RUVDS: отчёт по киберинцидентам

2025/2026

Общие положения

Киберинциденты и активность злоумышленников в целом были и остаются одними из самых значимых угроз, связанных с зависимостью бизнеса от цифровых решений. Ежедневно компании по всему миру сталкивается с риском многомиллиардных потерь, а их репутация находятся в зависимости от факторов, полностью контролировать которые становится всё сложнее.

Статистика основана на внутренних данных RUVDS:

в отличие от классических средств защиты, реагирующих на входящие атаки, система отслеживает аномалии, источником которых выступают виртуальные машины клиентов, блокируя их до нанесения ущерба внешним ресурсам.

Инфраструктура RUVDS объединяет **22 локации** по всему миру, вычислительные мощности RUVDS развернуты в дата-центрах уровня Tier IV со средним аптаймом 99,99%. Специфика работы хостинг-провайдера ставит его в уникальную позицию, вынуждая его контролировать не только входящий, но и исходящий трафик, для чего RUVDS внедрил **адаптивную модель поверхностного анализа пакетов (SPI).**

Ключевые выводы

По результатам анализа показателей за 2024-25 и 2025-2026 гг. мы зафиксировали двукратное снижение событий автоматической защиты и снижение событий с признаками SYN-флуда, почти двукратное снижение числа событий в день и рост объёмных аномалий в исходящем трафике.

Два сезона работы периметра безопасности RUVDS

	2024–25	2025–26
События автоматической защиты	11 500	5 822
События с признаками SYN-флуда	10 595	4 463
Автоматических блокировок при пересечении порога интенсивности	247	175
Ограничения по объёму исходящего трафика	658	1 184
В среднем событий в день	31	16

Повышение качества детектирования: внедрение адаптивной SPI повысило точность классификации до $F_1 \approx 0{,}97$, **сократив долю ложных срабатываний.**

80%

Рост ограничения по объёму исходящего трафика

58%

снижение событий с признаками SYN-флуда

49%

снижение событий автоматической защиты

Почти вдвое

снижено число событий в день

29%

снижение автоблокировок при пересечении порога интенсивности

31,97%

рост клиентского трафика



«В текущем виде наша адаптивная модель детектирования точнее отделяет аномалии от легитимных всплесков трафика — годом ранее, до внедрения адаптивной модели, мы регистрировали порядка 11 500 срабатываний. Но старая пороговая система не различала легитимные всплески и реальные угрозы, создавая высокий уровень ложных срабатываний. Новая модель точнее: число SYN-флуд-событий снизилось на 58% не потому, что атак стало меньше, а потому что детектор научился не реагировать на безобидные всплески. Но чувствительность системы к действительно опасным событиям выросла — объёмных аномалий зафиксировано на 80% больше, что связано с ростом качества детектирования на фоне естественного увеличения клиентского трафика».

— генеральный директор RUVDS Никита Цаплин.

Рыночный контекст

Картина, которую фиксирует RUVDS, не на 100% повторяет значения, которые наблюдают коллеги по рынку. Расхождения между источниками объясняются различиями в методиках: каждый провайдер измеряет атаки на свою клиентскую базу, со своими порогами детектирования и в своей точке наблюдения. По итогам 2025 года российский рынок защиты от DDoS-атак даёт противоречивую, но информативную картину:

Solar (Ростелеком-Солар)	560 тыс. DDoS-атак на российские компании за 9 месяцев 2025 г. — на 12 % меньше, чем за аналогичный период 2024 г Снижение связывается с перетоком атакующих к точечным и зондирующим атакам
Selectel	140 628 атак на клиентов облачной инфраструктуры за 2025 г. — на 25 % больше, чем в 2024 г. Максимальный объём одной атаки достиг 569 Гбит/с (+38 %), пиковая скорость — 193 млн пакетов/с (+16 %). Доля TCP SYN Flood выросла до 65 % (26 % годом ранее). Совокупная длительность атак — 22,7 тыс. часов
StormWall	Количество DDoS-атак в России выросло в 1,8 раза, в мире — в три раза. Зафиксирован резкий рост «ковровых» зондирующих атак (+83 %)

На этом фоне данные RUVDS занимают особое место: в отличие от перечисленных отчётов, мы измеряем не входящие атаки на клиентов, а исходящую аномальную активность из облака — события, в которых облачный ресурс является источником, а не целью.

В чем данные RUVDS согласуются со сводками рынка	**В чем сведения расходятся с рынком**
• SYN-флуд — доминирующий сетевой вектор (77 % событий у RUVDS; 65 % атак Selectel • Трафик «тяжелеет»: рост объёмных событий (+80 % у RUVDS) коррелирует с рекордными объёмами атак по данным Selectel • Общее снижение событий в российском сегменте фиксируется как минимум одним крупным игроком (Solar: −12 %)	Значительно более заметное общее снижение (−49%, у Solar −12 %) и противоположность тренду Selectel/ StormWall Это объясняется принципиально иным объектом наблюдения (исходящий, а не входящий трафик), иным составом правил и влиянием адаптивного детектирования, внедрённого в 2025 году

Методология

События регистрируются системой поверхностного анализа пакетов, работающей на уровне гипервизора (NDIS-драйвер RuStatExt, Свидетельство о государственной регистрации программы для ЭВМ № 202566819). Анализируются исключительно метаданные пакетов: IP-адреса, порты, TCP-флаги, объёмные и временные характеристики. Содержимое трафика не расшифровывается и не анализируется — это **принципиальное архитектурное решение, исключающее нарушение тайны связи.**

Событием считается однократное срабатывание автоматического порогового правила в пределах одного окна наблюдения.

Событие **не тождественно** «атаке» или «инциденту»: одна продолжительная атака может порождать несколько последовательных срабатываний

Длительная активность скомпрометированной ВМ — **десятки событий** за сутки, поэтому все цифры отчёта следует интерпретировать как объём сработавшей защиты, а не как число уникальных атак

Правило	Тип детектирующей аномалии	Окно	Реакция
SYN-флуд-подобная активность	Превышение порога интенсивности TCP SYN	20 мин	Регистрация события
Блокировка при высокой интенсивности	Превышение критического порога интенсивности	20 мин	Автоматическая блокировка источника
Ограничение по объёму трафика	Превышение порога исходящего трафика	24 ч	Ограничение скорости

Точные значения порогов не раскрываются по соображениям безопасности. Пороговые значения не являются статическими: система использует адаптивные механизмы, учитывающие профиль сетевой активности (Цаплин Н.А. Адаптивный алгоритм обнаружения вредоносного сетевого трафика // Препринты ИПМ им. М.В.Келдыша. 2026. № 58. 24 с. (https://keldysh.ru/papers/2026/prep2026_58.pdf)

Примечания:

- Все три правила контролируют исходящий трафик — отчёт отражает аномальную активность ресурсов внутри облака, а не входящие атаки на клиентов. Прямое сопоставление с отчётами, измеряющими входящие атаки (Solar, Selectel, StormWall), некорректно.
- Пороговые значения, используемые для обучения моделей определения аномалий, не изменялись в 2024-2025 гг.
- В 2025 г. внедрена адаптивная модель детектирования, что могло повлиять на число регистрируемых событий.
- Помесячные, отраслевые и географические распределения в текущей версии отчёта не приводятся.

Важное методологическое ограничение

RUVDS фиксирует снижение общего числа событий защиты **на 49% год к году**. Однако мы не приписываем это снижение исключительно внедрению SPI-системы.

Сокращение ложных срабатываний

Адаптивная модель детектирования ($F_1 \approx 0{,}98$) точнее отделяет аномалии от легитимных всплесков трафика, поэтому часть «событий» 2024 года могла не являться реальными угрозами Снижение в этом случае отражает не ослабление атак, а улучшение точности инструмента

Ускорение автоматической реакции

Блокировка сокращает число повторных срабатываний по одной и той же атаке: одно событие там, где раньше было несколько

Изменения в клиентской базе и профилях нагрузки

Внешние факторы

Общее изменение ландшафта угроз в РФ
(Solar фиксирует –12 % атак за 9 месяцев 2025 г.; возможен переток атакующих к другим векторам, не охватываемым нашими правилами)

На итоговую цифру могли повлиять несколько факторов:

Без контролируемого эксперимента разделить вклад перечисленных факторов невозможно. Мы рассматриваем наблюдаемое снижение как факт, заслуживающий дальнейшего изучения, а не как доказательство изолированной эффективности конкретной технологии. При этом точность детектирования (F_1) и скорость автоматической реакции являются измеряемыми и подтверждёнными характеристиками SPI-системы.

КЕЙС

ВМ клиента в зоне доступности X начала генерировать исходящий поток TCP SYN со скоростью, превышающей порог обнаружения.

В течение 20-минутного окна событие зафиксировано системой поверхностного анализа. Клиенту автоматически направлено уведомление.

При разборе инцидента на ВМ обнаружены следы компрометации / непреднамеренная активность приложения. Ресурс изолирован, повторных событий не зафиксировано.

Ключевые наблюдения

SYN-флуд: доминирующий, но отступающий вектор

События, характерные для SYN-флуда, составляют 77 % всех срабатываний 2025 года — это согласуется с данными Selectel, где доля TCP SYN Flood выросла с 26 % до 65 %. Годовое снижение числа SYN-событий в облаке RUVDS (–58 значительно глубже общерыночного и, вероятно, сочетает несколько причин: реальное сокращение SYN-активности, отсев ложных срабатываний адаптивной моделью и сокращение «хвостов» событий за счёт быстрой блокировки.

Рост «объёмных» событий: +80 % за год

Число ограничений по объёму исходящего трафика выросло с 658 до 1 184, а их доля в структуре событий увеличилась с 6 % до 20 %. Рост может объясняться двумя классами причин:

- Легитимный рост нагрузки: дата-интенсивные сервисы (видео, бэкапы, AI/ML-вычисления, файловые хранилища) всё чаще приближаются к порогу/
- Абьюз и вовлечение в атаки: скомпрометированные или неправомерно используемые ВМ, участвующие в объёмных DDoS-атаках, рассылках и проксировании.

Облако как плацдарм

Все три контролируемых правила относятся к исходящему трафику. Это осознанный выбор модели мониторинга: провайдер отвечает не только за то, чтобы клиента не атаковали, но и за то, чтобы из облака не атаковали других. События 2024–2025 годов подтверждают: облачные ресурсы периодически вовлекаются в подготовку или проведение внешних атак — и автоматическое обнаружение на уровне гипервизора позволяет ограничивать такую активность до эскалации, не нарушая тайну связи.

Окно реакции

По данным отрасли, до 83 % атак уровня L3/L4 укладываются в первые 30–60 минут (Selectel, 2025). Окно наблюдения и автоматическая реакция RUVDS спроектированы так, чтобы укладываться в этот интервал – событие фиксируется, а при пересечении жёсткого порога блокировка выполняется без участия оператора.

Основные рекомендации

По итогам начального периода эксплуатации системы и на основе проведенного анализа полученных результатов сформулированы рекомендации, для клиентов, включающие пять основных категорий:

- **Контролируйте не только входящий, но и исходящий трафик.** Компрометация одной ВМ способна превратить её в плацдарм для атак — с репутационными и правовыми последствиями для клиента.
- **Настройте мониторинг аномалий трафика на своих ВМ.** Резкий рост исходящих пакетов или объёма означает либо новую легитимную нагрузку, либо компрометацию. Оба случая требуют реакции.
- **Уведомляйте провайдера о планируемой «тяжёлой» нагрузке в виде миграции, массовых бэкапов, раздач крупных файлов заранее (за неделю).** Это позволит исключить ложные срабатывания ограничений по объёму.
- **Настройте фаервол (на уровне хоста или в панели облачного провайдера) так, чтобы весь исходящий трафик был заблокирован по умолчанию.** Открывайте только те порты, которые необходимы для работы конкретных приложений.
- **Реагируйте на уведомления системы защиты.** Событие фиксируется автоматически, но разбор причины и устранение уязвимости остаётся на стороне клиента.
- **Поддерживайте ПО и учётные данные в актуальном состоянии.** Значительная часть вовлечений облачных ресурсов в атаки начинается с устаревшего ПО и подобранных паролей.

Определения

Событие — срабатывание одного порогового правила в одном окне наблюдения.

SYN-флуд-подобная активность — исходящий поток TCP SYN, превышающий порог интенсивности (сотни пакетов/с) в течение 20 минут; включает как SYN-флуд-атаки, так и агрессивное сетевое сканирование.

Блокировка — автоматическое отключение источника при превышении критического порога интенсивности (тысячи пакетов/с) в течение 20 минут.

Ограничение — снижение скорости исходящего трафика источника при превышении порога объёма (сотни ГБ) за 24 часа.

SPI (Shallow Packet Inspection) — поверхностный анализ пакетов: извлечение и классификация на основе заголовков L2–L4 без доступа к содержимому трафика.

RuStatExt — NDIS-драйвер статистики сетевых пакетов на уровне гипервизора, используемый в системе защиты облака RUVDS (Свидетельство о государственной регистрации программы для ЭВМ № 202566819 от 11.07.2025).

Источники

Цаплин Н.А. **Адаптивный алгоритм обнаружения вредоносного сетевого трафика** // Препринты ИПМ им. М.В.Келдыша. 2026. № 58. 24 с. (https://keldysh.ru/papers/2026/prep2026_58.pdf)

Solar: **Отчет о DDoS-атаках на онлайн-ресурсы российских компаний за 9 месяцев 2025 года** (https://rt-solar.ru/analytics/reports/6170/)

Selectel: «**Атаки носят массовый характер»: аналитический отчет по DDoS за 2025 год**» (https://selectel.ru/blog/ddos-attack-report-2025/)

StormWall: **DDoS-атаки в 2025 году: что изменилось в мире и России** (https://stormwall.pro/resources/blog/ddos-trendy-2025)



support@RUVDS.com
8 (800) 775-97-42
+7 (495) 135-10-99