Воронов Дмитрий Юрьевич,
ассистент кафедры вычислительной техники института
информационных технологий РТУ МИРЭА, г. Москва

МАШИННОЕ ОБУЧЕНИЕ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ. ИННОВАЦИОННЫЕ ПОДХОДЫ К ПРЕДОТВРАЩЕНИЮ УГРОЗ

Аннотация. Современные компьютерные сети сталкиваются с постоянными угрозами безопасности, которые требуют новых и инновационных подходов для обнаружения и предотвращения атак. Одной из наиболее актуальных и перспективных технологий, применяемых в этой области, является машинное обучение, которое позволяет компьютерным системам обучаться на основе эталонных данных и ранее полученного опыта.

Ключевые слова: угрозы безопасности, машинное обучение, компьютерные сети.

Одной из важнейших задач в области безопасности вычислительных сетей является обнаружение вторжений и аномалий. Традиционные методы, основанные на правилах и сигнатурах, ограничены в своей способности обнаруживать новые и неизвестные угрозы. Машинное обучение позволяет создать модели, которые могут выявлять необычное поведение в сети, основываясь на обучении на исторических данных о нормальном функционировании сети. Алгоритмы машинного обучения, такие как алгоритмы кластеризации, классификации и нейронные сети, используются для создания моделей, которые могут обнаруживать аномалии и подозрительные активности.

Машинное обучение предлагает новые возможности для обнаружения вторжений и аномалий, основываясь на анализе больших объемов данных.

Применение алгоритмов машинного обучения позволяет создать модели, которые могут обучаться на исторических данных о нормальном функционировании сети и выделять аномальные активности, которые могут указывать на наличие вторжения.

Одним из популярных подходов к обнаружению вторжений и аномалий с использованием машинного обучения является методика обучения без учителя. В этом случае, модель обучается на неразмеченных данных, то есть данных, для которых неизвестно, являются ли они нормальными или аномальными. Модель старается выделить скрытые структуры и шаблоны в данных, в результате аномальные экземпляры данных будут отличаться от нормальных. При дальнейшем анализе таких аномалий можно обнаружить потенциальные угрозы безопасности.

Другой подход состоит в использовании алгоритмов классификации, которые обучаются на размеченных данных, где известно, какие экземпляры являются нормальными, а какие — аномальными. Модель обучается на этом размеченном наборе данных и затем может классифицировать новые экземпляры как нормальные или аномальные на основе изученных паттернов и характеристик [1].

Нейронные сети также широко применяются для обнаружения вторжений и аномалий. Рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN) могут анализировать последовательности данных или структурированные данные соответственно, что делает их эффективными инструментами для обнаружения аномалий в сетевой активности. Нейронные сети могут обнаруживать сложные паттерны и зависимости, которые могут быть незаметны для традиционных методов.

Одним из главных преимуществ использования машинного обучения в обнаружении вторжений и аномалий является его способность адаптироваться к новым и меняющимся угрозам. Модели машинного обучения могут обновляться и переобучаться на новых данных, что позволяет им эффективно

реагировать на новые виды атак. Кроме того, используя автоматизированную обработку данных, основанную на машинном обучении, становится возможным обрабатывать большие объемы данных в реальном времени, что позволяет оперативно реагировать на угрозы и предотвращать их распространение.

Еще одной важной областью применения машинного обучения в безопасности вычислительных сетей является прогнозирование угроз. Алгоритмы машинного обучения могут анализировать большие объемы данных о предыдущих инцидентах безопасности и выявлять шаблоны и тренды, которые могут указывать на будущие угрозы. Это позволяет сетевым администраторам вовремя принять меры и усилить защиту сети.

Прогнозирование угроз является важным аспектом обеспечения безопасности вычислительных сетей. Вместо реактивного реагирования на угрозы после их возникновения, прогнозирование угроз позволяет предвидеть потенциальные атаки и предотвратить или уменьшить негативные последствия.

Машинное обучение играет ключевую роль в прогнозировании угроз, поскольку позволяет анализировать большие объемы данных и выявлять паттерны и тенденции, которые могут указывать на будущие угрозы. Вот некоторые подходы и методы, используемые для прогнозирования угроз с помощью машинного обучения:

1. Анализ аномальных паттернов. Модели машинного обучения могут обучаться на исторических данных о предыдущих инцидентах безопасности и выявлять аномальные паттерны, которые могут быть связаны с потенциальными угрозами. Например, модель может выявить, что определенные события или комбинации событий, которые в прошлом предшествовали атаке, могут указывать на возможность атаки в будущем.

2. Обнаружение новых угроз. Машинное обучение может быть использовано для обнаружения новых и неизвестных угроз. При обучении модели на исторических данных о различных типах атак, она может научиться

выявлять схожие паттерны и характеристики в новых данных, которые могут указывать на появление новой угрозы. Это помогает предупреждать о появлении новых видов атак и принимать соответствующие меры заранее.

3. Анализ уязвимостей: Машинное обучение может быть использовано для анализа уязвимостей в сетевых системах и предсказания потенциальных уязвимостей, которые могут быть использованы злоумышленниками для атак. Модели машинного обучения могут обучаться на данных о известных уязвимостях и их характеристиках, а затем использовать эту информацию для прогнозирования возможных уязвимостей в новых ситуациях.

4. Анализ тенденций и контекста. Машинное обучение позволяет анализировать тренды и контекст в данных безопасности, таких как информация о новых угрозах, обновлениях программного обеспечения, изменениях в сетевой конфигурации и т. д. Модели машинного обучения могут выделять значимые тренды и предсказывать возможные сценарии угроз на основе этих данных[2].

Применение машинного обучения в прогнозировании угроз позволяет организациям быть более эффективными в предотвращении атак. Предварительное определение угроз и принятие соответствующих мер позволяют улучшить общую безопасность сети и защитить конфиденциальность, целостность и доступность данных.

Однако стоит отметить, что машинное обучение не является идеальным и полностью надежным инструментом. Возможны ошибки классификации, ложные срабатывания и адаптация атакующих к новым методам обнаружения. Поэтому важно сочетать машинное обучение с другими методами и подходами к обеспечению безопасности сети, такими как использование правил, многоуровневая защита и регулярное обновление системы безопасности.

Машинное обучение также может быть использовано для автоматизации процесса обучения систем безопасности. Вместо того чтобы полагаться

на ручное создание правил и сигнатур, алгоритмы машинного обучения могут самостоятельно обучаться на данных о сетевой активности и создавать модели, которые способны обнаруживать и предотвращать угрозы безопасности. Это позволяет более эффективно адаптироваться к новым и меняющимся угрозам и уменьшить необходимость вручную настраивать систему безопасности.

С развитием облачных технологий все больше организаций переходят к облачным системам безопасности. Машинное обучение играет важную роль в этих системах, обеспечивая мониторинг сетевой активности, обнаружение угроз и анализ данных в реальном времени. Алгоритмы машинного обучения могут оперативно реагировать на угрозы безопасности и предотвращать их распространение по облачной инфраструктуре.

Облачные системы безопасности представляют собой специализированные решения, которые обеспечивают безопасность вычислительных ресурсов, данных и приложений в облачной инфраструктуре. Машинное обучение играет важную роль в облачных системах безопасности, обеспечивая мониторинг сетевой активности, обнаружение угроз и анализ данных в реальном времени. В качестве примеров применения машинного обучения в облачных системах безопасности можно привести следующее:

1. Мониторинг и обнаружение угроз. Машинное обучение позволяет облачным системам безопасности анализировать большие объемы данных, получаемых из различных источников, включая лог-файлы сетевой активности, системные события, события безопасности и другие. Алгоритмы машинного обучения могут обучаться на этих данных, выявлять аномалии, распознавать сигнатуры известных атак и предупреждать о возможных угрозах в облачной инфраструктуре. Это позволяет оперативно реагировать на угрозы и предотвращать их распространение.

2. Идентификация вредоносного поведения. Машинное обучение может использоваться для создания моделей, которые могут идентифицировать вредоносное поведение в облачной среде. Например, модели машинного

обучения могут анализировать сетевую активность и поведение пользователей для выявления подозрительной активности, необычных запросов или несанкционированного доступа. Это помогает предотвращать атаки, связанные с вредоносным поведением, такие как внутренние угрозы или атаки «изнутри».

3. Управление уязвимостями. Машинное обучение может быть применено для обнаружения и управления уязвимостями в облачной инфраструктуре. Модели машинного обучения могут анализировать данные об уязвимостях, обновлениях программного обеспечения, патчах и других источниках информации, чтобы идентифицировать уязвимые компоненты и предложить соответствующие меры по устранению или снижению риска.

4. Обнаружение DDoS-атак. Машинное обучение может использоваться для обнаружения и защиты от распределенных атак отказа в обслуживании (DDoS). Модели машинного обучения могут анализировать трафик сети и выделять характеристики, связанные с DDoS-атаками, такие как необычно высокая нагрузка на сеть или большое количество запросов от определенных источников. Это позволяет оперативно реагировать на DDoS-атаки и принимать соответствующие меры для их смягчения или блокировки.

5. Автоматизация и оркестрация. Машинное обучение может быть интегрировано в системы автоматизации и оркестрации облачной безопасности. Это позволяет создавать интеллектуальные системы, которые автоматически реагируют на угрозы, принимают решения на основе анализа данных и выполняют соответствующие действия по обеспечению безопасности, такие как блокировка подозрительного трафика или изоляция уязвимых ресурсов.

Применение машинного обучения в облачных системах безопасности повышает эффективность и точность обнаружения угроз, а также позволяет оперативно реагировать на них. Это способствует обеспечению безопасности облачных ресурсов, защите конфиденциальности данных и надежности работы облачных приложений и сервисов.

Список литературы:

1. Шелухин О.И. Технологии машинного обучения в сетевой безопасности / О.И. Шелухин, С.Д. Ерохин, М.В. Полковников // серия «Интеллектуальные технологии информационной безопасности»; вып. 1, 2023 – 360с.

2. Артемов В. В. Классификация сетевого трафика / В.В. Артемов. – М.: Молодой ученый № 26, 27.06.2022 – 421с.