Беляев Сергей Николаевич, курсант
КВВУ им. С.М. Штеменко
Belyaev Sergey Nikolaevich
KVVU named after S.M. Shtemenko

Гизатуллин Александр Маратович, курсант
КВВУ им. С.М. Штеменко
Gizatullin Alexander Maratovich
KVVU named after S.M. Shtemenko

Новиков Назар Алексеевич, курсант
КВВУ им. С.М. Штеменко
Novikov Nazar Alekseevich
KVVU named after S.M. Shtemenko

Баданин Константин Александрович, преподаватель
КВВУ им. С.М. Штеменко
Badanin Konstantin Aleksandrovich
KVVU named after S.M. Shtemenko

Синицын Юрий Юрьевич, преподаватель
КВВУ им. С.М. Штеменко
Sinitsyn Yuri Yurievich
KVVU named after S.M. Shtemenko

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПО ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

FEATURES OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE CAPABILITIES TO BUILD A SYSTEM FOR PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS IN PERSONAL DATA INFORMATION SYSTEMS

Аннотация. В статье рассматриваются современные тенденции использования искусственного интеллекта (ИИ) в сфере аудита информационной безопасности. Рассмотрены существующие методы защиты данных, такие как шифрование и использование биометрии, и предложено использование искусственного интеллекта, таких как когнитивный анализ и машинное обучение. Описаны преимущества использования ИИ для защиты данных, такие как скорость и эффективность обработки информации и возможность дополнять существующие методы защиты. В целом, статья подчеркивает важность защиты данных и перспективы использования искусственного интеллекта для этой цели.

Abstract. The article discusses current trends in the use of artificial intelligence (AI) in the field of information security audit. It reviews existing data protection methods, such as encryption and the use of biometrics, and proposes the use of artificial intelligence, such as cognitive analysis and machine learning. The advantages of using AI for data protection are described, such as the speed and efficiency of information processing and the ability to complement existing protection methods. Overall, the article emphasizes the importance of data protection and the prospects for using artificial intelligence for this purpose.

Ключевые слова: Уязвимости, кибербезопасность, нейронные сети, искусственный интеллект (ИИ), обнаружение атак, сетевая безопасность, веб-приложения.

Keywords: Vulnerabilities, cybersecurity, neural networks, artificial intelligence (AI), attack detection, network security, web applications.

Введение

В современном цифровом мире защита информации становится одной из приоритетных задач для организаций, обрабатывающих персональные данные. Рост объемов данных и усложнение кибер-угроз требуют внедрения передовых технологий, среди которых особое место занимает искусственный интеллект (ИИ). Использование ИИ в системах защиты информации позволяет повысить эффективность обнаружения угроз, автоматизировать реагирование и минимизировать риски несанкционированного доступа.

1. Общие понятия и актуальность использования ИИ в информационной безопасности

1.1. Что такое искусственный интеллект в контексте информационной безопасности?

Искусственный интеллект – это совокупность методов и технологий, позволяющих автоматизировать процессы анализа данных, выявления аномалий и принятия решений на основе машинного обучения, нейронных сетей и других алгоритмов.

В области информационной безопасности ИИ используется для:

1. обнаружения аномалий в сетевом трафике;
2. распознавания вредоносных программ;
3. автоматического реагирования на инциденты;
4. оценки уязвимостей систем.

1.2. Актуальность использования ИИ при защите персональных данных

Обработка персональных данных требует соблюдения строгих нормативных требований (например, GDPR, ФЗ-152). Нарушения могут привести к серьезным штрафам и утрате доверия клиентов. В связи с этим системы защиты должны быть максимально эффективными и адаптивными.

ИИ позволяет:

1. своевременно выявлять попытки несанкционированного доступа;
2. автоматизировать мониторинг и аудит;
3. минимизировать человеческий фактор.

2. Особенности применения ИИ для построения системы защиты информации

2.1. Обнаружение аномалий и угроз

Использование методов машинного обучения позволяет обучать модели на исторических данных о нормальной работе системы и выявлять отклонения, которые могут свидетельствовать о попытках взлома или утечки данных.

Пример: нейронные сети анализируют сетевой трафик и выявляют необычные паттерны, характерные для атак типа "отказ в обслуживании" или "фишинг".

2.2. Автоматизация реагирования на инциденты

ИИ-системы могут автоматически блокировать подозрительные соединения или процессы, что значительно ускоряет реакцию на угрозы без необходимости вмешательства человека.

Пример: системы на базе ИИ могут автоматически отключать учетные записи при обнаружении подозрительной активности.

2.3. Анализ уязвимостей и предсказание рисков

Модели машинного обучения помогают предсказывать возможные уязвимости системы на основе анализа текущего состояния инфраструктуры и исторических данных о атаках.

2.4. Обеспечение соответствия нормативным требованиям

ИИ может автоматизировать процессы аудита и составления отчетов по соблюдению требований законодательства по защите персональных данных.

Введение в искусственный интеллект в области кибербезопасности

Основная цель применения искусственного интеллекта в области кибербезопасности заключается в повышении эффективности и точности защиты информации. ИИ способен обрабатывать и анализировать большие объемы данных, выявлять нестандартные и скрытые угрозы, оперативно реагировать на инциденты безопасности и принимать предупреждающие меры. Благодаря автоматизации процессов исследования и обнаружения уязвимостей, искусственный интеллект значительно сокращает время реакции на потенциальные угрозы и улучшает качество работы системы защиты информации.

Одним из ключевых способов применения искусственного интеллекта для защиты информации в информационных системах персональных данных является разработка алгоритмов машинного обучения для создания персонализированных систем безопасности. ИИ может адаптировать стратегии защиты в соответствии с поведением каждого конкретного пользователя, учитывая его предпочтения и особенности работы с данными. Такой подход к обеспечению безопасности позволяет повысить эффективность защиты информации и уменьшить вероятность успешных атак на информационные системы.

Основные принципы защиты информации в информационных системах

Первым и одним из основных принципов защиты информации является принцип минимизации доступа. Это означает, что каждый пользователь или система должны иметь доступ только к необходимой им информации и функционалу. Используя возможности искусственного интеллекта, система может автоматически управлять правами доступа, ограничивая их в соответствии с установленными политиками безопасности.

Вторым важным принципом является принцип мониторинга и обнаружения инцидентов. С помощью технологий искусственного интеллекта система может проводить непрерывный мониторинг активности пользователей, сетевого трафика и защитных мер, выявляя потенциальные угрозы и несанкционированные действия. Это позволяет оперативно реагировать на инциденты и предотвращать утечку конфиденциальной информации.

Третий принцип – это принцип шифрования данных. Использование шифрования позволяет защитить данные от несанкционированного доступа даже в случае утечки информации или нарушения целостности системы. Используя алгоритмы шифрования и технологии искусственного интеллекта, система может эффективно защитить данные как в покое, так и в процессе передачи и обработки.

В заключение, основные принципы защиты информации в информационных системах, особенно содержащих персональные данные, требуют комплексного подхода и использования современных технологий, включая возможности искусственного интеллекта.

Применение искусственного интеллекта для обеспечения безопасности персональных данных

Одним из основных способов применения искусственного интеллекта для обеспечения безопасности персональных данных является создание систем мониторинга и обнаружения аномалий. Алгоритмы машинного обучения и нейронные сети позволяют анализировать трафик данных в режиме реального времени и выявлять подозрительное поведение или необычные паттерны, что может свидетельствовать о возможной угрозе безопасности. Благодаря искусственному интеллекту системы могут автоматически реагировать на обнаруженные угрозы и принимать меры по их предотвращению.

Другим способом применения искусственного интеллекта является усовершенствование методов аутентификации и идентификации пользователей. Биометрические технологии, такие как распознавание лиц, голоса или отпечатков пальцев, в сочетании с искусственным интеллектом позволяют создать более надежные системы идентификации, исключающие возможность несанкционированного доступа к данным даже при украденных учётных данных.

Таким образом, применение возможностей искусственного интеллекта в системах защиты информации от несанкционированного доступа в информационных системах персональных данных позволяет повысить уровень безопасности и эффективности защиты личной информации

Технологии и инструменты искусственного интеллекта в борьбе с несанкционированным доступом

Одним из основных применений искусственного интеллекта в области защиты информации является использование машинного обучения для создания систем, способных обнаруживать аномальное поведение пользователей. Алгоритмы машинного обучения могут анализировать обычные паттерны активности и идентифицировать отклонения, которые могут свидетельствовать о несанкционированном доступе.

Другим инновационным подходом является применение нейронных сетей для анализа трафика в сети и выявления потенциальных угроз. Нейронные сети способны детектировать аномалии и атаки, которые могут остаться незамеченными более традиционными методами защиты. Благодаря своей способности к самообучению, нейронные сети могут адаптироваться к новым видам угроз и обеспечивать непрерывный мониторинг без необходимости постоянного вмешательства человека.

Важным элементом защиты персональных данных с помощью ИИ является анализ больших данных и создание прогностических моделей. Эти модели позволяют предсказывать потенциальные уязвимости и определять наиболее эффективные стратегии обеспечения безопасности персональных данных на основе исторических данных и данных о текущих угрозах.

Таким образом, технологии и инструменты искусственного интеллекта играют важную роль в обеспечении безопасности персональных данных и предотвращении несанкционированного доступа в информационных системах.

Актуальность проблемы защиты информации

Защита персональных данных стала одной из ключевых задач в условиях растущего числа кибератак, утечек информации и злоупотреблений с личными данными. По данным Международного фонда защиты данных, в 2020 году произошло более 4000 кибератак, из которых более 60% были нацелены на утечку персональных данных.

Искусственный интеллект как средство защиты информации

Искусственный интеллект охватывает широкий спектр технологий, включая машинное обучение, нейронные сети и обработку естественного языка. Применение ИИ в системах защиты информации позволяет значительно повысить их эффективность. Например, алгоритмы машинного обучения могут анализировать паттерны поведения пользователей, выявлять аномалии и предупреждать о возможных угрозах.

Анализ поведения пользователей

Одним из самых успешных методов использования ИИ является анализ поведения пользователей (User Behavior Analytics, UBA). Системы UBA собирают данные о действиях пользователей в реальном времени и создают их профиль. На основе обычного поведения системы могут автоматически идентифицировать отклонения, такие как необычные попытки входа или запросы на доступ к конфиденциальной информации.

Повышение уровня аутентификации

Другим важным аспектом является многофакторная аутентификация (MFA). Использование ИИ позволяет улучшить этот процесс. Алгоритмы могут автоматически определять контекст запроса на доступ и на основе анализа данных о пользователе предлагать различные уровни аутентификации. К примеру, если пользователь пытается войти из нового местоположения или с незнакомого устройства, система может запросить дополнительные подтверждения.

Интеллектуальные системы также могут использовать биометрические данные, такие как отпечатки пальцев или распознавание лиц, для повышения уровня безопасности. ИИ-технологии позволяют автоматизировать этот процесс и сделать его более безопасным и удобным для пользователей.

Совершенствование технологий защиты данных

Искусственный интеллект также может использоваться для улучшения уже существующих технологий защиты данных. Это включает в себя шифрование, управление доступом и защиту от вредоносного ПО.

Защита от вредоносного ПО

Алгоритмы ИИ способны выявлять и нейтрализовать вредоносное ПО более эффективно, чем традиционные методы. Они могут анализировать код и поведение программы, находя вредоносные функции еще до того, как они будут запущены. Это позволяет предотвратить проникновение вредоносного кода в систему и минимизировать убытки.

Преимущества и недостатки применения ИИ в защите данных

Хотя применение ИИ в защите данных имеет множество преимуществ, существуют и определенные недостатки, которые также необходимо учитывать.

Преимущества

1. Эффективность: Автоматизированные процессы уменьшают время реакции на угрозы и повышают условную безопасность системы.
2. Адаптивность: ИИ может подстраиваться под новые угрозы, обеспечивая актуальность методов защиты.
3. Снижение нагрузки на персонал: Системы, использующие ИИ, уменьшают необходимость постоянного контроля со стороны сотрудников, позволяя им сосредоточиться на более важных задачах.

Недостатки

1. Зависимость от данных: Эффективность ИИ-систем зависит от объема и качества данных, на основе которых проводится анализ.
2. Сложность реализации: Внедрение систем ИИ требует значительных ресурсов и времени, а также требуемых квалифицированных специалистов.
3. Риски утечки данных: При неправильной настройке ИИ-системы могут возникнуть новые уязвимости, что может привести к утечкам данных.

Будущее применения ИИ в защите информации

С учетом роста числа киберугроз и эволюции технологий, будущее применения ИИ в системе защиты информации выглядит многообещающим. Ожидается, что искусственный интеллект станет ключевым элементом кибербезопасности.

Развитие технологий

Существующие методы и алгоритмы будут совершенствоваться. Вероятнее всего, на первый план выйдут более «умные» системы, способные к самообучению и предсказанию атак. Это позволит организациям поддерживать высокий уровень безопасности, даже в условиях постоянно меняющихся угроз.

Роль и значимость искусственного интеллекта в защите информации

Одной из главных задач искусственного интеллекта в области защиты информации является анализ больших объемов данных для выявления необычного поведения пользователей или потенциальных злоумышленников. Алгоритмы машинного обучения позволяют создавать модели поведения пользователей и идентифицировать аномалии, что позволяет оперативно реагировать на возможные угрозы.

Кроме того, искусственный интеллект способен предсказывать вероятные атаки и разрабатывать эффективные стратегии обороны. За счет возможностей машинного обучения и анализа больших данных, системы защиты могут быть более адаптивными и реагировать на изменяющиеся угрозы в реальном времени.

Таким образом, роль и значимость искусственного интеллекта в защите информации от несанкционированного доступа в информационных системах персональных данных невозможно переоценить. Его применение позволяет существенно повысить эффективность и надежность систем безопасности, обеспечивая защиту ценных персональных данных от утечек и угроз.

Актуальные угрозы несанкционированного доступа к персональным данным

Современные информационные системы, содержащие персональные данные пользователей, сталкиваются с различными угрозами несанкционированного доступа. Киберпреступники постоянно совершенствуют методы атак и используют новейшие

технологии для получения доступа к конфиденциальной информации. Основные угрозы, с которыми сталкиваются системы защиты информации, включают в себя хакерские атаки, фишинг, DDoS-атаки, вирусы и троянские программы. Часто злоумышленники используют социальную инженерию для манипуляции сотрудниками и получения доступа к данным.

Заключение

Использование возможностей искусственного интеллекта при построении систем защиты информации от несанкционированного доступа является важным направлением современной информационной безопасности. Оно позволяет повысить эффективность обнаружения угроз, автоматизировать реагирование и обеспечить соответствие нормативным требованиям при обработке персональных данных.

Для преподавателей важно формировать у студентов понимание принципов работы таких систем, их преимуществ и ограничений, а также навыки практической работы с современными инструментами на базе ИИ.

Список литературы:

1. Применение нейронных сетей для обнаружения сетевых атак / В. В. Гладков, А. Г. Тараскина, С. И. Кузнецов [и др.] // Региональная информатика и информационная безопасность, Санкт-Петербург, 01–03 ноября 2017 года. Том Выпуск 4. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 73-74. – EDN UUJNKC.

2. Алашеев, В. В. Взгляды США на разработку доктрины информационного воздействия в киберпространстве / В. В. Алашеев, А. В. Акишин, М. Н. Чеснаков // Проблемы технического обеспечения войск в современных условиях: Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 года. Том 1. – Санкт-Петербург: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С. М. БУДЕННОГО" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, 2018. – С. 67-71. – EDN XMGZPF

3. Применение нейронных сетей при построении средств защиты информации / С. П. Ушаков, А. В. Акишин, Н. Н. Енин [и др.] // Проблемы научно-практической деятельности. Поиск и выбор перспективных решений: сборник статей VI международной научной конференции, Вологда, 25 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 32-39. – EDN ERREXB.

4. Применение искусственного интеллекта для обнаружения атак на веб-приложения / А. В. Акишин, Н. Н. Енин, К. Ю. Сопин [и др.] // Научные инструменты и механизмы перспективного инновационного развития общества: сборник статей XX международной научной конференции, Санкт-Петербург, 08 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 17-25. – EDN WMPULQ.