Штернберг Станислав Игорьевич
кандидат технических наук, доцент
Санкт-Петербургский государственный университет телекоммуникаций им М.А.Бонч-Бруевича
г. Санкт-Петербург
Смольницкий Павел Павлович
аспирант кафедры защищенных систем связи,
Санкт-Петербургский государственный университет телекоммуникаций им М.А.Бонч-Бруевича,
г. Санкт-Петербург.

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ОСНОВАННОЙ НА ПРОБЛЕМНО-ОРИЕНТИРОВАННОЙ КОНСТРУКЦИИ НЕЙРОННЫХ СЕТЕЙ, В ИНТЕРЕСАХ ВЫЯВЛЕНИЯ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ ПАКЕТНО-НЕЙРОСЕТЕВЫХ ПРОГРАММ

Аннотация: В статье рассматривается подход к созданию систем обнаружения вторжений (IDS), использующих адаптивные алгоритмы анализа сетевого трафика. Описывается математическая модель определения аномалий и программная реализация на языке Python, предназначенная для перехвата и классификации вредоносных пакетов в режиме реального времени. Применение адаптивных порогов фильтрации позволяет минимизировать ложноположительные срабатывания в динамических сетевых средах.

Ключевые слова: Информационная безопасность, обнаружение аномалий, адаптивный мониторинг, обучение без учителя, сетевой трафик, Python, AsyncIO, NumPy, SIEM.

Abstract: The article discusses an approach to creating intrusion detection systems (IDS) using adaptive algorithms for analyzing network traffic. A mathematical model for detecting anomalies and a Python software implementation designed to intercept and classify malicious packets in real time are described. The use of adaptive filtering thresholds minimizes false positives in dynamic network environments.

Keywords: Information security, anomaly detection, adaptive monitoring, unsupervised learning, network traffic, Python, AsyncIO, NumPy, SIEM.

1. Введение

Современный этап развития информационных технологий характеризуется стремительной цифровизацией бизнес-процессов и усложнением сетевых архитектур [3, с. 142]. В этих условиях киберугрозы приобретают беспрецедентную степень изменчивости и адаптивности, что делает традиционные методы защиты, основанные на поиске известных отпечатков атак, недостаточно эффективными [1, с. 23]. Основным ограничением классических средств защиты является их неспособность противодействовать угрозам «нулевого дня» и сложным целевым атакам (*APT*), которые имитируют реалистичное поведение пользователей или эксплуатируют ранее неизвестные уязвимости. [10, с. 37].

Интеллектуальный мониторинг сетевой безопасности, в отличие от традиционного анализа, ориентирован на выявление статистических аномалий в поведении узлов сети. Данный подход базируется на построении математического профиля состояния системы, что позволяет обнаруживать подозрительную активность даже при отсутствии соответствующих сигнатур в базах данных [2, с. 45]. Однако внедрение интеллектуальных методов сталкивается с проблемой высокой динамики сетевого трафика: естественные изменения нагрузки часто ошибочно классифицируются как атаки, что приводит к росту ложных срабатываний. Актуальность данного исследования обусловлена необходимостью разработки адаптивных механизмов мониторинга, способных самостоятельно подстраиваться под изменяющийся ландшафт угроз и сетевой статус. В работе предлагается методика, сочетающая математические метрики с программной реализацией на языке Python, что обеспечивает баланс между анализом и производительностью в высоконагруженных системах.

Научная новизна работы заключается в разработке и программной реализации методики непрерывного адаптивного мониторинга, которая отличается от существующих решений следующими аспектами: В отличие от классических систем обнаружения вторжений, использующих статические сигнатуры или жесткие пороги, предложенный подход реализует динамическую границу нормального состояния сети. Это позволяет системе автоматически подстраиваться под изменения трафика, исключая необходимость ручной перенастройки при изменении сетевой нагрузки.

Целью работы является разработка методического обеспечения и программно-алгоритмического комплекса для **адаптивного интеллектуального мониторинга трафика**, способного обеспечивать высокоточную идентификацию аномальных состояний защищенной сетевой инфраструктуры.

Научный интерес заключается в создании механизмов **адаптивного иммунитета** сетевой инфраструктуры. Исследование направлено на решение противоречия между чувствительностью трафика сети к новым угрозам и устойчивостью ложным тревогам. В центре внимания - алгоритмы написанные на языке Python, которые позволяют системе сохранять работоспособность при резком изменении сети.

2. Анализ связанных работ

Проблема интеллектуального анализа сетевого трафика на предмет выявления деструктивных воздействий является объектом интенсивных исследований последние два десятилетия. [2, с. 15] Текущие подходы к построению систем обнаружения вторжений (IDS) можно разделить на три основные группы:

Категория метода	**Ключевые представители / Технологии**	**Основные преимущества**	**Критические недостатки**	**Применимость в совр. инфраструктурах**
Сигнатурный (Детерминирова	Snort Suricata,	Минимальные вычислительн	Неспособность выявлять 0-	Вспомогательный уровень

нный)	экспертные правила	ые затраты; высокая точность для известных угроз.	day атаки; чувствительность к обфускации трафика.	защиты (L3/L4).
Статистический	Модели Гаусса, метод главных компонент (PCA)	Математическая прозрачность; высокая скорость обработки в реальном времени.	Высокий FPR из-за нестационарности трафика; плохая работа с «тяжелыми хвостами».	Анализ простых сетевых метрик в стабильных средах.
Машинное и глубокое обучение (ML/DL)	LSTM, GRU, Автокодировщики	Выявление сложных темпоральных зависимостей и скрытых паттернов атак.	Эффект «катастрофического забывания»; высокая ресурсоемкость обучения.	Системы анализа сложных APT-атак и аномалий сессий.
Адаптивный (Предложенный метод)	Python-реализация с рекуррентной подстройкой	Online-обучение без остановки мониторинга; устойчивость к смене контекста.	Необходимость начальной калибровки профиля.	Высоконагруженные динамические защищенные сети.

Таблица 1— Таблица методов систем обнаружения вторжений

Современное состояние исследований в области защиты сетевых инфраструктур характеризуется переходом от жестких алгоритмов к гибким адаптивным моделям. Анализ литературы позволяет выделить три основных этапа развития технологий мониторинга.

2.1. Сигнатурный анализ и детерминированные модели

Исторически первыми появились системы, работающие на основе экспертных правил отпечатков атак [1, с. 88]

Преимущество: Минимальное количество ложных срабатываний на известные угрозы. **Недостаток**: Полная неэффективность против атак нулевого

дня и модифицированных вредоносных активностей [3, с. 412]. Связанные работы показывают, что в условиях высоконагруженных сетей объем правил сигнатурного анализа растет экспоненциально, что создает критическую нагрузку на вычислительные узлы [6, с. 115].

2.2. Статическое машинное обучение (ML)

Для решения проблемы неизвестных атак исследователи начали применять алгоритмы классического ML: метод опорных векторов (SVM), случайные леса (Random Forest) и k-ближайших соседей. [10, с. 38]

Недостаток: Большинство этих методов требует предварительного обучения на размеченных датасетах , которые быстро устаревают.

Вывод: Статические модели не учитывают ситуацию, когда нормальное поведение сети меняется (например, при обновлении ПО), а система продолжает считать это атакой [5, с. 46].

2.3. Современные нейросетевые подходы (DL)

Работы сфокусированые на использовании рекуррентных нейронных сетей и автокодировщиков для поиска аномалий.

Недостаток: Несмотря на высокую точность, нейросети являются «черными ящиками» и требуют огромных мощностей .Для задач мониторинга в реальном времени на обычных серверах их применение часто оказывается экономически и технически неоправданным.

2.4. Сравнительный анализ и обоснование предлагаемого метода

На основе изученных работ выявлен пробел: существующие методы либо слишком просты, либо избыточно сложны , и почти никто не предлагает рекуррентное обновление математического профиля без остановки системы.

Метод	**Адаптивность**	**Скорость (High-EPS)**	**Обнаружение новых атак**
Сигнатурный	Низкая	Средняя	Нет

Нейросети (DL)	Высокая	Низкая	Да
Предлагаемый метод (Python/Mahalanobis)	Высокая	Высокая	Да

Таблица 2 — Сравнение подходов

3. Предлагаемая методология мониторинга

В основе работы лежит концепция метода динамического программирования сетевых состояний, которая интегрирует методы многомерного статистического анализа с механизмами непрерывного самообучения. В отличие от классических систем обнаружения вторжений (IDS), использующих статические сигнатуры, данная методология ориентирована на выявление скрытых или неявных проявлений отклоняющегося поведения сети, в высоконагруженных потоках данных (**High-EPS**), характерных для современных защищенных инфраструктур.

3.1. Гибридная модель анализа и экстракция признаков

Методология предполагает разделение процесса обработки трафика на два функциональных, а именно:

Цифровой фильтр: Выполняет низкоуровневое извлечение первичных метрик, такие как энтропия и распределение протоколов и формирование текущего вектора состояния в режиме реального времени. **Система обработки и анализа данных:** Осуществляет вычисление степени статистического отклонения текущего состояния от накопленного эталона.

3.3. Адаптация и компенсация «дрейфа концепции»

Для обеспечения устойчивости системы к изменениям сетевого трафика реализован алгоритм последовательного обновления параметров. Модель непрерывно корректирует границы «области нормы», используя сглаживание с убыв для весовых коэффициентов. Это позволяет: Минимизировать уровень ложноположительных срабатываний (FPR) при штатном масштабировании

сервисов, а также обеспечить функционирование системы в условиях априорной неопределенности относительно новых типов киберугроз.

3.4. Программная реализация на базе Python

Технологический стек, включающий библиотеки NumPy и AsyncIO, позволяет перенести вычислительную нагрузку на матричные операции. Это минимизирует временные издержки при обработке пакетов и обеспечивает масштабируемость методики в распределенных сетях, позволяя использовать её в качестве интеллектуального модуля в составе современных SIEM-решений.

Программная реализация и производительность

Вычислительная эффективность предложенного метода обеспечивается использованием **Python**-библиотек **NumPy** (для высокоскоростных матричных операций) и **AsyncIO** (для параллельной обработки событий). Такой подход гарантирует устойчивость системы к высоким нагрузкам и позволяет бесшовно внедрять разработанный интеллектуальный модуль в структуру корпоративных **SIEM-решений**.

Категория признака	**Название (Feature ID)**	**Описание и математическая суть**	**Тип детектируемой аномалии**
Временные (Time-Based)	**IAT (Inter-Arrival Time)**	Среднее время между поступлением пакетов в потоке. Выявляет автоматизированную активность.	Сканирование портов, брутфорс, DDoS-атаки типа "Flood".
	Flow Duration	Общая длительность сессии. Помогает отличить короткие запросы от длительных утечек данных.	Эксфильтрация данных (Data Exfiltration), бот-сети.

Объемные (Volume-Based)	**Packet Count (Src/Dst)**	Соотношение входящих и исходящих пакетов. Резкий перекос указывает на аномальную передачу.	Скомпрометированные узлы, работа C&C серверов.
	Avg Packet Size	Средний размер полезной нагрузки пакета в байтах.	Туннелирование трафика (ICMP/DNS tunneling).
Структурные (Structural)	**TCP Flags (Entropy)**	Распределение флагов (SYN, ACK, RST, PSH). Оценивается через энтропию или счетчик.	Попытки обхода защитных механизмов, атипичные сканы.
Сетевые (Network-Context)	**Port Cardinality**	Количество уникальных портов назначения за фиксированное окно времени.	Вертикальное и горизонтальное сканирование сети.

Таблица 3— признаков адаптивного интеллектуального мониторинга

3.1. Математическая модель признакового пространства

В основе математического обеспечения системы лежит формализованное описание сетевого трафика как нестационарного случайного процесса, параметры которого подлежат идентификации в реальном времени.

$x_{t=}\varphi(p_t) = [x_{t1}, x_{t2}, \dots x t_k]^T$ (ИТЭФ), 2021)

Формула 1. Вектор состояния сетевого события в момент времени t

Компоненты вектора $\boldsymbol{x_t}$ включают показатели нагрузки, временные интервалы $\Delta\tau$ статистические дескрипторы заголовков.

4.Требования к адаптивности

1. **Автономное обучение без учителя**.

Система должна самостоятельно формировать «портрет» нормального поведения сетевой инфраструктуры на основе входящего потока данных. Исключается необходимость предварительной ручной разметки трафика или жесткого задания пороговых значений администратором. Алгоритм должен распознавать постепенные или сезонные изменения в структуре трафика (например, рост нагрузки в рабочие часы или обновление ПО на узлах) как легитимную эволюцию сети, а не как серию аномалий. Система обязана плавно корректировать свои внутренние критерии «нормы» вслед за этими изменениями. Механизм адаптации должен обладать фильтрацией. Это необходимо, чтобы злоумышленник не мог «приучить» систему к вредоносному трафику, постепенно увеличивая его объем. Система должна отличать кратковременный опасный всплеск от долгосрочного изменения штатного режима.

2. Работа в реальном времени

Процесс переобучения и подстройки профиля безопасности должен происходить параллельно с анализом текущих пакетов. Не допускается остановка цикла мониторинга или перевод системы в «режим обучения», при котором защита временно отключается. Система должна балансировать между усвоением новых данных и сохранением знаний о базовых критических аномалиях. Адаптивность не должна приводить к тому, что через длительное время система перестанет реагировать на классические векторы атак только потому, что они давно не встречались. Требование к изменению чувствительности в зависимости от внешних факторов. Например, в периоды низкой сетевой активности система должна автоматически понижать строгость контроля, а в пиковые часы — расширять их для предотвращения ложных срабатываний.

Рекуррентный механизм самообучения Разработан алгоритм итерационного обновления параметров математической модели без остановки процесса фильтрации. Новизна заключается в использовании функции доверия,

которая защищает обучающую выборку от «отравления». Система способна отличать кратковременные аномальные всплески от долгосрочных легитимных изменений инфраструктуры. Научно обоснована и реализована программная архитектура на языке Python (с применением AsyncIO и векторизации NumPy), обеспечивающая математическую обработку потоков данных в реальном времени. Это снимает традиционное ограничение «вычислительной избыточности» интеллектуальных методов анализа при работе в высоконагруженных сетях.

Заключение

В статье представлена комплексная разработка системы защиты сетевой инфраструктуры, основанная на принципах самообучения. Основной упор сделан на то, чтобы система могла самостоятельно отличать DDOS атаку, от обычного изменения нагрузки. В статье представлена авторское видение самообучающейся системы защиты, способной функционировать в условиях неопределенности сетевого трафика. Написан алгоритм, который самостоятельно формирует понимание стабильности сети.

В дальнейшем планируется расширение функционала системы за счет интеграции нейросетевых моделей глубокого обучения и механизмов его реагирования, для обеспечения комплексной защиты зашифрованного трафика в высоконагруженных распределенных сетях.

Список литературы:

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — М.: ДМК Пресс, 2020. — 434 с.

2. Васильев, С. С. Математические методы в задачах анализа сетевого трафика / С. С. Васильев, В. А. Коротков. — М.: Наука, 2022. — 215 с.

3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 6-е изд. — СПб.: Питер, 2023. — 992 с.

4. Шолле, Ф. Deep Learning с помощью Python / Ф. Шолле. — СПб.: Питер, 2023. — 400 с

5. NumPy Reference. Array processing for numbers [Электронный ресурс]: https://numpy.org/doc/

6. AsyncIO Library. Asynchronous I/O, event loop, and concurrency [Электронный ресурс]. —https://docs.python.org/3/library/asyncio.html

7. Сетевая надежность Семенов Ю.А. (ГНЦ ИТЭФ) [Электронный ресурс] http://book.itep.ru/4/45/network_r.html

8. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е., АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ СБОРА ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ С ОТКРЫТЫХ РЕСУРСОВ И МОНИТОРИНГА ИНФОРМАЦИОННЫХ РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ // T-Comm: Телекоммуникации и транспорт. Т. 12. № 10. 2018. С. 36-40