УДК 001.895

АКТУАЛЬНОСТЬ РАЗРАБОТКИ АЛГОРИТМОВ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Сташишин А.И. (ИТМО), **Согришина М. О.** (ИТМО), **М. Креславский** (ИТМО)
Научный руководитель – кандидат экономических наук, доцент Павлова Е. А. (ИТМО)

Введение. В современной цифровой экосистеме повсеместное присутствие мобильных приложений стало определяющей характеристикой современной жизни. Широкое распространение мобильных приложений привело к накоплению огромного количества конфиденциальных данных в этих приложениях, что повысило важность внедрения надежных мер безопасности для защиты от утечек данных, несанкционированного доступа и киберугроз.

Более того, динамичный характер мобильных приложений в сочетании с разнообразием операционных систем и архитектур устройств создает уникальные проблемы безопасности, которые невозможно решить только традиционными мерами кибербезопасности. Появление таких технологий, как искусственный интеллект (далее - ИИ), открывает новые многообещающие возможности для повышения безопасности мобильных приложений. Алгоритмы ИИ, благодаря своей способности учиться на данных, выявлять закономерности и предвидеть потенциальные угрозы, представляют собой новый подход к кибербезопасности.

Основная часть. Разработка передовых алгоритмов защиты цифровых данных в мобильных приложениях подчеркивается рядом убедительных факторов. Огромное количество пользователей, использующих мобильные приложения для конфиденциальных информации, означает огромные потенциальные последствия одного нарушения безопасности. Учитывая, что во всем мире используются миллиарды мобильных устройств, масштабы компрометации данных являются беспрецедентными. Кроме того, личный характер данных, хранящихся на этих устройствах — от финансовой информации и личной переписки до медицинских записей и данных о местонахождении — делает потенциальные последствия нарушений безопасности особенно тревожными.[1]

Рассмотрим основные аспекты внедрения ИИ как метода защиты данных в мобильных приложения:

1. Уязвимости в мобильных приложениях. Одной из основных проблем безопасности мобильных приложений является разнообразие уязвимостей, которыми могут воспользоваться злоумышленники. Эти уязвимости варьируются от неадекватного шифрования данных до небезопасного хранения и передачи данных, а также недостатков в механизмах аутентификации. Например, многие приложения не могут правильно реализовать шифрование SSL/TLS, в результате чего данные подвергаются перехвату во время передачи. Более того, некоторые приложения хранят конфиденциальную информацию, такую как пароли и личные данные, в виде обычного текста на устройстве, что делает ее доступной любому, кто получит несанкционированный доступ к телефону

2. Усилия по повышению безопасности мобильных приложений. Разработчики и специалисты по безопасности используют различные стратегии для снижения рисков: внедрение более надежных методов шифрования, проведение регулярных проверок безопасности и использование методов безопасного кодирования, внедрение методов биометрической аутентификации. Одним из новых методов по защите данных является внедрение ИИ и машинное обучение Алгоритмы искусственного интеллекта могут помочь обнаружить и отреагировать на необычные модели поведения, указывающие на потенциальные угрозы безопасности.

Рассмотрим технологии искусственного интеллекта в защите данных:

В основе применения ИИ в области безопасности данных лежит машинное обучение — подмножество ИИ, которое позволяет системам учиться на основе шаблонов данных и совершенствоваться с течением времени без явного программирования. Алгоритмы машинного обучения могут анализировать обширные наборы данных для выявления аномалий, которые указывают на потенциальные угрозы безопасности, такие как попытки несанкционированного доступа или подозрительные действия по краже данных.[2]

1. Обработка естественного языка (NLP): NLP позволяет понимать и интерпретировать человеческий язык, что делает его критически важной технологией для выявления и смягчения угроз, таких как фишинговые атаки. Анализируя язык и шаблоны, используемые в электронных письмах, сообщениях и сообщениях в социальных сетях, NLP может помочь выявить попытки фишинга и предупредить пользователей о потенциальных угрозах.

2. Обнаружение аномалий: алгоритмы ИИ могут анализировать миллионы транзакций в режиме реального времени, чтобы обнаружить аномалии, которые отклоняются от нормальных моделей поведения, указывая на потенциальные угрозы безопасности. Например, если учетная запись пользователя внезапно инициирует перевод крупной суммы денег, система искусственного интеллекта может пометить это как подозрительное и принять превентивные меры.

3. Предиктивная аналитика: ИИ может прогнозировать потенциальные инциденты безопасности до того, как они произойдут, анализируя тенденции и закономерности в данных..

4. Автоматизированное реагирование на угрозы. При обнаружении угрозы системы ИИ могут автоматически инициировать действия по снижению риска, такие как изоляция затронутых систем, блокировка подозрительных IP-адресов или уведомление администраторов.

5. Расширенная аутентификация. ИИ усиливает меры безопасности за счет методов биометрической аутентификации, таких как распознавание лиц и сканирование отпечатков пальцев, которые злоумышленникам сложнее подделать, чем традиционные пароли.

Выводы. В заключение отметим, интеграция технологий ИИ в стратегии защиты данных очень актуальна. Она представляет собой значительный прогресс в борьбе с киберпреступностью. Используя машинное обучение, нейронные сети и обработку естественного языка, ИИ обеспечивает динамичный и интеллектуальный подход к защите цифровых активов, что очень востребовано на сегодняшний день. Однако успешное внедрение ИИ в защиту данных требует баланса между технологическими инновациями и этической ответственностью, гарантируя, что по мере развития наших возможностей по защите данных также будет поддерживать самые высокие стандарты конфиденциальности.

Список использованных источников:

1. Литвин Илья Ильич ОСОБЕННОСТИ СБОРА, ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ // Вестник Уральского юридического института МВД России. 2021. №4. URL: https://cyberleninka.ru/article/n/osobennosti-sbora-obrabotki-i-zaschity-personalnyh-dannyh-iskusstvennym-intellektom (дата обращения: 04.02.2024).

2. Димова К.В., Ешенко Р.А. Разработка приложения для защиты персональных данных с учетом выбора оптимальных методов шифрования // Вестник Хабаровского государственного университета экономики и права. 2019. №2 (100). URL: https://cyberleninka.ru/article/n/razrabotka-prilozheniya-dlya-zaschity-personalnyh-dannyh-s-uchetom-vybora-optimalnyh-metodov-shifrovaniya (дата обращения: 04.02.2024).