Министерство Образования Республики Беларусь

Белорусский Национальный Технический Университет

Факультет информационных технологий и робототехники

Кафедра **“**Технология разработки программного обеспечения**”**

Реферат на тему

ИИ в сфере информационной безопасности

Выполнили: студенты группы 10701322

ФИТР БНТУ

Бородкин Дмитрий Владимирович

Серов Данил Викторович

Минск, 2024

Оглавление

[Введение 3](#_Toc160628935)

[Стратегии обеспечения безопасности 4](#_Toc160628936)

[Экономическая эффективность ИИ в Информационной Безопасности 6](#_Toc160628937)

[Выводы 7](#_Toc160628938)

### Введение

На сегодняшний день искусственный интеллект является актуальной

информацией в Интернете и в категориях информационных навыков.

Информационная безопасность, несомненно, является основой любых

данных. Информационная безопасность требует соблюдения

конфиденциальности, целостности и доступности информации,

предотвращения несанкционированного раскрытия и использования

информации, предотвращения фальсификации и уничтожения информации, а

также обеспечения того, чтобы авторизованные пользователи и программы

могли использовать информацию своевременно. Искусственный интеллект в

информационной безопасности в приложении не имеет существенных

изменений, но применение искусственного интеллекта приведет к скачку

генерации и передачи информации и изменению характеристик, а также к

новым возможностям информационной безопасности. Например, растущее

число вирусов, таких как вирус WannaCry, вирус Petya и вирус CopyCat,

привлекло к информационной безопасности беспрецедентное внимание.

Искусственный интеллект играет все более важную роль в информационной

безопасности, особенно в защите и нападении. Как правильно использовать и

улучшить защиту за счет улучшения информационной безопасности стали

горячей темой в отрасли.

### Стратегии обеспечения безопасности

Несколько стратегий искусственного интеллекта в мире коснулись информационной безопасности. Хотя подробные описания различны, общая логика в основном одинакова, включая следующие аспекты:

1) надежность, это основной показатель безопасности и контроля искусственного интеллекта. То есть работа видимым для пользователя способом; доверенный, то есть вывод системы, приемлемый для пользователя;

2) проверяемость и допустимость являются логически естественными расширениями двусмысленности и достоверности.

3) вопросы морали и конфиденциальности в первую очередь связаны с чувствительностью данных.

4) ответственность означает ответственность планировщиков и организаторов системы искусственного интеллекта в отношении результатов поведения системы искусственного интеллекта.

Сравнивая вышеперечисленные аспекты, проблема режима ответственности является более целенаправленной, и теперь она в основном отражается в разделении ответственности за несчастные случаи, например, во время вождения автомобиля.

Искусственный интеллект разрушает существующую индустрию информационной безопасности. Например, выявление утечек паролей и неправильное использование является хорошим примером. Этот тип атаки становится все более распространенным, поскольку электронные письма и пароли людей попадают в темные сети после утечки данных. Например, уязвимость Equifax привела к раскрытию миллионов действительных писем; в Yahoo! нарушение данных злоумышленники получили информацию об учетной записи на 500 миллионов 7-я ежегодная международная конференция по геопространственным знаниям и интеллекту.

Поскольку люди склонны повторно использовать пароли, преступники будут случайным образом пробовать разные электронные письма и пароли на разных машинах в надежде на успех. Чтобы идентифицировать этот тип атаки, искусственный интеллект устанавливает базовый уровень для пользователей, которые подключаются и входят в систему на нескольких устройствах каждый день. Для человека принято пробовать сотни логинов на сервере, но трудно найти человека, пытающегося подключиться на 100 разных машинах и войти только один раз. Искусственный интеллект также может использоваться для автоматической оценки потенциальных ошибок в открытом исходном коде.

Однако другим приложением с точки зрения уязвимости является обзор и прогнозирование. Если объявлена новая уязвимость, можно использовать данные журнала, чтобы узнать, использовалась ли она в прошлом. Или, если это действительно новая атака, искусственный интеллект может оценить, достаточно ли доказательств, чтобы определить, каков следующий шаг злоумышленника. Искусственный интеллект также хорошо справляется с утомительными, повторяющимися задачами, такими как поиск определенного шаблона. Его реализация может облегчить ограничения ресурсов, с которыми сталкиваются большинство центров управления безопасностью. Методы защиты привилегированных пользователей Высокое значение учетной записи привилегированного пользователя. Привилегированные пользователи часто становятся жертвами атак Advanced Persistent Threat (APT). Цель состоит в том, чтобы заставить привилегированного пользователя раскрыть учетные данные или загрузить вредоносное ПО. Это дает злоумышленнику плацдарм в сети.

Злой умысел. Привилегированные пользователи могут преднамеренно подвергать опасности данные организации для личной выгоды, шпионажа или других злонамеренных целей. Они могут действовать как «волк-одиночка» или сотрудничать с хакерской группой или бизнес-конкурентом. Примеры злонамеренных действий включают в себя:

Внедрение логической бомбы, троянского коня, бэкдора или

вредоносного ПО в систему организации.

Развертывание вируса или вредоносного ПО в системах клиентов.

Сбор конфиденциальных или служебных данных.

Мониторинг привилегированных пользователей

Мониторинг привилегированных пользователей сопряжен со значительными техническими и операционными трудностями, поскольку привилегированным пользователям для выполнения своей работы требуется неограниченный доступ. Кроме того, технологические стратегии должны выходить за рамки встроенного аудита баз данных или управления информационными событиями безопасности (SIEM), поскольку эти инструменты предоставляют огромные объемы информации, но мало контекста, с помощью которого можно понять предупреждения.

Вместо этого надежная технологическая стратегия позволяет организации:

Отслеживание привилегированного доступа к конфиденциальным данным: отслеживайте доступ всех привилегированных пользователей к файлам и базам данных (включая доступ к локальной системе), проверяйте создание пользователей и новые предоставленные привилегии и ограничивайте использование учетных записей с общими привилегиями.

Блокировать или предупреждать о подозрительных действиях: выявлять поведение пользователей, которое отличается от обычных шаблонов доступа, а также предупреждать и блокировать подозрительные действия, которые могут указывать на злоупотребление привилегиями. Пользователи, выполняющие несанкционированные действия, должны быть помещены в карантин, а их привилегии должны быть пересмотрены. Аудиторские отчеты и аналитические инструменты необходимы для поддержки судебных расследований.

Выявление несанкционированных изменений привилегий: убедитесь, что изменения в объектах данных и системах данных должным образом авторизованы. Несанкционированные действия должны быть тщательно расследованы, и должны быть реализованы меры контроля для предотвращения будущих инцидентов.

Разделение обязанностей: убедитесь, что привилегированные пользователи не могут контролировать себя, так как они могут изменять элементы управления безопасностью, чтобы скрыть свои нестандартные действия.

Устранение избыточных и неиспользуемых прав: определение пользователей с высокими привилегиями, проверка того, что привилегии необходимы для роли и обязанностей пользователя, отмена чрезмерных прав пользователя и удаление бездействующих пользователей

### Экономическая эффективность ИИ в Информационной Безопасности

ИИ может быть использован в информационной безопасности для обнаружения и предотвращения кибератак, анализа угроз и вредоносного кода, а также для управления комплексной системой безопасности. Внедрение ИИ в область информационной безопасности может значительно повысить уровень защиты информации и снизить риски кибератак.

Экономическая эффективность полученного ПО в результате внедрения ИИ может быть высокой благодаря следующим причинам:

1. Автоматизация процессов: ИИ может автоматизировать многие процессы, связанные с обнаружением и предотвращением кибератак, что позволяет сократить время и ресурсы, затрачиваемые на обеспечение безопасности.

2. Сокращение человеческого фактора: Использование ИИ позволяет снизить риски, связанные с ошибками человека, так как система способна оперативно обнаруживать и реагировать на угрозы без участия человека.

3. Быстрая реакция на угрозы: ИИ способен анализировать большие объемы данных и выявлять угрозы быстрее, чем человек, что позволяет сократить время реакции на кибератаки и снизить возможные убытки.

4. Предсказание угроз: ИИ может использоваться для прогнозирования потенциальных угроз и разработки мер по их предотвращению, что помогает снизить риски и экономические потери.

5. Обнаружение угроз: ИИ способен анализировать большие объемы данных и идентифицировать необычное поведение или признаки угрозы, что помогает оперативно обнаруживать потенциальные атаки.

### Выводы

Таким образом, применение искусственного интеллекта в целях кибербезопасности позволяет компаниям эффективно защищать свою информацию и реагировать на угрозы, обеспечивая безопасность высокого уровня. В результате использования ИИ компании могут сэкономить ресурсы на обеспечение безопасности, уменьшить риски финансовых потерь от кибератак и повысить эффективность работы системы защиты.