DOI: 10.15514/ISPRAS-2026-38(2)-2

Адаптивные методы и средства поверхностного анализа пакетов для обнаружения аномалий в зашифрованном трафике

[1] *Н.А. Цаплин, ORCID: 0009-0004-8196-5847 <ntsaplin@gmail.com>*
[2] *А.П. Петров, ORCID: 0000-0001-5244-8286 <i@alexander-petrov.ru>*
[3] *Д.Ю. Ковалев, ORCID: 0000-0003-4180-3056 <dkovalev@frccsc.ru>*

[1] *Институт прикладной математики им. М.В. Келдыша РАН, Россия, 125047, Москва, Миусская пл., д.4.*

[2] *Институт проблем управления им. В.А. Трапезникова РАН, Россия, 117997, Москва, ул. Профсоюзная, д. 65.*

[3] *Федеральный исследовательский центр "Информатика и управление" РАН, Россия, 119333, г. Москва, ул. Вавилова, д.44, кор.2.*

Аннотация. Массовое шифрование сетевого трафика делает традиционный глубокий анализ пакетов неприменимым, что требует перехода к поверхностному анализу на основе метаданных уровней OSI L2–L4. В данной работе предложен адаптивный подход к обнаружению аномалий в зашифрованном трафике, сочетающий высокопроизводительный сбор статистик, модифицированный жадный алгоритм отбора признаков и динамическую настройку гиперпараметров моделей машинного обучения. Реализация выполнена в виде NDIS-драйвера RuStatExt для Hyper-V Extensible Switch, обеспечивающего агрегацию трафика и извлечение признаков без снижения пропускной способности канала. На основе данных, собранных с более чем 2000 виртуальных машин в промышленной облачной среде, проведено сравнение методов отбора признаков (LASSO, RFE, жадный алгоритм) и моделей (Isolation Forest, Local Outlier Factor, One-Class SVM) при статической и динамической настройке параметров. Наилучший результат F1-меры, равный 0.78, достигнут моделью Isolation Forest с признаками, отобранными предложенным алгоритмом, при статической настройке гиперпараметров, что почти в 2 раза превосходит базовый подход с полным набором признаков. Драйвер не вносит статистически значимых накладных расходов при нагрузке 1 Гбит/с. Результаты подтверждают, что точное обнаружение аномалий возможно без расшифровки трафика, что обеспечивает применимость решения в современных облачных инфраструктурах.

Ключевые слова: поверхностный анализ пакетов (SPI); обнаружение аномалий; нежелательный трафик; отбор признаков; жадный алгоритм.

Для цитирования: Цаплин Н.А., Петров А.П., Ковалев Д.Ю. Адаптивные методы и средства поверхностного анализа пакетов для обнаружения аномалий в зашифрованном трафике. Труды ИСП РАН, том 38, вып. 2, 2026 г., стр. 21–34. DOI: 10.15514/ISPRAS–2026–38(2)–2.

Благодарности: Авторы выражают благодарность руководителям отделов разработки и ИТ ООО “МТ ФИНАНС” А.В. Томиленко и В.И. Грабарчуку за полезные обсуждения и внимание к работе.

Adaptive methods and tools for shallow packet inspection in anomaly detection within encrypted network traffic

[1] *N.A. Tsaplin, ORCID: 0009-0004-8196-5847 <ntsaplin@gmail.com>*
[2] *A.P. Petrov, ORCID: 0000-0001-5244-8286 <i@alexander-petrov.ru>*
[3] *D.Yu. Kovalev, ORCID: 0000-0003-4180-3056 <dkovalev@frccsc.ru>*

[1] *Keldysh Institute of Applied Mathematics, Russian Academy of Sciences, 4, Miusskaya Sq., Moscow, 125047, Russia.*

[2] *V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, 65, Profsoyuznaya St., Moscow, 117997, Russia.*

[3] *Federal Research Center "Computer Science and Control", Russian Academy of Sciences, bld. 2, 44, Vavilova st., Moscow, 119333, Russia.*

Abstract. The widespread adoption of encrypted network traffic severely limits the applicability of Deep Packet Inspection in modern cloud infrastructures. This paper addresses the challenge of accurate and scalable anomaly detection using Shallow Packet Inspection – an approach that relies solely on metadata from packet headers at OSI layers 2-4, without accessing payload contents. We propose a lightweight, kernel-level SPI framework implemented as a driver for the Hyper-V Extensible Switch, named RuStatExt, which aggregates traffic into flows and extracts statistical features with negligible performance overhead. To maximize detection quality, we introduce a modified greedy feature selection algorithm and a dynamic hyperparameter tuning strategy that scales linearly with the number of monitored virtual machines. The methodology includes filtering of virtual machines, comparison of feature selection techniques, evaluation of unsupervised models, and assessment of detection quality using Precision, Recall, and F1-score. Practical validation is performed using synthetic L2-L4 attacks (SYN/UDP floods) and high-load traffic over a 1 Gb/s link. Our experiments show that Isolation Forest, combined with features selected by the proposed greedy algorithm and dynamically tuned hyperparameters, achieves an F1-score of 0.78, nearly 2 times higher than the static configuration using all features. Crucially, the RuStatExt driver introduces no statistically significant degradation in network throughput for either TCP or UDP traffic.

Keywords: Shallow Packet Inspection (SPI); anomaly detection; unwanted traffic; feature selection; greedy search.

For citation: Tsaplin N.A., Petrov A.P., Kovalev D.Yu. Adaptive methods and tools for shallow packet inspection in anomaly detection within encrypted network traffic. Trudy ISP RAN/Proc. ISP RAS, vol. 38, issue 2, 2026, pp. 21-34 (in Russian). DOI: 10.15514/ISPRAS-2026-38(2)-2.

Acknowledgements: The authors express their gratitude to the heads of the Development and IT departments of MT FINANCE LLC, A.V. Tomilenko and V.I. Grabarchuk, for helpful discussions and their attention to this work.

1. Введение

Современные облачные инфраструктуры активно используются для размещения критически важных сервисов – от государственных информационных систем до финансовых и телекоммуникационных платформ. Однако вместе с ростом сложности и масштабируемости таких систем увеличивается и поверхность атак: злоумышленники всё чаще применяют распределённые атаки на уровне сетевого и транспортного стека (L3/L4 OSI), в частности SYN- и UDP-флуд. Эти атаки нацелены не на уязвимости приложений, а на исчерпание ресурсов инфраструктуры, что делает их особенно опасными в условиях высокой плотности виртуальных машин (ВМ). Наряду с ними осуществляются информационные атаки, направленные на подрыв социальной стабильности [1-2].

Для противодействия таким угрозам традиционно применяются системы обнаружения вторжений (Intrusion Detection Systems, IDS), основанные на глубоком анализе пакетов (Deep Packet Inspection, DPI). DPI предполагает полный доступ к содержимому полезной нагрузки

сетевых пакетов, включая прикладной уровень, что позволяет точно классифицировать трафик, выявлять вредоносные паттерны и блокировать атаки. Однако массовое внедрение сквозного шифрования (через протоколы TLS/SSL, HTTPS, IPSec, а также мессенджеры и VPN-сервисы) делает DPI либо технически невозможным, либо экономически и юридически нецелесообразным. Расшифровка трафика требует значительных вычислительных ресурсов, специализированного оборудования и нарушает принципы конфиденциальности, закреплённые в регуляторных рамках (включая GDPR и российское законодательство о персональных данных).

В этих условиях всё большую актуальность приобретает поверхностный анализ пакетов (Shallow Packet Inspection, SPI) – подход, ограничивающийся исключительно метаданными заголовков протоколов уровней L2–L4 (Ethernet, IP, ICMP, TCP, UDP). Такие данные содержат информацию о типах пакетов, направлении потока, количестве переданных байт и пакетов, флагах TCP и других характеристиках, которые не зависят от содержимого прикладного уровня. SPI полностью совместим с зашифрованным трафиком, может быть реализован с минимальными накладными расходами и особенно эффективен при интеграции на уровне гипервизора, например, в рамках Hyper-V Extensible Switch, где возможно перехватывать весь межмашинный трафик без необходимости в сетевом зеркалировании или дополнительных аппаратных средствах.

Однако существующие SPI-подходы страдают от двух ключевых ограничений: (1) использование неоптимальных или полных наборов признаков без учёта корреляций, и (2) применение фиксированных гиперпараметров моделей машинного обучения, что снижает устойчивость при масштабировании. Как показано в [3-4], даже небольшие изменения в структуре трафика приводят к резкому падению качества обнаружения.

На основе этого авторами формулируется следующая исследовательская гипотеза:

Комбинация (1) вычислительно эффективного отбора признаков на основе модифицированного жадного алгоритма и (2) динамической настройки гиперпараметров моделей машинного обучения, линейно масштабируемой от числа наблюдений, позволяет достичь статистически значимого повышения F1-меры (> 0.7) в задаче обнаружения аномалий в зашифрованном трафике по сравнению с базовыми SPI-подходами, использующими полный набор признаков и фиксированные гиперпараметры.

Основной вклад работы заключается в:

- реализации легковесного NDIS-драйвера для Hyper-V Extensible Switch, способного агрегировать трафик в потоки и извлекать статистики без снижения пропускной способности канала;
- предложении модифицированного жадного алгоритма отбора признаков, устойчивого к корреляциям, с механизмом допуска кратковременных ухудшений метрики, что позволяет преодолеть локальные минимумы в условиях сильных корреляций;
- введении стратегии динамической настройки гиперпараметров;
- экспериментальном подтверждении $F1 > 0.7$, что сравнимо или превосходит подобные SPI-решения.

Предлагаемый подход не требует доступа к содержимому трафика, совместим с любыми зашифрованными протоколами и может быть интегрирован в существующие облачные стеки без модификации приложений или клиентских устройств. Решение нацелено на баланс между точностью обнаружения, производительностью и масштабируемостью – ключевыми требованиями для современных систем сетевой безопасности.

В разделе 2 рассмотрены существующие подходы к отбору признаков, преимущества и новизна предложенного подхода. В разделе 3 описана архитектура драйвера RuStatExt, его взаимодействие с виртуальным коммутатором Hyper-V Extensible Switch, механизм агрегации трафика в потоки, работа с памятью ядра и классификация пакетов на уровнях L2-L4. Представлены результаты нагрузочного тестирования, подтверждающие отсутствие статистически значимого влияния драйвера на пропускную способность канала и потребление ресурсов ЦПУ при обработке трафика на скорости 1 Гб/с. В разделе 4 описана подготовка данных, предложен модифицированный жадный алгоритм отбора признаков, а также подходы к статической и динамической настройке гиперпараметров. В разделе 5 производится сравнительный анализ эффективности различных моделей машинного обучения в задаче обнаружения аномалий. В заключении обобщаются ключевые результаты исследования: показано, что оптимальной является комбинация Isolation Forest с признаками, отобранными предложенным жадным алгоритмом, при динамической настройке гиперпараметров.

2. Родственные работы

Поверхностный анализ пакетов получил широкое распространение как альтернатива глубокому анализу в условиях массового шифрования сетевого трафика. SPI ограничивается метаданными уровней OSI L2–L4, такими как число пакетов, объём байтов, флаги TCP (включая SYN/ACK) и типы протоколов, и может быть реализован на уровне гипервизора, включая коммутатор Hyper-V Extensible Switch. Однако эффективность таких систем напрямую зависит от качества отбора признаков и адаптивности моделей машинного обучения.

Существующие методы отбора признаков демонстрируют серьезные ограничения в условиях сетевой статистики. Рекурсивное исключение признаков требует многократного обучения модели и не применимо к алгоритмам без учителя, не предоставляющим коэффициентов важности, таким как Isolation Forest. LASSO-регуляризация, в свою очередь, склонна оставлять лишь один признак из сильно коррелированной группы, например, между числом пакетов и объемом байтов, что приводит к потере диагностически значимой информации.

Параллельно, большинство современных SPI-систем используют фиксированные гиперпараметры, что, как показано в работах [3-4], приводит к резкому падению качества при существенном изменении числа виртуальных машин или профиля нагрузки. Некоторые подходы, такие как siForest [5] (F2-мера достигает 0.6), улучшают метрики Isolation Forest за счет структурированного разбиения данных, но также предполагают статическую настройку и не интегрированы на уровне ядра ОС.

Недавние исследования [6-9] подчеркивают критическую роль отбора признаков: на датасете CIC-IDS2017.Так, F1-мера для вариационного автоэнкодера варьируется от 0.65 (при использовании всех признаков) до 0.85 (при отборе топ-17 признаков по корреляции), в то время как метод опорных векторов достигает лишь 0.4 [6]. Это демонстрирует, что даже при фиксированной модели качество SPI может отличаться более чем в два раза, причем исключительно за счет состава признаков.

Современные системы, такие как Kitsune [7], используют автоэнкодеры для обнаружения аномалий в реальном времени, но требуют значительных вычислительных ресурсов и чувствительны к сдвигу распределения (concept drift). Подходы на основе статистик, вычисляемых по скользящему окну и SVM (SFSC [8]) достигают F1 до 0.75, однако полагаются на экспертный отбор признаков и не масштабируются на динамические облачные среды. Более того, как показано в [9], даже небольшой сдвиг в распределении трафика (например, при добавлении новых ВМ) может снизить F1 на 10% у статических моделей, что подтверждает необходимость адаптивных стратегий либо через онлайн-обучение [9], либо через динамическую настройку гиперпараметров.

Таким образом, в научной и инженерной практике сохраняется значительный пробел: отсутствуют решения, которые одновременно (1) обеспечивают высокопроизводительный сбор метаданных на уровне ядра ОС, (2) реализуют вычислительно эффективный отбор признаков, устойчивый к корреляциям и совместимый с моделями без учителя и без коэффициентов, и (3) поддерживают динамическую, масштабируемую настройку гиперпараметров. Настоящая работа устраняет этот пробел за счёт реализации легковесного NDIS-драйвера, модифицированного жадного алгоритма отбора признаков и стратегии динамической настройки гиперпараметров.

3. Реализация и оценка производительности SPI-драйвера RuStatExt

Для решения задачи мониторинга сетевой активности в условиях массового шифрования трафика был разработан высокопроизводительный NDIS-драйвер RuStatExt, интегрированный в Hyper-V Extensible Switch и реализующий поверхностный анализ пакетов исключительно на основе метаданных уровней L2-L4. Драйвер не взаимодействует с полезной нагрузкой прикладного уровня, что делает его полностью совместимым с зашифрованным трафиком и исключает юридические и производственные риски, связанные с расшифровкой.

3.1 Архитектура драйвера и механизм агрегации потоков

RuStatExt реализован как расширение (extension) виртуального коммутатора Hyper-V и использует стандартный интерфейс NDIS (Network Driver Interface Specification) для перехвата сетевых пакетов на путях ingress (входящий трафик) и egress (исходящий трафик). При обработке каждого пакета драйвер:

- определяет тип протокола на основе заголовков Ethernet (L2), IP (L3) и TCP/UDP (L4);
- для ARP-пакетов – анализирует поле Ethernet Type;
- для IP-пакетов – проверяет значение поля Protocol, поддерживая GRE, ICMP, TCP, UDP;
- для TCP дополнительно анализирует флаги SYN и ACK, что позволяет выявлять признаки SYN-флуд-атак [10].

Для каждого порта виртуального коммутатора (PortId) драйвер ведёт агрегированную статистику по следующим метрикам: PacketsIn/Out, BytesIn/Out, TcpSynIn/Out, TcpSynAckIn/Out, TcpIn/Out, UdpIn/Out, IcmpIn/Out, ArpIn/Out, GreIn/Out. Агрегация выполняется в режиме реального времени с интервалом 600 секунд, что соответствует типичной длительности большинства L3/L4-атак [11]. Данные сохраняются в текстовом формате и могут быть переданы системам анализа без задержек.

Драйвер использует невыгружаемый пул памяти ядра ОС через функцию ExAllocatePoolWithTag из библиотеки wdm.h. Это гарантирует, что данные всегда находятся в физической памяти и не вызывают page fault, что критично для стабильности сетевого драйвера.

Структура данных хранится в виде хэш-таблицы, где ключом служит PortId, а значением – структура NicStatEntry с накопленной статистикой. Для разрешения коллизий используется метод цепочек переполнения. Обновление счётчиков выполняется атомарными операциями (InterlockedIncrement), что исключает необходимость блокировок и обеспечивает корректность при параллельной обработке пакетов. Важно отметить, что архитектура NDIS-расширения не использует прерывания IRQ, так как не взаимодействует напрямую с сетевым оборудованием, и не копирует данные в пользовательское пространство – вся логика выполняется в ядре ОС.

3.2 Результаты оценки производительности

Для объективной оценки влияния драйвера на производительность была создана тестовая среда:

- Хост: Windows Server 2016, 2 × Intel Xeon Gold 6234 (3.3 ГГц), 64 ГБ ОЗУ;
- Гостевые ВМ: Kali Linux 2024.1 и Elementary OS 7.1, по 1 ЦПУ и 64 МБ ОЗУ;
- Сетевое соединение: внешний коммутатор, 1 Гбит/с;
- Инструмент: iperf3 (версии 3.16 и 3.9 соответственно);
- Конфигурация: 4 параллельных потока, длительность – 60 с.

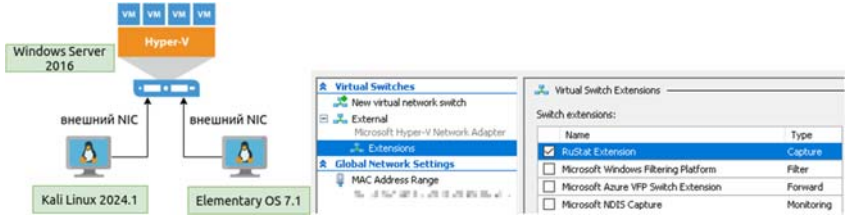

Рис. 1. Схема стенда (слева) и драйвер как расширение виртуального коммутатора (справа).
Fig. 1. Test setup schematic (left) and driver configuration as a virtual switch extension (right).

Тесты проводились как для TCP без ограничения скорости (-b 0 по умолчанию), так и для UDP с явным заданием размера пакета (-l 1400) и отключением ограничения (-b 0). Каждая конфигурация (с драйвером и без) повторялась не менее 20 раз в соответствии с методикой RFC 2544 [12]. Замеры проводились между двумя ВМ под Linux, так как Microsoft не рекомендует использовать iperf3 непосредственно на Windows для сравнительных тестов [13].

Среднее снижение пропускной способности при активном мониторинге составило 5.7 Мбит/с для TCP, что меньше одного стандартного отклонения и статистически не значимо. В случае UDP даже наблюдался небольшой рост средней скорости, что объясняется естественной волатильностью сети.

Измерения загрузки ЦПУ на хосте показали увеличение менее чем на 0.5%, что также не выходит за пределы погрешности. Таким образом, драйвер RuStatExt не создаёт заметной нагрузки на систему даже при полной загрузке канала 1 Гбит/с.

Драйвер RuStatExt демонстрирует высокую производительность и минимальные накладные расходы, что подтверждает его пригодность для развёртывания в промышленных облачных инфраструктурах. Архитектура на основе NDIS, использование атомарных операций и невыгружаемой памяти обеспечивают стабильность и масштабируемость, а агрегация метаданных на уровне L2-L4 позволяет эффективно выявлять аномалии без доступа к зашифрованному содержимому трафика.

Табл. 1. Скорость передачи трафика (Мбит/с).
Table 1. Traffic transmission rate (Mbit/s).

Протокол	Конфигурация	Мин.	Среднее	Макс.	Ст. откл.
TCP	Без RuStatExt	804	852.8	884	21.35
	С RuStatExt	806	847.1	886	23.71
UDP	Без RuStatExt	292	310.4	327	10.08
	С RuStatExt	289	315.3	339	12.91

4. Методы отбора признаков и адаптивной настройки гиперпараметров

Эффективность поверхностного анализа пакетов (SPI) в задаче обнаружения аномалий напрямую зависит от качества используемых признаков и адаптивности моделей машинного обучения. В данном разделе описывается методология подготовки обучающих данных, предлагается модифицированный жадный алгоритм отбора признаков, сравнивается с альтернативами (LASSO, RFE), а также вводится подход динамической настройки гиперпараметров, масштабируемый от объёма данных.

4.1 Подготовка данных и разметка аномалий

Исходные данные поступают от драйвера RuStatExt, который каждые 600 секунд агрегирует статистику по каждому порту виртуального коммутатора Hyper-V. Для каждой виртуальной машины (ВМ) формируются временные ряды по следующим метрикам: *PacketsIn/Out, BytesIn/Out, TcpSynIn/Out, TcpSynAckIn/Out, TcpIn/Out, UdpIn/Out, IcmpIn/Out, ArpIn/Out, GreIn/Out*.

Для повышения релевантности выборки применяется фильтрация ВМ по активности. Исключаются:

- ВМ с низкой интенсивностью трафика (*OutgoingTcpSyn* < 0.01 за 10 мин);
- ВМ с экстремально высокими всплесками (*OutgoingTcpSyn* > 300);
- ВМ с нестабильным поведением (высокая дисперсия *OutgoingTcpSyn*).

В ходе исследования участвовало 27 виртуальных машин, отобранных по критериям стабильности трафика и активности. Для каждой ВМ раз в 600 секунд формировался вектор из 18 признаков на основе статистик L2-L4. На основе экспертных правил и анализа публичных отчётов о DDoS-атаках [14-15], аномалии размечаются следующим образом:

- SYN-флуд: превышение порога 30 pps в течение 70 мин или 100 pps в течение 20 мин по метрике OutgoingTcpSyn;
- UDP-флуд: превышение 35 000 pps по общему исходящему трафику за 20 мин.

Для оценки качества моделей учитывается временной сдвиг: если аномалия произошла в момент *t*, она считается обнаруженной, если хотя бы одна точка в интервале *[t-k, t]* (где k = 10 мин) предсказана как аномалия. С учётом того, что 83% атак уровня L3/L4 длятся от 30 до 60 минут [16], допускается временной сдвиг предсказания: если аномалия произошла в момент *t*, она считается корректно обнаруженной, если хотя бы одна точка в интервале *[t-600, t]* была предсказана как аномалия. Все эксперименты проводились на реальных данных, собранных драйвером RuStatExt в промышленной облачной среде (хостинг-провайдер RUVDS).

4.2 Модифицированный жадный алгоритм отбора признаков

Прямой перебор всех подмножеств признаков имеет экспоненциальную сложность $O(2^m)$ и неприменим при $m > 10$. Для решения этой задачи предложен модифицированный жадный алгоритм, сочетающий forward selection и backward elimination [17].

Алгоритм начинает с пустого (или случайного) набора признаков и на каждом шаге может как добавлять признак, максимизирующий F1-меру (forward); так и удалять наименее значимый признак, если это улучшает метрику (backward).

Ключевая модификация – введение параметров *allow_forward_failure* и *allow_backward_failure*, разрешающих однократное отступление от локального улучшения метрики. Это позволяет преодолевать локальные минимумы, вызванные сильной корреляцией между признаками (например, *IncomingPackets* и *IncomingBytes*).

Дополнительно оценка производится по F_β-мере с $\beta = 0.5$, что даёт больший вес точности (важно для SOC-систем, где ложные срабатывания критичны).

Для объективной оценки предложенного подхода сравнивались три метода отбора признаков:

- LASSO (L1-регуляризация): эффективно обнуляет коэффициенты, но склонен выбирать только один признак из коррелированной группы, что снижает релевантность в условиях сетевой статистики.
- RFE (Recursive Feature Elimination): требует многократного обучения модели, что вычислительно затратно и не применимо ко всем моделям (например, модель Isolation Forest не предоставляет коэффициентов важности).
- Модифицированный жадный алгоритм: обеспечивает среднюю вычислительную сложность ($O(N^2)$), не требует градиентов или коэффициентов, устойчив к корреляциям и пригоден для обработки в реальном времени.

Сравнение методов по ключевым критериям приведено в табл. 2. LASSO и RFE требуют либо линейной модели, либо возможности оценки важности признаков (например, коэффициентов), что делает их неприменимыми к таким моделям, как Isolation Forest. Кроме того, LASSO склонен выбирать лишь один признак из коррелированной группы (например, IncomingPackets или IncomingBytes), теряя дополнительную информацию. В отличие от них, предложенный модифицированный жадный алгоритм не требует градиентов или коэффициентов, устойчив к корреляциям и совместим со всеми рассмотренными моделями. Его вычислительная сложность составляет $O(N^2)$, что позволяет использовать его в условиях реального времени, что критично для систем мониторинга облачных инфраструктур.

4.3 Адаптивная настройка гиперпараметров

Традиционный GridSearch использует фиксированные гиперпараметры, что не учитывает изменение масштаба данных (число ВМ, объём трафика). Для устранения этого ограничения предложен динамический GridSearch, в котором гиперпараметры задаются как линейные функции от N (числа наблюдений):

- *contamination* = a / N – доля аномалий уменьшается с ростом N;
- *n_estimators* = $a*N$ – чем больше данных, тем больше деревьев;
- *n_neighbors* = $a*N$ – чем выше плотность, тем больше соседей для LOF;
- *leaf_size* = $a*N$ – масштабирование структур данных под объём памяти.

Коэффициенты подбирались эмпирически, чтобы параметры оставались в разумных пределах даже при очень больших значениях *N*. Такой подход обеспечивает масштабируемость без потери точности и особенно эффективен при изменении состава облачного пула ВМ.

5. Оценка точности обнаружения аномалий при различных подходах к обучению в задаче SPI-анализа

Для оценки эффективности предложенных методов отбора признаков и адаптивной настройки гиперпараметров было проведено систематическое сравнение ряда моделей машинного обучения в условиях поверхностного анализа пакетов (SPI). Качество моделей оценивалось по трём метрикам:

- Точность (Precision) – доля верно предсказанных аномалий среди всех срабатываний;
- Полнота (Recall) – доля обнаруженных аномалий среди всех истинных;

- F1-score – гармоническое среднее, рассчитанное с параметром β = 0.5, что придаёт больший вес точности (важно для SOC-систем, где ложные срабатывания недопустимы).

Эксперименты проводились в четырёх конфигурациях:

- All + Static – использование всех 18 признаков, фиксированные гиперпараметры (базовые модели машинного обучения, применяемые в SPI-анализе являются эталонными для оценки эффективности методов подбора признаков и динамической настройки параметров);
- Greedy + Static – признаки, отобранные модифицированным жадным алгоритмом, статическая настройка;
- All + Dynamic – все признаки, динамическая настройка гиперпараметров (линейная зависимость от N);
- Greedy + Dynamic – комбинация жадного отбора и динамической настройки.

Табл. 2. Сравнение методов отбора признаков.
Table 2. Comparison of feature selection methods.

Критерий / Метод	Модифицированный жадный алгоритм	LASSO	RFE (Recursive Feature Elimination)	Random Forest (встроенный отбор)
Точность (F1)	Высокая: $F1 \geq 0{,}75$	Средняя: $0{,}5 < F < 0{,}75$	Средняя-высокая: $F1 > 0{,}5$	Высокая: $F1 \geq 0{,}75$
Вычислительная сложность	Средняя: $O(N^2)$	Высокая: $O(N^3)$	Высокая: многократное обучение модели	Средняя: от $O(n*\log n)$ до $O(N^2)$
Масштабируемость	Высокая	Ограничена при большом числе признаков	Умеренная (зависит от базового классификатора)	Высокая
Устойчивость к корреляциям	Да (благодаря `allow_forward_failure` и `allow_backward_failure`)	Нет (выбирает 1 из коррелированной группы)	Зависит от модели (например, SVM плохо)	Да (оценивает важность в ансамбле)
Тип подхода	Гибрид (forward + backward)	Фильтрация (L1-регуляризация)	Итеративное удаление	Встроен в обучение
Требует коэффициентов модели	Нет	Да	Да	Да
Применим к Isolation Forest	Да	Нет (нелинейная модель)	Нет (IF не даёт коэффициентов)	Нет (отбор внешний)
Подходит для реального времени	Да	Ограничено	Нет	Да

Сравнивались следующие модели:

- Isolation Forest (IF) – метод обнаружения аномалий на основе случайных деревьев;
- Local Outlier Factor (LOF) – оценка локальной плотности;
- One-Class SVM (1SVM) – построение разделяющей гиперплоскости вокруг нормальных данных;
- Density – метод из библиотеки Etna, работающий с одним признаком (OutgoingTcpSyn) в скользящем окне.

Модели Median, DBSCAN и k-means показали $F1 < 0.03$ и были исключены из основного анализа.

Результаты приведены в табл. 3.

Табл. 3. Результаты тестирования различных методов подбора признаков и параметров.
Table 3. Results of testing various methods of feature and parameter selection.

Метод	Признаки	Параметры	avg. precision	avg. recall	avg. F1
IF	Baseline	Baseline	0.386	0.327	0.354
	Greedy	**Static**	**0.886**	**0.676**	**0.778**
	Lasso	Static	0.523	0.456	0.474
	RF	Static	0.841	0.653	0.751
	All	Dynamic	0.5	0.375	0.458
	Greedy	Dynamic	0.821	0.625	0.736
	Lasso	Dynamic	0.568	0.619	0.548
	RF	Dynamic	0.773	0.699	0.707
LOF	Baseline	Baseline	0.1722	0.507	0.175
	Greedy	Static	0.214	0.107	0.179
	Lasso	Static	0.143	0.107	0.131
	RF	Static	0.429	0.262	0.364
	All	Dynamic	0.074	0.068	0.070
	Greedy	Dynamic	0.071	0.036	0.060
	Lasso	Dynamic	0.143	0.071	0.119
	RF	Dynamic	0.227	0.163	0.189
1SVM	Baseline	Baseline	0.059	0.613	0.071
	Greedy	Static	0.043	0.726	0.052
	Lasso	Static	0.071	0.119	0.065
	RF	Static	0.027	0.191	0.032
	All	Dynamic	0.064	0.571	0.075
	Greedy	Dynamic	0.125	0.459	0.117
	Lasso	Dynamic	0.108	0.595	0.118
	RF	Dynamic	0.099	0.589	0.111

Наилучший результат показала модель Isolation Forest с признаками, отобранными модифицированным жадным алгоритмом, и статической настройкой гиперпараметров: $F1$ = 0.778. Это почти в 2.2 раза выше, чем в базовой конфигурации (All + Static, $F1$ = 0.354).

Отбор признаков является критичным: переход от полного набора признаков к подмножеству из 7 ключевых (OutgoingTcpSyn, IncomingPackets, OutgoingBytes, IncomingTcp, OutgoingUdp, IncomingIcmp, OutgoingArp) привёл к резкому росту Precision – с 0.386 до 0.886 при статической настройке. Динамическая настройка не улучшила результат для IF в условиях фиксированного пула ВМ. Это указывает на то, что для задачи обнаружения

кратковременных атак оптимальные гиперпараметры (например, contamination = 0.0001) остаются стабильными и не требуют масштабирования от N.

Модель Density, работающая только с OutgoingTcpSyn, достигла *F1* = 0.393, что подтверждает диагностическую ценность данного признака как основного индикатора SYN-флуда, однако уступает комбинированному подходу.

LOF и 1SVM продемонстрировали низкий *F1* из-за несбалансированности: LOF – низкий Recall, 1SVM – крайне низкий Precision (много ложных срабатываний).

Модифицированный жадный алгоритм отобрал 7 признаков из 18. Наибольший вклад в *F1* внесли:

- OutgoingTcpSyn – прямой индикатор SYN-флуда;
- IncomingPackets – отражает реакцию инфраструктуры на атаку (например, генерацию RST-пакетов);
- OutgoingUdp – ключевой для обнаружения UDP-флуда.

Это подтверждает, что даже простой набор метрик, если он грамотно отобран, может обеспечить высокую точность без доступа к payload.

Полученный результат (F1 = 0.778) сопоставим с современными работами в области обнаружения аномалий в зашифрованном трафике:

- в [3, 4] при использовании DPI и полного набора признаков F1 колеблется в диапазоне 0.70–0.85;
- новейший метод siForest [5] на аналогичных данных демонстрирует F1 ≈ 0.76.

Таким образом, предложенный подход не уступает современным ML-решениям, несмотря на использование только метаданных L2–L4.

6. Заключение

В условиях массового шифрования сетевого трафика традиционные методы глубокого анализа пакетов (DPI) теряют применимость, что делает актуальным переход к поверхностному анализу (SPI) на основе метаданных уровней L2–L4. В данной работе показано, что высокая точность обнаружения аномалий достижима даже без доступа к содержимому трафика, при условии грамотного отбора признаков и адаптивной настройки моделей машинного обучения.

Представленный NDIS-драйвер RuStatExt для Hyper-V Extensible Switch обеспечивает агрегацию метаданных в реальном времени и не вносит статистически значимых накладных расходов на производительность: тесты на канале 1 Gb/s с использованием iperf3 подтвердили отсутствие снижения пропускной способности при активном мониторинге.

Экспериментальная оценка показала, что наилучший результат в задаче выявления SYN- и UDP-флуда достигается при использовании модели Isolation Forest в сочетании с признаками, отобранными модифицированным жадным алгоритмом. При статической настройке гиперпараметров достигнута F1-мера 0,778, что почти в 2,2 раза превосходит результаты при использовании полного набора признаков и фиксированных параметров (F1 = 0,353). Динамическая настройка гиперпараметров, масштабируемая линейно от объёма данных, оказалась менее эффективной в условиях стабильного пула виртуальных машин. При этом она улучшает результат относительно базовой статической настройки на полном наборе признаков, но не превосходит лучшую статическую настройку при использовании отобранного набора признаков. Таким образом, динамическую настройку следует рассматривать как компонент, повышающий масштабируемость и переносимость параметров IF при росте или изменении инфраструктуры.

Предложенный подход обеспечивает точное, ресурсно-эффективное и масштабируемое обнаружение аномалий в зашифрованном трафике и может быть интегрирован в SOC-

системы облачных провайдеров для раннего выявления сетевых атак. Чтобы обеспечить воспроизводимость, мы сделали анонимизированный набор данных общедоступным [18].

Список литературы / References

[1]. Ахременко А.С., Стукал Д.К., Петров А.П. Сеть или текст? Факторы распространения протеста в социальных медиа: теория и анализ данных. Полис. Политические исследования, 2020, № 2, с. 73-91. DOI: 10.17976/jpps/2020.02.06. / Akhremenko A.S., Stukal D.K., Petrov A.P. Network or text? Factors of protest diffusion in social media: theory and data analysis. Polis. Political Studies, 2020, no. 2, pp. 73-91 (in Russian). DOI: 10.17976/jpps/2020.02.06.

[2]. Михайлов А.П., Петров А.П., Прончев Г.Б., Прончева О.Г. Моделирование спада общественного внимания к прошедшему разовому политическому событию. Доклады Академии наук, 2018, т. 480, № 4, с. 397-400. DOI: 10.7868/S0869565218160028. / Mikhailov A.P., Petrov A.P., Pronchev G.B., Proncheva O.G. Modeling the decline of public attention to a past single political event. Reports of the Russian Academy of Sciences, 2018, vol. 480, no. 4, pp. 397-400 (in Russian). DOI: 10.7868/S0869565218160028.

[3]. Taher K. A., Jisan B. M. Y., Rahman M. M. Network intrusion detection using supervised machine learning technique with feature selection. In: 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), IEEE, 2019, pp. 643-646.

[4]. Kumar K., Batth J. S. Network intrusion detection with feature selection techniques using machine-learning algorithms. International Journal of Computer Applications, 2016, vol. 150, no. 12.

[5]. Djidjev C. siForest: Detecting Network Anomalies with Set-Structured Isolation Forest. Department of Co mputer Science, University of Texas at Austin, 2024.

[6]. Zhang P., He F., Zhang H., Hu J., Huang X., Wang J., Yin X., Zhu H., Li Y. Real-Time Malicious Traffic Detection With Online Isolation Forest Over SD-WAN, IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2105-2119, 2023. DOI: 10.1109/TIFS.2023.3262121.

[7]. Mirsky Y., Doitshman T., Elovici Y., Shabtai A., Kitsune: An ensemble of autoencoders for online network intrusion detection, arXiv preprint. Available at: https://arxiv.org/pdf/1802.09089, accessed 21.03.2026.

[8]. Sharafaldin I., Lashkari A.H., Ghorbani A.A., Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy (ICISSp), 2018, pp. 108-116.

[9]. Ding Z., Fei M. An anomaly detection approach based on isolation forest algorithm for streaming data using sliding window. IFAC Proc. Vol., vol. 46, no. 20, pp. 12-17, 2013.

[10]. Kaushik A.K., Pilli E.S., Joshi R.C. Network forensic analysis by correlation of attacks with network attributes. In: Information and Communication Technologies: International Conference, ICT 2010, Kochi, Kerala, India, September 7-9, 2010. Proceedings. Springer, Berlin, Heidelberg, 2010, pp. 124-128.

[11]. Network-layer DDoS attack trends for Q2 2020: website. Available at: https://blog.cloudflare.com/ru-ru/network-layer-ddos-attack-trends-for-q2-2020/, accessed 02.12.2024.

[12]. Ramaswamy S., et al. Multiclass cancer diagnosis using tumor gene expression signatures. Proceedings of the National Academy of Sciences, 2001, vol. 98, no. 26, pp. 15149-15154.

[13]. Packet Flow through the Extensible Switch Data Path: сайт. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/network/packet-flow-through-the-extensible-switch-data-path, accessed 09.04.2024.

[14]. Benchmarking Methodology for Network Interconnect Devices: сайт. Available at: https://datatracker.ietf.org/doc/html/rfc2544, accessed 01.04.2024.

[15]. Vedula V., Lama P., Boppana R., Trejo L.A. On the detection of low-rate denial of service attacks at transport and application layers. August 2021. Available at: https://www.researchgate.net/figure/The-impact-of-a-pulse-shaped-SYN-flooding-attack-with-an-average-rate-of-25-rps-and_fig1_354227118, accessed 21.03.2026.

[16]. Kocyigit E. et al. Enhanced feature selection using genetic algorithm for machine-learning-based phishing URL detection. Applied Sciences, 2024, vol. 14, no. 14, article 6081.

[17]. Tsaplin N. S., Petrov A. P., Kovalev D. V. Greedy Feature Selection for Network Traffic Shallow Packet Inspection. In Proceedings of the XXVII International Conference on Data Analytics and Management in Data Intensive Domains (DAMDID / RDD 2025), 2025.

[18]. Цаплин Н. А., Петров А. П., Ковалев Д. Ю. Анонимизированный датасет сетевого трафика. GitHub, 2025. Доступно по адресу: https://github.com/ntsaplin/greedy_search_mod, дата обращения: 21.03.2026.

Информация об авторах / Information about authors

Никита Александрович ЦАПЛИН – аспирант ИПМ им. М.В. Келдыша РАН. Сфера научных интересов: применение машинного обучения в области анализа сетевого трафика.

Nikita Aleksandrovich TSAPLIN is a postgraduate student at the Keldysh Institute of Applied Mathematics (IPM) RAS. Research interests: application of machine learning in network traffic analysis.

Александр Пхоун Чжо ПЕТРОВ – доктор физико-математических наук, главный научный сотрудник ИПУ РАН. Сфера научных интересов: математическое моделирование в социальных науках.

Alexander Phoun Chzho PETROV – Dr. Sci. (Phys.-Math.), Chief Reseacher at the Institute of Control Sciences RAS. Research interests: mathematical modeling in social sciences.

Дмитрий Юрьевич КОВАЛЕВ – научный сотрудник ФИЦ ИУ РАН. Сфера научных интересов: применение машинного обучения в областях с интенсивным использованием данных.

Dmitry Yurievich KOVALEV – research scientist at FRC CSC RAS. Research interests: machine learning in data intensive domains.