DOI 10.58351/2949-2041.2025.28.11.010

Соловьев Александр Александрович, Слушатель
КВВУ

ПРИМЕНЕНИЕ СИСТЕМ НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАЗРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ СЕТИ

Аннотация. В статье рассматриваются подходы и методы применения современных систем на базе искусственного интеллекта (Далее – ИИ) при проектировании и эксплуатации конфиденциальных сетей. Описаны ключевые задачи обеспечения конфиденциальности, роли ИИ в обнаружении аномалий

и управлении доступом, а также архитектурные принципы интеграции ИИ-компонентов в сеть. Приведены рекомендации по оценке рисков и обеспечению соответствия нормативным требованиям [1, 2].

Ключевые слова: Конфиденциальная сеть, искусственный интеллект, обнаружение аномалий, управление доступом, приватность

Современные сети связи обрабатывают огромные объёмы ограниченной информации – персональные данные, коммерческая тайна и служебная корреспонденция. Обеспечение конфиденциальности в таких сетях требует сочетания криптографических средств, организационных мер и интеллектуальных механизмов контроля. Повсеместное применение методов искусственного интеллекта (машинного обучения, глубокого обучения, методов анализа поведения пользователей) открывает новые возможности для повышения уровня защиты, но в то же время создаёт дополнительные вызовы, связанные

с прозрачностью, надёжностью и соответствием нормативным требованиям [1].

Задачи и требования к конфиденциальной сети

Основные задачи, которые должна решать конфиденциальная сеть: защита целостности и конфиденциальности передаваемых данных, управление доступом и аутентификация субъектов, обнаружение и реагирование на инциденты безопасности, а также обеспечение устойчивости к внутренним угрозам. Требования формулируются как технические (шифрование, сегментация трафика, изоляция ресурсов), так и организационные (политики доступа, аудит, мониторинг) [1]. Дополнительно предъявляются требования к соответствию законодательству (например, Федеральный закон РФ №152-ФЗ «О персональных данных») и отраслевым стандартам [2].

Роль ИИ в обеспечении конфиденциальности

ИИ позволяет решать несколько ключевых задач при создании конфиденциальной сети:

1) Обнаружение аномалий и инцидентов. Модели машинного обучения анализируют сетевой трафик и поведение пользователей, выявляя отклонения

от нормального поведения, которые могут указывать на утечки данных

или компрометацию узлов. Такие системы дополняют сигнатурные решения

и способны обнаруживать ранее неизвестные угрозы.

2) Управление доступом на основе контекста. Системы интеллектуального контроля доступа принимают решения с учётом множества факторов: местоположения, временных характеристик, поведения пользователя и состояния устройств. Это позволяет реализовать динамические политики «наименьших привилегий», сокращающие риск несанкционированного доступа.

3) Анонимизация и приватизация данных. Методы дифференциальной приватности и генеративные модели помогают публиковать агрегированные данные или обучать аналитические модели без раскрытия исходных конфиденциальных значительно снижая риск утечек при обмене данными между доменами.

4) Оптимизация криптографических операций и управления ключами. ИИ может прогнозировать нагрузки и адаптировать параметры шифрования (например, выбор алгоритма, режимов работы, ротацию ключей) для баланса между безопасностью и производительностью.

Архитектура интеграции ИИ в конфиденциальную сеть

При проектировании конфиденциальной сети с ИИ-компонентами рекомендуется придерживаться многослойной архитектуры:

• Уровень периметра и шифрования: реализация криптографической защиты каналов, VPN, TLS, сегментация сети.

• Уровень сбора телеметрии: централизованный сбор логов, сетевого трафика и метрик с устройств, и приложений.

• Уровень аналитики и ИИ: модели для обнаружения аномалий, прогнозирования рисков и принятия решений по доступу. Важно обеспечить изоляцию вычислений ИИ и защищённое хранение обучающих данных.

• Уровень оркестрации и реагирования: автоматизированные механизмы применения политик, изоляции узлов и уведомления операторов.

Ключевой принцип – минимизация доверия к ИИ-моделям: решения, влияющие на критические операции (например, автоматическое блокирование узла или изменение криптопараметров), должны предусматривать многоуровневую проверку и человеческий контроль.

Практические методы и алгоритмы

Для задачи обнаружения утечек и аномалий часто применяются алгоритмы на основе машинного обучения: кластеризация (для сегментации трафика), методы обнаружения выбросов, рекуррентные нейронные сети и модели трансформеров для анализа последовательностей сетевых запросов.

Для управления доступом используются модели классификации и правила на основе вероятностных оценок риска доступа.

При использовании методов генерации заместительных (синтетических) данных или дифференциальной приватности важно оценивать утечки информации через модели и применять технические меры защищённой тренировки (федеративное обучение, ограничение градиентов, добавление шума).

Оценка рисков и соответствие нормативам

Внедрение ИИ в конфиденциальную сеть требует комплексной оценки рисков: влияние ошибок модели на безопасность, уязвимости к атакам на модели, приватность обучающих данных. Необходимо проводить регулярные тестирования, аудит моделей и документирование принимаемых решений. Соответствие нормативным требованиям достигается сочетанием технических мер (шифрование, аудит) и процедур (политики управления данными, журналирование) [1, 2].

Рекомендации по внедрению

1) Начинать с пилотных проектов на ограниченных сегментах сети,

где можно безопасно оценить эффективность ИИ-решений.

2) Обеспечить защищённую инфраструктуру для хранения и обработки обучающих данных: использование шифрования, сегментации и контроля доступа.

3) Внедрять механизмы интерпретируемости и объяснимости для критичных моделей, чтобы операторы понимали причины срабатываний и могли принимать информированные решения.

4) Организовать процессы непрерывного мониторинга моделей

и регулярной перенастройки с учётом новых данных и выявленных инцидентов.

Заключение

Системы на базе искусственного интеллекта при правильном проектировании и внедрении способны существенно повысить уровень конфиденциальности сетевой инфраструктуры за счёт раннего обнаружения аномалий, адаптивного управления доступом и

улучшенной аналитики. В тоже время они требуют тщательного управления рисками, прозрачности моделей и соответствия нормативным требованиям. Комбинация традиционных методов информационной безопасности с ИИ-инструментами и чётко определёнными процедурами контроля обеспечивает сбалансированный подход к защите конфиденциальной информации в современных сетях.

Список литературы:

1. ГОСТ Р ИСО/МЭК 27001-2012. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2012.

2. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». – [Электронный ресурс]. – Режим доступа: http://www.consultant.ru