommendations in the field of standardization of the Bank of Russia (RS BR IBBS 2.5-2014) "Ensuring information security of organizations of the banking system of the Russian Federation" dated 01.06.2014.

3. Pupentsova S., Kolotov V. Economic security and information protection in the era of digitalization // Economics and Management: a scientific and practical journal. 2020. No. 6. pp. 172-177.