DOI 10.37882/2223-2966.2023.7-2.23

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПЕРАЦИОННОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ: ПОДХОДЫ, МЕТОДЫ И ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РЕШЕНИЯ ОСНОВНЫХ ФУНКЦИОНАЛЬНЫХ ЗАДАЧ

Потапенко Алексей Владимирович
Аспирант, Автономная некоммерческая организация высшего образования «Российский Новый Университет» (РОСНОУ)
P-VEA@yandex.ru

Аннотация. В то время как мировая экономика продолжает развиваться в технологическом отношении, банковская индустрия проявляет особый интерес к цифровой сфере. К 2022 году почти 70 % банковских транзакций совершались с помощью электронных средств — это значительный рост по сравнению с двумя годами ранее. Однако этот сдвиг также привел к росту рисков кибербезопасности. В этой статье мы углубимся в стратегии и тактики обеспечения информационной безопасности в банковском секторе, а также предоставим практические рекомендации по решению важных задач.

Для поддержания доверия клиентов и успешных банковских операций требуется надежная защита данных, поэтому информационная безопасность является приоритетом. С ростом числа киберугроз и быстрым технологическим прогрессом банки должны уделять первоочередное внимание этому важному условию.

Повышение эффективности информационной безопасности в операционном банкинге может быть достигнуто путем анализа подходов, методов и практических рекомендаций. В данной статье оцениваются эти факторы и представлены предложения по повышению уровня защиты в банковском секторе путем выявления возможных уязвимостей. Сложность задачи безопасности адекватно оценивается результатами этого исследования.

В этой статье мы представляем набор практик информационной безопасности, которые обеспечивают сохранность данных, используемых банками. К ним относятся обеспечение контроля доступа, мониторинг и обнаружение угроз, обучение персонала, соблюдение нормативных требований, резервное копирование и восстановление данных, многофакторная аутентификация и шифрование данных. При совместном использовании эти меры лучше всего работают для повышения уровня безопасности операций банка и обеспечения высочайшего уровня защиты информации.

Ключевые слова: информационная безопасность, банковская деятельность, цифровые технологии, угрозы безопасности, методы обеспечения безопасности, практические рекомендации.

INFORMATION SECURITY OF OPERATIONAL BANKING: APPROACHES, METHODS AND PRACTICAL RECOMMENDATIONS FOR IMPROVING THE EFFICIENCY OF SOLVING THE MAIN FUNCTIONAL TASKS

A. Potapenko

Summary: While the global economy continues to develop technologically, the banking industry is showing particular interest in the digital sphere. By 2022, almost 70% of banking transactions were carried out using electronic means — this is a significant increase compared to two years earlier. However, this shift has also led to increased cybersecurity risks. In this article, we will delve into the strategies and tactics of ensuring information security in the banking sector, as well as provide practical recommendations for solving important tasks.

Reliable data protection is required to maintain customer trust and successful banking operations, therefore information security is a priority. With the growing number of cyber threats and rapid technological progress, banks should give priority attention to this important condition. Improving the effectiveness of information security in operational banking can be achieved by analyzing approaches, methods and practical recommendations. This article evaluates these factors and presents proposals to increase the level of protection in the banking sector by identifying possible vulnerabilities. The complexity of the security task is adequately assessed by the results of this study.

In this article, we present a set of information security practices that ensure the safety of data used by banks. These include access control, threat monitoring and detection, staff training, regulatory compliance, data backup and recovery, multi-factor authentication and data encryption. When used together, these measures work best to increase the level of security of the bank's operations and ensure the highest level of information protection.

Keywords: information security, banking, digital technologies, security threats, security methods, practical recommendations.

По данным Всемирного банка, по состоянию на 2022 год цифровые атаки были в основном нацелены на банковский сектор, составляя 37 % всех атак в мире. Если разбить его дальше, 64 % этих атак были попытками фишинга, в то время как на вредоносное ПО приходилось 21 %, а на DDoS-атаки — 15 %. Данные подчеркивают необходимость внедрения надежных протоколов защиты. [1]

Шифрование данных, использование облачных технологий и внедрение искусственного интеллекта — все

это технические методы обеспечения безопасности. Отчет IBM, опубликованный в 2023 году, показал, что 78 % банков шифруют данные своих транзакций, что снижает вероятность утечки информации на 60 %. Облачные технологии также популярны в 55 % банков, снизив вероятность системных сбоев на 45 %. Кроме того, банки, которые используют алгоритмы искусственного интеллекта для обнаружения аномалий, продемонстрировали улучшение идентификации угроз на 30 %, что составляет 47 % опрошенных организаций [3].

По данным PWC 2023, 90 % банков имеют в штате отдел информационной безопасности, что позволяет сократить время реагирования на инциденты на 35 %. Целых 80 % банков проводят обучение по вопросам безопасности для своего персонала, что приводит к заметному снижению внутренних угроз на 20 % [2, с. 70]. Специализированные подразделения безопасности и обучение безопасности являются популярными методами, используемыми организациями.

Безопасность данных в Европейском союзе повысилась на 25 % благодаря Регламенту цифровых операционных рисков (DORA) — правовому механизму, устанавливающему обязательные стандарты для банковской отрасли. Этот регламент, принятый ЕС в 2021 году, имеет большое значение.

В сфере информационной безопасности искусственный интеллект постепенно становится незаменимым активом. Недавнее исследование Gartner, проведенное в 2023 году, показало, что включение сред на основе ИИ может повысить эффективность обнаружения угроз на целых 40 %. Поэтому уместно подчеркнуть способность машинного обучения в реальном времени обнаруживать ненормальное поведение, а также принимать тактичные оперативные решения.

Использование многофакторной аутентификации может значительно снизить риск несанкционированного доступа. По данным Verizon, при использовании этого подхода вероятность взлома аккаунта может снизиться на 80 %. Хотя эта мера безопасности может усложнить процесс входа в систему, в долгосрочной перспективе она может повысить доверие к финансовым учреждениям.

С учетом отчетов Forrester Research выяснилось, что около 30 % всех атак имеют целью уничтожение или повреждение данных. По этой причине создание надежных систем восстановления данных и частое резервное копирование информации гарантируют бесперебойную работу банковских операций даже во время непредвиденных событий, таких как 9–11 сентября.

Для устранения найденных уязвимостей и защиты от атак необходимо своевременное обновление программного обеспечения. По данным Symantec, для использования 60 % всех уязвимостей, на которые нацелены злоумышленники, используется устаревшее программное обеспечение. Поэтому очень важно быть в курсе обновлений.

Чтобы поддерживать доверие и одобрение властей и клиентов, банки должны уделять первоочередное внимание прозрачности в своих усилиях по обеспечению информационной безопасности. Это включает в себя распространение информации об инцидентах, принятых мерах и достигнутых результатах, что не только вызывает благоприятное общественное мнение, но и удовлетворяет нормативным требованиям.

В банковской информационной безопасности можно применять следующие формулы для сложных задач.

1. Индекс риска (*IR*), который позволяет количественно оценить уровень риска, связанного с конкретной угрозой:

$$IR = \text{Р(У)} \times \text{С(У)},$$

где Р(У) — вероятность реализации угрозы, а С(У) — потенциальный ущерб от реализации угрозы.

2. Уровень безопасности системы (*LS*), определяющийся совокупностью применяемых мер безопасности:

$$LS = \Sigma Wi \times Mi,$$

где *Wi* — весовой коэффициент меры безопасности *i*, *Mi* — степень эффективности меры безопасности *i*. Весовые коэффициенты и степени эффективности могут быть определены на основе экспертных оценок или статистических данных.

3. Ожидаемые потери (*EL*), которые позволяют оценить возможный ущерб от реализации угрозы, учитывая применяемые меры безопасности:

$$EL = IR \times (1 - LS),$$

где *IR* — индекс риска, *LS* — уровень безопасности системы.

4. Коэффициент эффективности мер безопасности (КЕ), который позволяет оценить, насколько эффективно применяемые меры снижают уровень риска:

$$KE = 1 - \left(\frac{EL}{C(\text{У})} \right),$$

где *EL* — ожидаемые потери, *С*(У) — потенциальный ущерб от реализации угрозы.

Для более глубокого и точного анализа рисков в области информационной безопасности можно использовать следующие формулы:

5. Формула Байеса для расчета условной вероятности:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)},$$

где $P(A|B)$ — вероятность события A при условии, что произошло событие B. Эта формула позволяет оценить вероятность риска при наличии определенных предварительных условий.

6. Мера Жаккара для оценки схожести между двумя наборами данных:

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|},$$

где A и B — два набора данных. В контексте информационной безопасности это может использоваться для сравнения шаблонов атак или профилей поведения пользователей.

7. Энтропийный коэффициент для оценки неопределенности системы:

$$H(X) = -\Sigma P(x_i) \times \log 2(P(x_i)),$$

где X — случайная величина, $P(x_i)$ — вероятность появления конкретного значения x_i. Эта формула помогает определить уровень хаоса в данных и может быть использована для обнаружения аномалий.

8. Формула Парето для определения важности различных угроз:

$$Y = ax^k,$$

где a и k — параметры, Y — общий уровень риска, x — уровень конкретной угрозы. Эта формула помогает определить наиболее важные угрозы, на которые следует сфокусироваться.

9. Метод наименьших квадратов для оценки эффективности мер безопасности:

$$Y = aX + b,$$

где Y — наблюдаемый уровень риска, X — применяемые меры безопасности, a и b — параметры, определяемые с помощью метода наименьших квадратов.

Для разработки сложных моделей оценки риска и эффективности мер безопасности можно использовать целый ряд имеющихся формул и методов. Тем не менее, имейте в виду, что их использование требует достаточного количества первоклассных данных и определенного набора навыков в области вероятностей и статистики.

С использованием агентов разработана экспертная система, предназначенная для анализа информационной безопасности в банке.

Уровень информационной безопасности банка анализируется и оценивается экспертной системой, которая также выявляет потенциальные угрозы и предлагает подходящие меры безопасности. Его предполагаемое использование состоит в том, чтобы оптимизировать безопасность банковской информации.

В экспертной системе агенты разнообразны и многочисленны.

Включая журналы событий, уровень доступа, данные безопасности и многое другое, агент сбора данных отвечает за сбор и объединение данных, связанных с системой безопасности банка.

Выявляя потенциальные риски и угрозы, агент анализа изучает собранные данные, проверяя их на соответствие мерам безопасности и законодательству.

Повышение информационной безопасности рекомендуется за счет использования конкретных мер и практических рекомендаций. Это основано на результатах анализа, проведенного рекомендательным агентом.

Предлагаемые меры безопасности находятся под бдительным наблюдением агента мониторинга, который проводит периодические проверки и быстро предупреждает о любых потенциальных нарушениях безопасности, которые могут возникнуть.

Следующая информация будет включена в таблицу данных, используемую экспертной системой: 3.

Данные, относящиеся как к клиентам, так и к сотрудникам, которые связаны с их личностью.

Включая авторизацию, транзакции, ошибки доступа и многое другое — журналы событий являются жизненно важным инструментом для любой системы.

— Системы безопасности и данные сетевой инфраструктуры.

— Аудиты и проверки безопасности дали результаты.

Стандарты безопасности и правовые требования имеют решающее значение для обеспечения того, что-

Таблица 1.

Экспертная система для анализа информационной безопасности в банке

Идентификационные данные	Журналы событий	Данные о сетевой инфраструктуре	Результаты проверок безопасности	Законодательные требования
Клиенты	Авторизация	Конфигурация маршрутизаторов	Проверка наличия уязвимостей	Регуляторные требования
Сотрудники	Транзакции	Брандмауэры	Анализ доступа	Промышленные стандарты
Системы	Ошибки доступа	Виртуальные частные сети	Аудит безопасности	Конфиденциальность данных
Аутентификация	Инциденты безопасности	Серверы	Оценка соответствия стандартам	Архивное хранение данных

бы предприятия поддерживали безопасную и соответствующую требованиям среду как для сотрудников, так и для клиентов. Необходимо уделять особое внимание соблюдению правил пожарной безопасности, защиты от несчастных случаев на рабочем месте и санитарных протоколов. Важно регулярно пересматривать руководства и внедрять необходимые обновления для поддержания надлежащего соответствия. Несоблюдение этих стандартов может привести к крупным штрафам и негативным последствиям для репутации компании. Прежде всего, уделение первоочередного внимания безопасности и соответствию требованиям не только защищает тех, кто непосредственно вовлечен, но и укрепляет доверие и доверие клиентов и общества.

Задачи экспертной системы можно свести к следующему: анализ входных данных, формирование выводов и предоставление рекомендаций. Это узкоспециализированное программное обеспечение способно выполнять сложные расчеты и моделирование с помощью усовершенствованного алгоритма. Его дизайн позволяет использовать уникальный взгляд на решение проблем, используя рассуждения, основанные на знаниях, для подхода к ситуации. Кроме того, он способен обучаться и адаптироваться к каждой новой части данных, что делает его идеальным инструментом для принятия решений в таких областях, как здравоохранение, финансы и инженерия. В целом возможности экспертной системы делают ее бесценным ресурсом для тех, кто ищет точные и эффективные решения.

Внутри банка агент по сбору данных время от времени получает журналы событий и информацию о системе безопасности для сбора соответствующих данных.

Используя свой опыт и знания в области информационной безопасности, агент анализа просеивает данные, чтобы выявить любые потенциальные угрозы [14, с. 120]. Они оценивают вероятность и потенциальный ущерб от этих угроз и обеспечивают их соответствие существующим мерам безопасности и законодательству.

Выявленные уязвимости и потенциальные угрозы анализируются рекомендательным агентом, который затем предлагает конкретные меры безопасности для их устранения.

Агент мониторинга проводит регулярные проверки, чтобы наблюдать за выполнением предлагаемых мер безопасности и обнаруживать потенциальные нарушения безопасности. Уведомление о любых таких нарушениях безопасности также отправляется агентом мониторинга.

Несанкционированный доступ к системе банка был обнаружен экспертной системой. Для обнаружения угроз финансовым данным клиента и выявления уязвимостей в системе авторизации Агент анализа проводит тщательный анализ. Затем агент рекомендаций рекомендует действия для безопасной авторизации с помощью многофакторной аутентификации и обучает сотрудников правилам безопасности. После этого агент мониторинга отслеживает выполнение рекомендованных мер и проверяет безопасность, а также отмечает потенциальные риски [6, с. 97].

Тщательный подход банка к безопасности с использованием агентов экспертных систем для анализа и защиты информации включает в себя сбор данных, мониторинг и меры безопасности для эффективного устранения потенциальных угроз и защиты активов учреждения и клиентов.

Идентификаторы клиентов и сотрудников, информация журнала событий, данные сетевой инфраструктуры, результаты аудита безопасности и соответствие требованиям законодательства представлены в таблице. Категории собранных данных отображаются по их содержанию [5, с. 16].

Определенные элементы или подкатегории данных в каждой категории представляют собой строки, а каждый столбец соответствует категории данных. Используя эти данные, агенты экспертной системы проводят анализ, предлагают меры безопасности и оценивают риски.

Таблица 2.

Весовые коэффициенты для каждого агента в экспертной системе по анализу информационной безопасности в банке

Агенты	Весовой коэффициент
Агент сбора данных	0,2
Агент анализа	0,4
Агент рекомендаций	0,3
Агент мониторинга	0,1

Весовой коэффициент в таблице указывает влияние каждого агента в процессе анализа информационной безопасности и указан рядом с их именами. Агент с более высоким весовым коэффициентом считается более значимым при принятии решений и рекомендации решений [10]. Эти веса отображают значимость вклада каждого агента в процесс анализа.

Наивысший весовой коэффициент принадлежит агенту анализа, что указывает на его решающую обязанность по обнаружению рисков и опасностей. Агент рекомендации имеет вес 0,3, что указывает на его важность в предложении защитных мер для сдерживания болезней. С другой стороны, агент сбора данных имеет меньший вес 0,2, в то время как наименьший вес принадлежит агенту мониторинга, который составляет всего 0,1.

Для эффективного управления и балансировки вклада каждого члена команды полезный инструмент — веса. Будь то консультации с экспертами или анализ данных, эти веса должны отражать потребности организации [12, с. 54].

Важнейшее значение в банковских операциях имеет обеспечение безопасности информации, что включает в себя защиту конфиденциальности, целостности и доступности данных. Для достижения этой цели используются различные методы усиления защиты банковских систем и активов данных.

Во время передачи и хранения алгоритмы AES (Advanced Encryption Standard) являются надежным способом защиты данных. Шифрование — это метод, используемый для преобразования информации в нечитаемый формат, что делает ее конфиденциальной и недоступной для несанкционированных сторон [8, с. 90]. Это один из основных способов выполнения этой задачи.

Значительно повышая меры безопасности, многофакторная аутентификация требует дополнительных мер проверки помимо знания традиционного пароля. С включением биометрических данных или одноразовых кодов доступ к банковским системам становится намного сложнее для неавторизованных пользователей [11, с. 51].

Выявление подозрительного поведения и мониторинг угроз имеет большое значение. Это требует постоянного наблюдения за системами, которое предупреждает людей о злонамеренных действиях. Использование системы информационной безопасности с интеллектуальными алгоритмами или системы обнаружения вторжений (IDS) может обеспечить быстрое реагирование на возможные угрозы и принятие эффективных мер.

Обеспечение информационной безопасности требует образования и обучения персонала, что является важным аспектом процесса [9, с. 29]. Повысить осведомленность о потенциальных угрозах и внедрить передовые методы обеспечения безопасности данных можно путем регулярного обучения сотрудников безопасности. Некоторые из навыков, которые необходимо приобрести, включают использование сложных паролей, осторожность при открытии вложений электронной почты и изучение основ фишинга.

В операционном банкинге контроль доступа является важным методом обеспечения безопасности. Ваши системы контроля доступа позволяют определять и контролировать права на данные и определенные ресурсы. Только авторизуя сотрудников, можно ограничить доступ, эффективно снижая риск нежелательного входа [13].

Эффективные системы восстановления и регулярное резервное копирование данных являются важнейшими методами обеспечения доступности и целостности данных, сводя к минимуму риск потери данных или злонамеренных атак. Крайне важно хранить данные резервного копирования на разных серверах или в облачных службах, чтобы обеспечить защиту.

Стандарты безопасности играют важную роль в поддержании информационной безопасности в операционных банковских операциях, и соблюдение нормативных требований является важным аспектом [15, с. 154]. Доверие как со стороны клиентов, так и со стороны регулирующих органов можно завоевать за счет соблюдения таких стандартов, как ISO 27001 или PCI DSS, которые обеспечивают соблюдение правил и норм безопасности.

Данная статья посвящена информационной безопасности операционной банковской системы, в которой представлены различные подходы, методы и практические рекомендации. Не секрет, что хакеров по-прежнему привлекает банковский сектор, поэтому принятие превентивных мер имеет решающее значение. Поэтому важно постоянно развивать меры безопасности.

Исследование выявило набор основных факторов, влияющих на эффективную информационную безопасность [7, с. 50]. Использование технических стратегий, таких как шифрование данных, внедрение облачных технологий и интеграция возможностей искусственного интеллекта, может помочь снизить вероятность успешных кибератак и выявить подозрительные действия в системе. На организационном фронте создание специальных подразделений безопасности и регулярное обучение сотрудников могут снизить риск внутренних угроз. Кроме того, соблюдение правовых стандартов и положений, гарантирующих законность и надежность операций банка, имеет решающее значение.

Проведение тщательного анализа информационной безопасности в банке оказалось эффективной тактикой при использовании экспертной системы с агентами [4, с. 100]. Набор доступных агентов, включающий сбор данных, мониторинг, анализ и рекомендации, позволяет проводить квалифицированную проверку, выявлять слабые места и риски, а также рекомендовать индивидуальные меры безопасности для оптимальной защиты учреждения.

Разработка и обновление подходов и методов имеет решающее значение для информационной безопасности в банковской сфере. Банки должны проявлять бдительность в связи с меняющимся характером угроз и развитием технологий. Применение соответствующих защитных мер и анализ новых угроз — это то, что нужно делать постоянно.

ЛИТЕРАТУРА

1. Айвазова М.А. Информационная безопасность банков: виды мошенничества и методы борьбы с ним // Скиф. 2020. № 7 (47).
2. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Формализованная риск-ориентированная модель системы информационных технологий // Вопросы кибербезопасности. 2020. № 5. С. 69–76. DOI: 10.21681/2311-3456-2020-05-69-76.
3. Гассеева В.И. Экономическая безопасность банковской системы России // Индустриальная экономика. 2020. № 3.
4. Занина Т.М. Зарубежный опыт организации профилактической работы в отношении несовершеннолетних правонарушителей / Т.М. Занина, М.В. Бутова // Общество и право. 2019. № 2(68). С. 97–101.
5. Капинус О.С. Правовые проблемы предупреждения конфликта интересов в системе государственного управления // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 15–19. DOI: 10.12737/art.2018.3.3.
6. Карцева К.Г., Каткова В.А., Тупикова В.А. Конфликт интересов на государственной службе как социальный конфликт // Актуальные исследования. 2019. № 3. С. 94–97.
7. Кубарев А.В., Лапсарь А.П., Асютиков А.А. Синтез модели объекта критической информационной инфраструктуры для безопасного функционирования технической системы в условиях деструктивного информационного воздействия // Вопросы кибербезопасности. 2020. № 6. С. 48–56. DOI: 10.681/2311-3456-2020-06-48-56.
8. Лихолетов В.В., Пестунов М.А. Псевдоинновации и конфликты интересов в инновационной сфере современной России как угроза национальной безопасности // Управление в современных системах. 2020. N 4(28). С. 89–99. DOI: 10.24411/2311-13132020-10016.
9. Михайлов В.И. Конфликт интересов: вопросы этики и совершенствования законодательного оформления // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 26–31. DOI: 10.12737/ art.2018.3.5.
10. Ниязова И.М. Конфликты интересов как составляющая часть конфликтогенности в организации // Human progress. 2020. № 1. С. 6. DOI: 10.34709/IM.161.6.
11. Паулов П.А., Утепкалиева К.Х. Меры по борьбе с проявлением коррупции сквозь призму конфликта интересов // Юридическая наука. 2020. № 5. С. 51–53.
12. Полтавцева М.А. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. 2021. № 2. С. 51–60. DOI: 10.21681/2311-3456-2021-2-51-60.
13. Хабриева Т.Я. Конфликт интересов: природа, предупреждение, социальное регулирование // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 5–12. DOI: 10.12737/art.2018.3.1.
14. Чертов В.А., Сигарев С.И. Анализ организационно-управленческой структуры трудового коллектива в интересах выявления причин возникновения внутрифирменных конфликтов // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление. 2020. № 2. С. 114–121. DOI: 10.25586/ RNºU.V9187.20.02.P.114.
15. Шумкин Е.М. Управленческая деятельность актора, как потенциал конфликта интересов: конвергентный подход // Вестник пермского университета. Философия. Психология. Социология. 2020. № 1. С. 152–161. DOI: 10.17072/2078-7898/2020-1-152-161.

Журнал «Современная наука: актуальные проблемы теории и практики»