доктор технических наук, доцент
С. И. Козьминых

Профессор кафедры КБ-4
«Интеллектуальные системы информационной безопасности»
МИРЭА-Российский технологический университет

Профессор кафедры «Прикладной информатики
и информационной безопасности»
РЭУ им. Г.В. Плеханова

«Использование искусственного интеллекта для обеспечения информационной безопасности в банках»

Введение:

В современном мире финансовая сфера сталкивается с возрастающими вызовами в области информационной безопасности. Увеличение числа и сложности кибератак на банки требует внедрения инновационных подходов для защиты данных клиентов и предотвращения финансовых потерь. Искусственный интеллект (ИИ) предоставляет уникальные возможности для повышения уровня безопасности, предлагая автоматизацию процессов обнаружения и предотвращения угроз. Исследование применения ИИ в данной области становится актуальным в связи с необходимостью адаптации к новым вызовам цифровой эпохи.

Цель и задачи исследования

Целью данного исследования *является изучение возможностей и разработка модели использования технологий искусственного интеллекта для обеспечения информационной безопасности в банковской сфере.*

Задачи исследования *включают анализ существующих методов защиты, оценку потенциала ИИ в автоматизации процессов обнаружения и предотвращения угроз, а также предоставление рекомендаций по его интеграции в банковские системы.*

Анализ текущих угроз и кибератак на финансовые учреждения

История кибератак на финансовую сферу полна примеров, иллюстрирующих их разрушительные последствия. В 2016 году Центральный банк Бангладеш стал жертвой масштабной атаки, в результате которой злоумышленники похитили 81 миллион долларов США. Атака была осуществлена через систему SWIFT, что выявило уязвимость даже высокозащищенных межбанковских систем. В 2019 году Capital One подвергся атаке, в ходе которой были скомпрометированы персональные данные более 100 миллионов клиентов. Это событие не только нанесло финансовый ущерб, но и значительно подорвало доверие клиентов к компании. Эти инциденты подчеркивают необходимость улучшения методов защиты и внедрения инновационных технологий для предотвращения подобных ситуаций. Многие компании, включая российские, используют технологии искусственного интеллекта для снижения затрат и увеличения доходов, а также для оптимизации рабочих процессов и повышения производительности. Таким образом, применение таких технологий может стать одним из ключевых шагов в обеспечении безопасности в финансовой сфере.

Ограничения традиционных методов защиты данных

Традиционные методы защиты данных, несмотря на их долговременное использование, имеют ряд существенных недостатков, которые делают их менее эффективными в условиях современных киберугроз. Согласно отчету IBM Security за 2022 год, организациям требуется в среднем 287 дней для выявления и устранения утечек данных. Это свидетельствует о том, что традиционные подходы не способны оперативно реагировать на угрозы. Кроме того, исследование компании Accenture выявило, что 68% организаций сталкивались с потерей данных из-за использования устаревших технологий защиты. Это указывает на неспособность таких методов адаптироваться к новым вызовам. Прогнозы Cybersecurity Ventures утверждают, что к 2025 году ущерб от киберпреступности может достичь 10,5 триллионов долларов, что подтверждает необходимость пересмотра существующих подходов к обеспечению безопасности. Таким образом, традиционные методы защиты данных требуют модернизации и дополнения инновационными решениями, чтобы соответствовать современным требованиям.

Необходимость внедрения инновационных подходов

В банковском секторе «развитие инновационных подходов в развитии банковского сектора способствует совершенствованию сферы экономической и цифровой безопасности». Интеграция новых технологий в банковскую сферу может не только улучшить качество услуг, но и повысить общую безопасность финансовых операций, учитывая необходимость комплексного подхода к обеспечению защиты данных и предотвращению мошенничества.

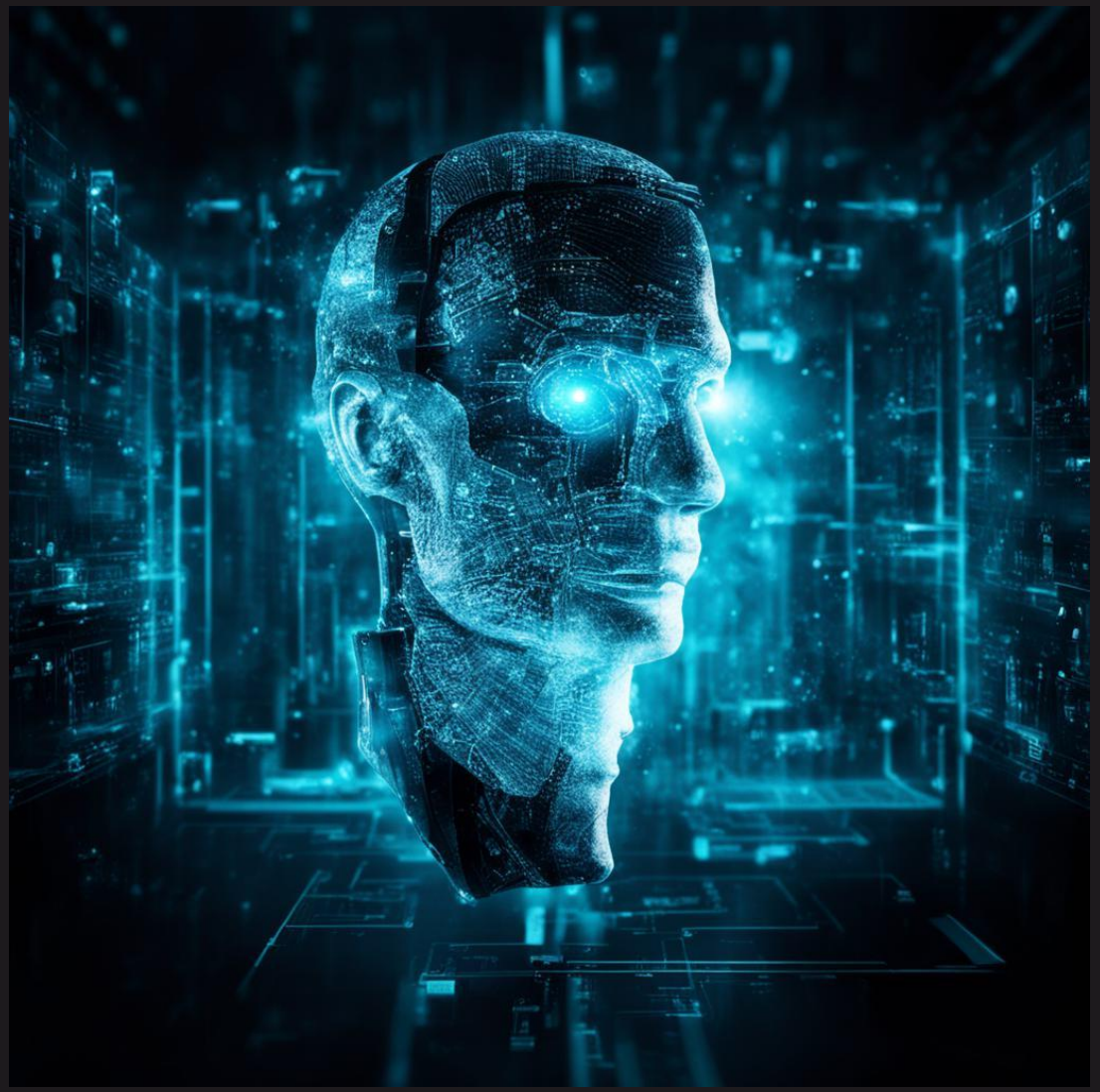
Основные технологии ИИ и их применение в кибербезопасности

Искусственный интеллект включает множество технологий, каждая из которых находит свое применение в сфере кибербезопасности. Машинное обучение представляет собой процесс, при котором алгоритмы обучаются на исторических данных для выявления закономерностей и аномалий. В банковском секторе это направление активно используется для анализа транзакций и обнаружения мошеннической активности. Компании, такие как IBM, разрабатывают решения, позволяющие обрабатывать большие объемы данных в реальном времени, что значительно ускоряет процесс принятия решений.

Основные технологии ИИ и их применение в кибербезопасности

Использование искусственного интеллекта в бизнес-процессах, позволяет ускорить обработку данных и снизить количество ошибок по сравнению с ручной обработкой, высвобождая ресурсы для выполнения более сложных задач. Глубокое обучение, являющееся подвидом машинного обучения, помогает моделировать сложные паттерны поведения, что способствует более точному предсказанию потенциальных угроз. Анализ больших данных предоставляет банкам возможность обрабатывать огромные массивы информации из различных источников, что, в свою очередь, способствует своевременному выявлению и предотвращению угроз безопасности.

Основные технологии ИИ и их применение в кибербезопасности



Технологии искусственного интеллекта играют ключевую роль в обнаружении угроз и предотвращении кибератак. Системы, такие как Darktrace, используют машинное обучение для анализа сетевого трафика и выявления аномалий, которые могут указывать на наличие угроз. Эти решения позволяют идентифицировать потенциальные атаки на ранних стадиях, что значительно снижает риски. Исследования продемонстрировали, что применение ИИ для анализа логов и сетевого трафика может сократить время обнаружения угроз на 96%, что подчеркивает его эффективность по сравнению с традиционными методами.

Обзор успешных кейсов использования ИИ в финансовой сфере

Одним из ярких примеров успешного применения искусственного интеллекта в банковской сфере является внедрение компанией JPMorgan Chase системы COiN (Contract Intelligence). Эта система, основанная на технологиях машинного обучения, предназначена для анализа финансовых документов с целью выявления потенциальных рисков. Благодаря COiN банку удалось автоматизировать процесс обработки информации, что сэкономило более 360 тысяч часов работы сотрудников ежегодно. Такой подход не только снижает затраты, но и минимизирует вероятность ошибок, связанных с человеческим фактором. С другой стороны, банк HSBC активно использует ИИ для обнаружения мошеннических операций. Система, анализирующая большие данные и применяющая методы машинного обучения, продемонстрировала значительные улучшения в точности выявления подозрительных транзакций. В результате количество ложных срабатываний снизилось на 20%, что повысило эффективность работы системы безопасности и доверие клиентов к банку.

Обзор успешных кейсов использования ИИ в финансовой сфере

Эффективность использования искусственного интеллекта для обеспечения безопасности банков подтверждается данными отчетов и практическими результатами. Согласно исследованию компании Capgemini 69% банков, внедривших ИИ в свои системы безопасности, отметили значительное снижение числа успешных кибератак. Это свидетельствует о способности ИИ не только обнаруживать, но и предотвращать угрозы. Примером служит опыт банка Barclays, где применение технологий ИИ позволило сократить время реакции на инциденты безопасности с нескольких часов до нескольких минут, что существенно повысило устойчивость системы и минимизировало возможные последствия атак. Кроме того, использование технологий машинного обучения и анализа больших данных в крупных международных банках значительно повышает эффективность финансовых операций. Таким образом, интеграция ИИ в банковские системы безопасности не только демонстрирует свою эффективность, но и становится необходимостью в современных условиях.

Обзор развития и регулирования ИИ

2019	Национальная стратегия развития искусственного интеллекта на период до 2030 г. (указ Президента № 490).
2020	Перспективная программа стандартизации по приоритетному направлению «Искусственного интеллект» на 2021-2024 г. Концепция развития регулирования отношений в сфере технологий ИИ и робототехники до 2024 г. (Распоряжение Правительства № 2129). Перечень поручений Президента РФ по итогам конференции «Путешествие в мир Искусственного интеллекта».
2021	Кодекс этики в сфер ИИ (Альянс в сфере ИИ).
2022	Начал работу Национальный цетр развития ИИ при Правительстве РФ.
2023	Регистрация первой в России межотраслевой системы добровольной сертификации в области ИИ (СДС Интеллометрика).

Обзор развития и регулирования ИИ

2024	Декларация об ответственной разработке и использовании сервисов на основе генеративного ИИ (приложение к Кодексу этики). Изменения к Национальной стратегии развития искусственного интеллекта на период до 2030 г. (Указ Президента № 124).
2025-2026	Актуализация Концепции развития регулирования отношений в сфере технологий ИИ и робототехники до 2024 г. (Распоряжение Правительства № 2129). Ожидается внесение изменений в УК в части наказания за использование ИИ при совершении преступлений. Ожидается дополнение в БДУ ФСТЭК новых угроз связанными с ИИ. Ожидается появление отраслевых рекомендаций для КФС. Ожидается внесение изменений в приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации не составляющей государственную тайну, содержащейся в государственных информационных. системах».

Преимущества ИИ перед традиционными методами

Искусственный интеллект (ИИ) демонстрирует значительное превосходство над традиционными методами в области обнаружения киберугроз благодаря высокой точности выявления угроз. Согласно отчету компании IBM, системы, использующие ИИ, достигают точности до 95%, что значительно превышает показатели традиционных методов, ограничивающихся 85%. Это связано с тем, что ИИ способен анализировать огромные объемы данных в режиме реального времени и выявлять аномалии, указывающие на потенциальные угрозы. Кроме того, исследование Гарвардского университета показало, что ИИ сокращает время обнаружения кибератак с 280 до 30 минут, что является значительным улучшением. Быстрая реакция на инциденты позволяет минимизировать последствия, особенно в банковской сфере, где каждая минута может быть критической.

Преимущества ИИ перед традиционными методами

Согласно данным аналитической компании Gartner, банки, использующие ИИ для обеспечения безопасности, сокращают операционные расходы на 30% по сравнению с организациями, применяющими традиционные методы. Это связано с автоматизацией процессов мониторинга и анализа, что снижает необходимость в ручной обработке данных. Исследование McKinsey также подтверждает эффективность этих технологий, показав, что внедрение ИИ позволяет сократить потери от кибератак на 40%. Это приводит к экономии в миллиарды долларов ежегодно. Таким образом, использование ИИ не только повышает уровень безопасности, но и способствует значительному снижению финансовых и временных затрат, что делает его привлекательным инструментом для банковской сферы.

Описание предлагаемой модели автоматизации процессов защиты данных

Предлагаемая модель автоматизации процессов защиты данных в банковских системах основывается на интеграции технологий искусственного интеллекта (ИИ) для повышения эффективности и быстродействия системы. Главным элементом структуры модели является модульный подход, где каждая функциональная часть системы отвечает за выполнение конкретных задач. Важным аспектом является то, что «роль искусственного интеллекта в цифровой трансформации банковской системы включает автоматизацию обслуживания клиентов, управление рисками и борьбу с финансовым мошенничеством». В модели предусмотрено взаимодействие между модулями анализа, мониторинга, аутентификации и управления угрозами, что обеспечивает комплексный подход к защите информации.

Интеграция ИИ в существующую инфраструктуру банков

Интеграция технологий искусственного интеллекта в банковскую инфраструктуру требует многоуровневого подхода, который охватывает модернизацию существующих систем, разработку новых решений и обучение персонала. Примером успешного внедрения ИИ служит инициатива Bank of America, реализованная еще в 2021 году, когда была внедрена система для анализа транзакций в реальном времени. Это позволило увеличить выявление мошеннических операций на 60%, что подчеркивает значительный потенциал применения ИИ в банковской сфере.

Интеграция ИИ в существующую инфраструктуру банков

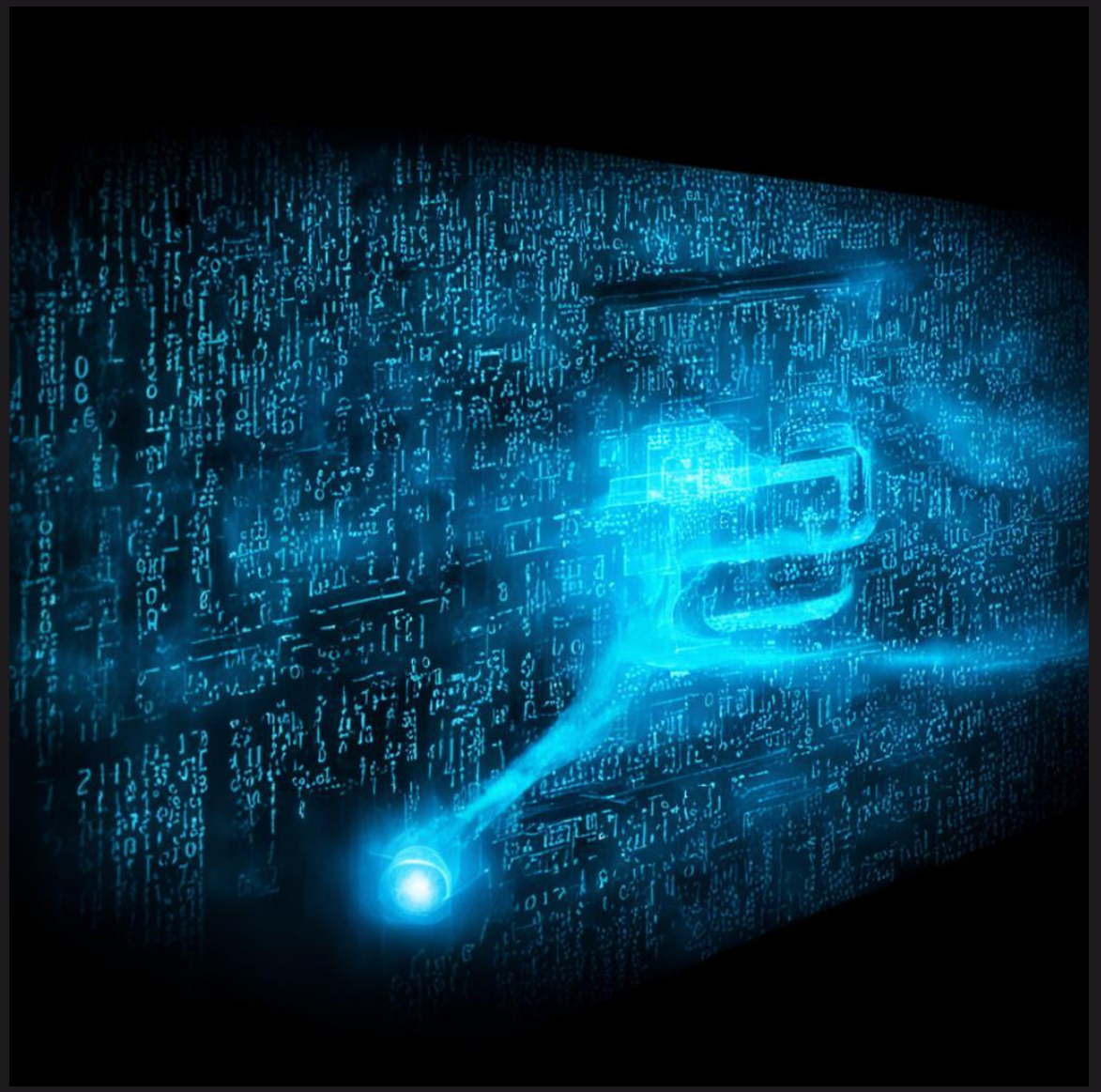
Ключевые этапы интеграции включают оценку текущих возможностей, разработку стратегии внедрения ИИ, а также тестирование и адаптацию новых технологий в реальных условиях. Такой подход помогает минимизировать риски и обеспечивает плавный переход к использованию ИИ в банковской инфраструктуре. Важным аспектом является подготовка специалистов, что подтверждается утверждением: «Ключевые направления подготовки: разработка и администрирование информационных систем для глобальных финансовых операций с использованием ИИ и квантовых технологий»

Методы оценки эффективности предложенной модели

Критерии оценки эффективности модели искусственного интеллекта в банковских системах безопасности играют ключевую роль в определении ее практической ценности. Одним из важнейших критериев является точность обнаружения угроз, которая позволяет минимизировать риски утечек данных и кибератак. Согласно отчету IBM Security, системы на базе ИИ способны значительно ускорить процесс выявления угроз, сокращая время их обнаружения на 96%. Это подтверждает высокую эффективность таких моделей в обеспечении безопасности банковских данных.

Методы оценки эффективности предложенной модели

Для оценки эффективности предложенной модели используются различные методы и инструменты анализа. Одним из наиболее распространенных является метод A/B тестирования, который позволяет сравнивать результаты работы системы с использованием ИИ и без него, обеспечивая объективную оценку влияния технологии на безопасность. В частности, внедрение ИИ в банке Bank of America привело к снижению числа ложных срабатываний на 80%, что подчеркивает значимость таких технологий.



Методы оценки эффективности предложенной модели

В дополнение к A/B тестированию, применение аналитических инструментов для мониторинга и анализа данных способствует выявлению слабых мест в системе и их устранению, что повышает общую надежность модели. Важно также учитывать, что «проанализированы международные стандарты и подходы – GDPR, проект Регламента ЕС об ИИ (EU AI Act), стандарт ISO/IEC 23894:2023. Эти нормативные акты создают основу для обеспечения безопасности и эффективности применения ИИ в различных сферах.

Рекомендации по адаптации ИИ для банковских учреждений

Внедрение искусственного интеллекта (ИИ) в банковскую систему представляет собой сложный, но необходимый процесс, требующий четко выработанных стратегий и последовательного подхода. Согласно отчету McKinsey, 60% банков уже активно используют технологии ИИ для повышения эффективности и безопасности своих операций. Первым шагом к успешной интеграции ИИ является определение ключевых областей, где его применение может принести наибольшую пользу, таких как анализ данных, автоматизация обработки информации и улучшение клиентского сервиса.

Рекомендации по адаптации ИИ для банковских учреждений

Например, банк JPMorgan Chase внедрил систему COiN, использующую ИИ для анализа юридических документов, что значительно сократило время обработки информации. Эти случаи подчеркивают важность инвестиций в разработку и адаптацию ИИ-решений, соответствующих специфическим потребностям банковской отрасли. Кроме того, использование чат-ботов на основе ИИ уже продемонстрировало свою эффективность, снизив затраты на обслуживание клиентов на 30%. Эти достижения показывают, что последовательное внедрение ИИ не только улучшает операции банков, но и способствует оптимизации расходов, что делает его неотъемлемой частью современной банковской системы.

Рекомендации по адаптации ИИ для банковских учреждений

Для адаптации ИИ в банковских учреждениях необходимо:
1. Определить целесообразность применения ИИ исходя из анализа рисков конкретных бизнес-процессов и категории обрабатываемой информации.
2. Оценить баланс между эффективность применения ИИ и ущербом от реализации рисков применения ИИ.

Рекомендации по адаптации ИИ для банковских учреждений

Для адаптации ИИ в банковских учреждениях необходимо:

1. Определить требования и рекомендации по применению ИИ.

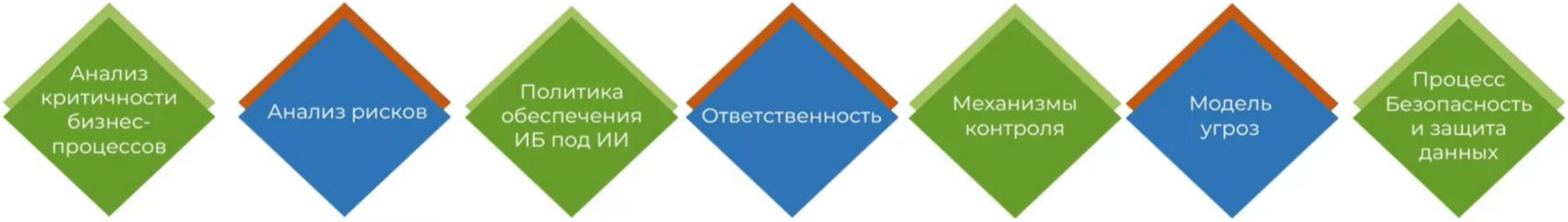
2. Не рекомендуется для объектов КФС использовать полностью автоматическое применение процедур генеративных и других моделей ИИ в случаях когда :

- риски от применения оцениваются как высокие или неприемлемые;

- результат принятия решения не может быть формально описан в виде алгоритма;

- технически не реализуемы требования законодательных актов по защите информации в отношении системы ИИ.

Этапы проектирования и разработки безопасной системы ИИ



Провести анализ критичности бизнес-функций, процессов и обрабатываемой информации, которые передаются на автоматическое исполнение с использованием технологий ИИ

Провести анализ рисков, включая риски информационной безопасности и определить приемлемость остаточных рисков

Доработка и разработка отдельной Политики обеспечения ИБ при применении технологий ИИ

Определить ответственных за организацию и контроль за реализацией Политики ИБ под ИИ

Документировать механизмы контроля за реализацией требований Политики ИБ под ИИ, в том числе с использованием средств мониторинга, аудита и информирования о ее соблюдении

Перед использованием технологий ИИ в процессах ФО рекомендуется разработать Модель угроз безопасности информации

В целях нейтрализации угроз безопасности ИИ при их разработке и использовании рекомендуется реализовать процесс «Безопасность и защита данных» (ГОСТ Р 71539-2024)

Политика безопасности ИИ

При формировании Политики безопасности ИИ необходимо соблюдать целевые свойства ИБ:

1. Целостность.

2. Конфиденциальность.

3. Доступность.

4. Киберустойчивость.

5. Прозрачность.

Принципы и политика безопасности ИИ

Принцип предоставления минимальных прав и полномочий

Принцип минимизации персональных данных, используемых для обучения

Процесс безопасной разработки на этапах жизненного цикла систем ИИ

Повышение осведомленности

Роли и ответственность

Соответствие («комплаенс»)

Реализация и последствия

ИБ при аутсорсинге и применении открытых моделей

Маркировка и уведомление

Сокращение объема сведений, разрешенных к распространению

Регистрация и реагирование на инциденты защиты информации

Планирование мероприятий по реагированию на нештатные ситуации

Пересмотр Политики

Основные угрозы безопасности технологий ИИ

1. Угроза нарушения функционирования «Обхода» средств, реализующих технологии ИИ.

2. Угроза модификации ИИ путем искажения «Отравления» обучаемых данных.

3. Угроза раскрытия информации о модели ИИ.

4. Угроза хищения обучаемых данных.

5. Угроза модификации модели ИИ, например путем внедрения бэкдоров (закладок).

6. Угроза приведения модели ИИ в состояние «отказ в обслуживании».

7. Угроза манипуляции поведения модели ИИ.

8. Угроза подмены модели ИИ.

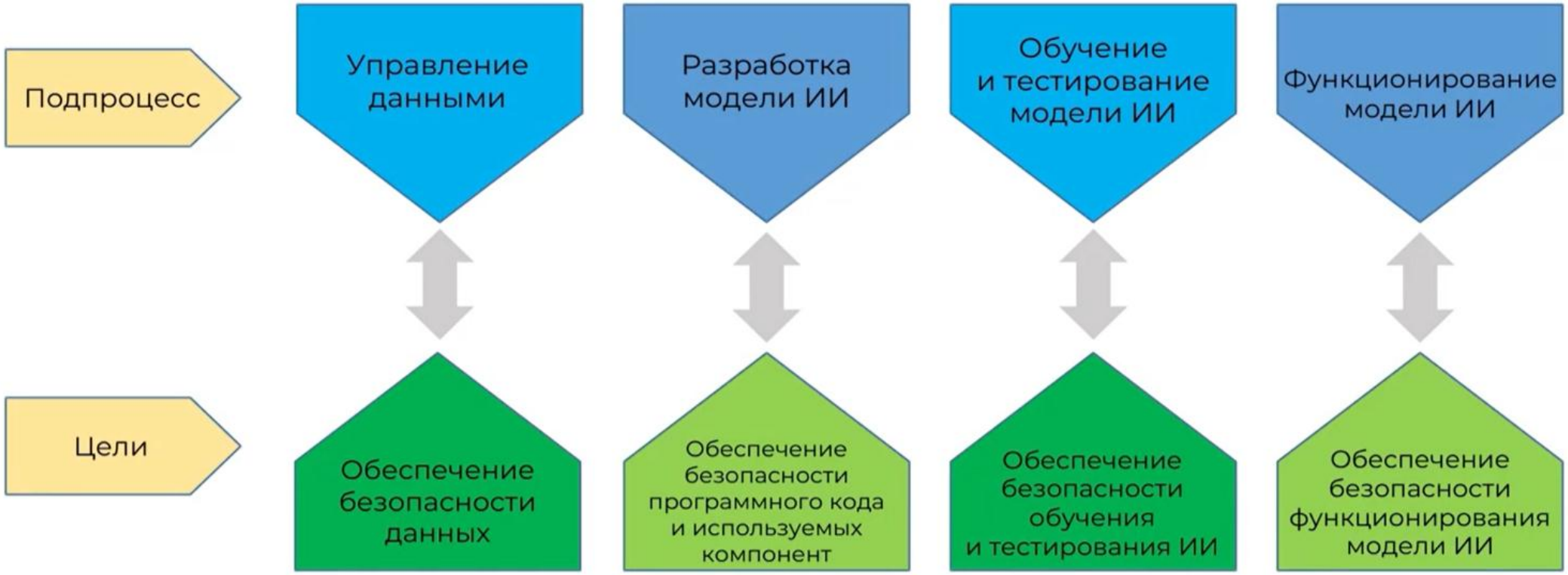
Способы реализации угрозы безопасности

1. ***Файзинг.*** *Генерация и ввод случайных входных данных.*
2. ***Внедрение бэкдора.*** *Внедрение злонамеренных закладок в код модели ИИ.*
3. ***Злонамеренная модификация алгоритма обучения модели ИИ.***
4. ***Извлечение данных.*** *Получение конфиденциальной информации из модели ИИ.*
5. ***Вредоносная инъекция.*** *Изменение поведения модели ИИ путем модификации или обхода системных инструкций с использованием специальных входных данных.*
6. ***Метод «губки».*** *Ввод вредоносных входных данных в целях нарушить функционирование ресурсов.*
7. ***Отравление обучающих данных.*** *Модификация набора обучающих данных в целях нарушения функционирования модели ИИ.*
8. ***«Состязательные атаки».*** *Вид атак с целью получения неверных выводов модели ИИ путем ввода искаженных данных.*

Риски информационной безопасности

1. Риски связанные с управлением данными.
2. Риски нарушения функционирования модели.
3. Рики отсутствия прозрачности модели.
4. Риски, связанные с поставщиками услуг и использование технологий ИИ с открытым кодом.
5. Риски нарушения способности финансовой организации поддерживать операционную устойчивость.

Процесс обеспечения информационной безопасности



*В соответствии с ГОСТ Р 71539-2024 (ИСО/МЭК 5338:2023). Национальный стандарт Российской Федерации. Искусственный интеллект. Процессы жизненного цикла системы искусственного интеллекта (утв. и введен в действие Приказом Росстандарта от 28.10.2024 N 1539-ст)

Процесс обеспечения информационной безопасности при управлении данными

1. Контроль и очистка аномальных данных в наборах обучающих и тестовых данных.
2. Шифрование защищаемой информации передаваемой за пределы контролируемой зоны.
3. Контроль целостности набора обучающих и тестовых данных.
4. Использование методов обезличивания персональных данных.
5. Использование метода гарантированного стирания данных при необходимости уничтожения набора обучающих и тестовых данных.

Процесс обеспечения информационной безопасности при обучении ИИ

1. Использование метода повышения устойчивости модели ИИ.
2. Использование протоколов конфиденциального вычисления.
3. Использование метода федеративного обучения.
4. Использование технологии маркировки выходных результатов работы систем ИИ.
5. Проведение ежегодного тестирования на проникновение и анализ уязвимостей для обеспечивающих систем.
6. Проведение тестирования на предмет «отравления» на этапе обучения и тестирования модели ИИ.
7. Периодическое дообучение модели ИИ.

Процесс обеспечения информационной безопасности при функционировании модели ИИ

1. Шифрование входных и выходных данных.

2. Контроль и очистка аномальных входных и выходных данных.

3. Регистрация событий, связанных с входными и выходными данными.

4. Ограничение параметров потока данных.

5. Определение показателей штатного функционирования модели ИИ и обеспечение их мониторинга.

Процесс обеспечения информационной безопасности при аутсорсинге ИИ

Варианты аутсорсинга:

- предоставление подготовленных наборов данных для обучения;

- предоставление модели ИИ и инфраструктуры ее размещения, но свои данные для обучения;

- полное использование системы ИИ поставщика услуг.

Основа и базовые рекомендации:

- Стандарт Банка России СТО БР ИББС -1.4-2018;

- Управление риском нарушения информационной безопасности.

Дополнительные рекомендации:

- оценка доверия для сторонних данных моделей ИИ;

- контроль целостности для сторонних данных и моделей ИИ на все цепочке поставки;

- обучение на очищенных, синтетических, обезличенных или специально подготовленных данных;

- в договоре - ответственность поставщика услуг в случае нарушения безопасности сервисов ИИ и обязательность по представлению информации о найденных уязвимостях и выявленных инцидентах ИБ.

Ожидаемые результаты и преимущества использования ИИ

Внедрение искусственного интеллекта (ИИ) в системы информационной безопасности банков обещает значительное улучшение их эффективности. Исследование McKinsey указывает на то, что применение ИИ может сократить затраты на безопасность до 30%, что делает его не только эффективным, но и экономически целесообразным решением. По данным IBM, системы ИИ способны сократить время обнаружения угроз с нескольких дней до нескольких минут, что существенно повышает оперативность реагирования на инциденты. Таким образом, использование ИИ не только улучшает защиту от киберугроз, но и оптимизирует процессы управления безопасностью в банках.

Будущее развитие технологий ИИ в финансовой безопасности

В 2021 году 40% организаций финансового сектора начали использовать ИИ для выявления угроз и управления рисками, что подчеркивает растущую значимость этих технологий в предотвращении кибератак и минимизации рисков. Одним из ключевых направлений является разработка систем анализа транзакций в реальном времени. Например, компании, такие как JPMorgan Chase, внедряют ИИ для обработки больших объемов данных, что позволяет снизить случаи мошенничества на 30%. Эти достижения демонстрируют потенциал ИИ в создании более защищенной и устойчивой финансовой системы. В частности, «были построены регрессионные модели, позволяющие оценить влияние внедрения ИИ-технологий на ключевые показатели эффективности финансовых организаций».

Вывод:

Применение искусственного интеллекта в области информационной безопасности банков имеет важное значение, так как позволяет существенно повысить устойчивость банковских систем к кибератакам. Технологии ИИ обеспечивают более высокую точность и скорость обнаружения угроз по сравнению с традиционными методами, что снижает вероятность успешных атак и минимизирует финансовые потери. Кроме того, использование ИИ способствует оптимизации затрат на обеспечение безопасности, что является важным аспектом для банковских учреждений.

СПАСИБО ЗА ВНИМАНИЕ