

Результаты опроса по сетевой безопасности 2025

Основные выводы и инсайты

148

Представителей организаций по всей России приняли участие в исследовании

В исследовании приняли участие 148 представителей организаций по всей России – от малого бизнеса до крупных предприятий, как в коммерческом, так и в государственном секторе. Выборка охватывает широкий круг заказчиков и партнёров из ключевых отраслей, включая ИТ, науку, образование, финансы и здравоохранение. В опросе представлены специалисты, инженеры и управленцы, отвечающие за ИТ и информационную безопасность. Такая структура позволяет получить объективную оценку состояния ИБ-инфраструктуры на российском рынке.

60%

Организаций завершили или завершат переход на отечественные сетевые решения

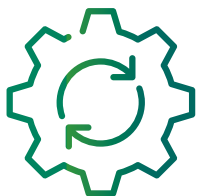
Завершение этапа технологического перехода

Большинство организаций (60%) завершили или завершат переход на отечественные сетевые решения до конца 2025-го года. В ближайшей перспективе акцент может сместиться с соответствия базовым требованиям на оценку эксплуатационных характеристик и устойчивости решений в реальных условиях.



Рост потребности в расширенной функциональности

Участники исследования демонстрируют интерес к возможностям, выходящим за рамки базовой фильтрации трафика. Это включает в себя IDS/IPS, поведенческий анализ, интеграцию с системами реагирования и использование Threat Intelligence.



Запрос на баланс между производительностью и доступностью

Выбор решений с производительностью до 1–10 Гбит/с остаётся типичным. Для NGFW до 10 Гбит/сек, а для криптошлюза до 1 Гбит/сек. Это указывает на устойчивый спрос на надёжные решения среднего уровня с хорошим соотношением цена/качество.



Эволюция критериев выбора вендора

В условиях насыщенного предложения и завершения импортозамещения компании уделяют всё больше внимания не только техническим характеристикам, но и таким факторам, как удобство администрирования, полнота документации, гибкость лицензирования и уровень технической поддержки.

Импортозамещение

Многие участники (47%) указали, что уже полностью перешли на отечественные решения в сегменте межсетевых экранов и криптошлюзов. Те, кто ещё в процессе замещения, планируют завершить переход в 2026-м году и позднее. Варианты с комбинированным использованием зарубежных и российских решений встречаются всё реже.

Межсетевой экран какого производства вы используете?



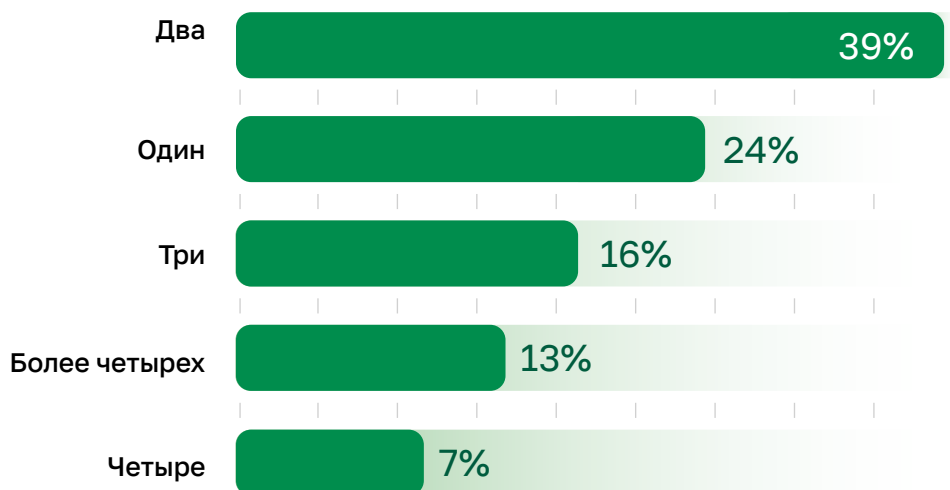
Какие у вас планы по замене иностранных межсетевых экранов?



Процессы импортозамещения в сегменте сетевой безопасности близки к завершению. Ожидается постепенное смещение внимания с технической замены на эксплуатационные характеристики и удобство интеграции.

Сценарии использования

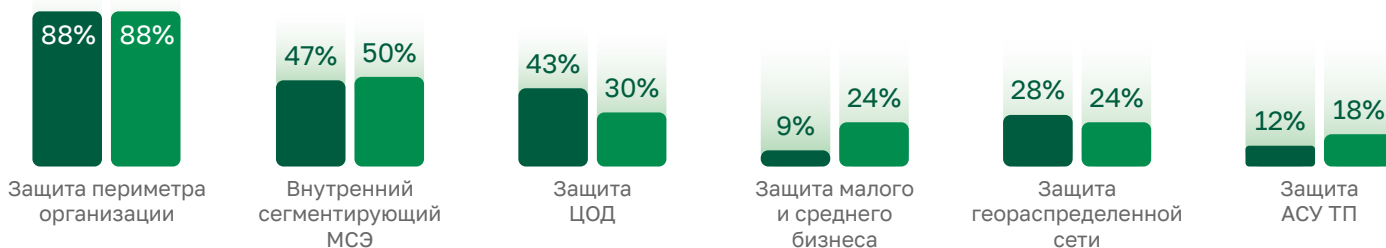
- Только 24% используют одного вендора по сетевой безопасности. Большинство рынка использует двух и более.



- Сценарии использования NGFW и VPN-шлюзов почти не изменились по сравнению с нашим прошлогодним исследованием.

NGFW

88% респондентов используют NGFW для защиты периметра организации, а 50% - для внутреннего сегментирования.



VPN-шлюзы

83% применяют для удаленного доступа, а 60% для объединения площадок. Отмечаем рост на потребность в организации защищенного удаленного доступа.



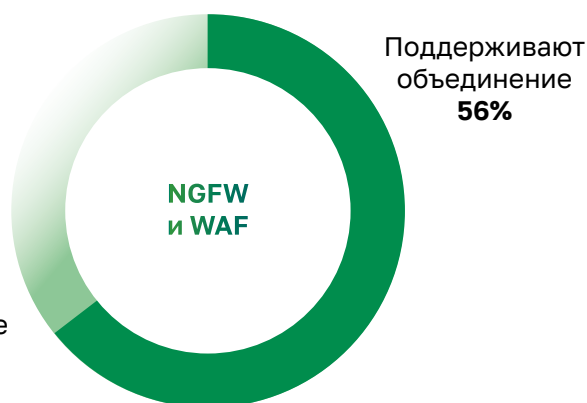
Конвергенции

■ Отношение к экосистемам в кибербезопасности:



Только 30% опрошенных полностью поддерживают экосистемы кибербезопасности, т.е. зависимость от одного вендора. 53% респондентов хотят вендорнезависимую экосистему ИБ.

■ Интеграция NGFW и криптошлюзов:



30% респондентов видят ограничения в объединении функционала NGFW и криптошлюзов в рамках одной платформы. Для 19% ограничения по эксплуатации СКЗИ не позволят эффективно эксплуатировать NGFW, а 11% считают, что это разные средства, которые эксплуатируются разными специалистами. Ещё 12% не знакомы с данным вопросом.

30% респондентов видят ограничения в объединении NGFW и WAF. 17% респондентов ответили, что это разные средства, которые эксплуатируются разными специалистами. 13% не видят в этом необходимости. Ещё 14% не знакомы с данным вопросом.

Функционал

■ Влияние открытого кода на выбор МСЭ:

47%

Респондентов в 2024 году считали, что открытый код не значим при выборе МСЭ

34%

Респондентов в 2025 году не считают наличие компонентов с открытым исходным кодом значимым при выборе МСЭ

33%

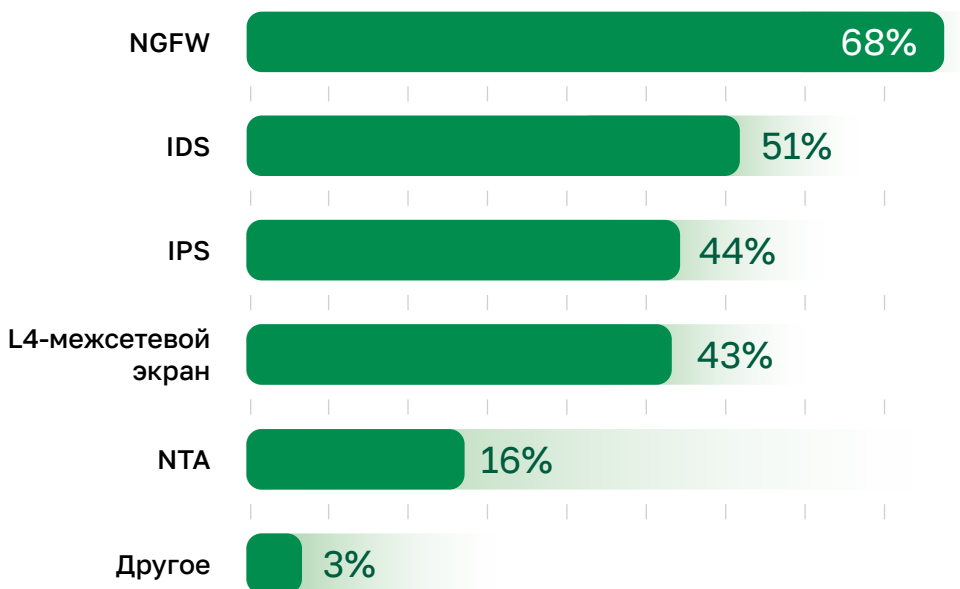
Респондентов ответили, что наличие открытого исходного кода в МСЭ незначительно, но повлияет на его выбор

22%

Респондентов придерживаются мнения, что это важный фактор

■ СЗИ для защиты внутренней сети предприятия:

Чаще всего используют только NGFW, также предпочитают связку МСЭ, IDS и IPS. Только 16% опрошенных используют NTA-системы для мониторинга и анализа трафика. Почти половина опрошенных предпочитают использовать системы класса IDS/IPS.



Тоже подтверждается ответами респондентов на следующий вопрос.

■ Механизмы защиты внутренней сети:

86%

Используют фильтрацию трафика между сегментами

77%

Используют обнаружение и блокировку атак

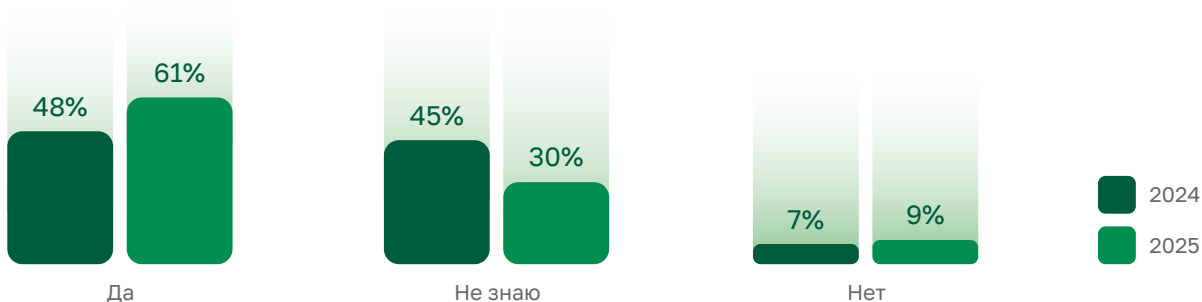
75%

Применяют журналирование трафика

Функционал

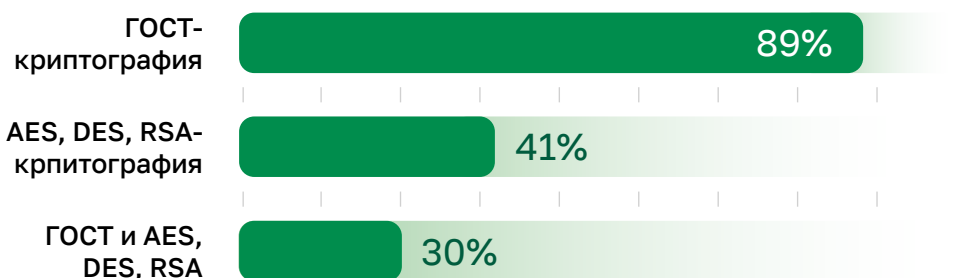
■ Использование индикаторов компрометации и интерес к Threat Intelligence:

С 2024-го года повысилась доля респондентов, которым важны индикаторы компрометации, а также снизилось число опрошенных, которые не однозначно к ним относились. Threat Intelligence в NGFW становится популярнее, более 50% респондентов хотели бы видеть в своих продуктах такую интеграцию.



■ Алгоритмы шифрования для Site-to-Site VPN:

Тренд на завершение импортозамещения прослеживается и в ответах на данный вопрос. Теперь большинству необходима поддержка ГОСТ-криптографии при построении Site-to-Site VPN.



■ Операционные системы для VPN-клиентов:

96%

Клиентов требуют поддержку **Windows**

93%

Клиентов требуют поддержку **Linux**

39%

Клиентов требуют поддержку мобильных платформ **Android**

21%

Клиентов требуют поддержку **iOS** (менее актуальна)

Функционал

89%

Опрошенным необходима реализация комплаенс-контроля соответствия удаленного рабочего места

Комплаенс-контроль соответствия удаленного рабочего места установленной политике безопасности перед подключением по VPN: Для 89% опрошенных необходима реализация комплаенс-контроля соответствия удаленного рабочего места установленной политике безопасности перед подключением по VPN.

- Схемы аутентификации удаленных пользователей вы используете для защищенного удаленного доступа:

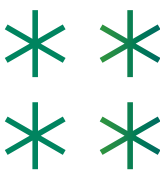
Наиболее часто используют «Логин и пароль» (86%), а также активно используются различные сертификаты (50% и 43%). Многофакторная аутентификация применяется реже (36% и 18%). В данном вопросе у респондентов была возможность множественного выбора, следовательно многие совмещают использование различных средств аутентификации.



86%
«Логин и пароль»



50%
Сертификаты на компьютере пользователя



36%
Получение одноразового пароля



43%
Сертификат на USB-токене



18%
Push в мобильном приложении

Функционал

■ Основные проблемы NGFW:

39%

Стабильность

34%

Простота администрирования

37%

Производительность

28%

«Всего хватает»

■ Безопасность публикуемых приложений:

Здесь респонденты посчитали одинаково важными все 4 варианта:

- защита от атак
- защита от DDoS
- разграничение прав доступа к защищаемым ресурсам
- предоставление доступа к конкретным приложениям, а не сетям.

68%

Защита от атак

64%

Защита от DDoS

59%

Разграничение прав доступа к защищаемым ресурсам

55%

Предоставление доступа к конкретным приложениям, а не сетям

3%

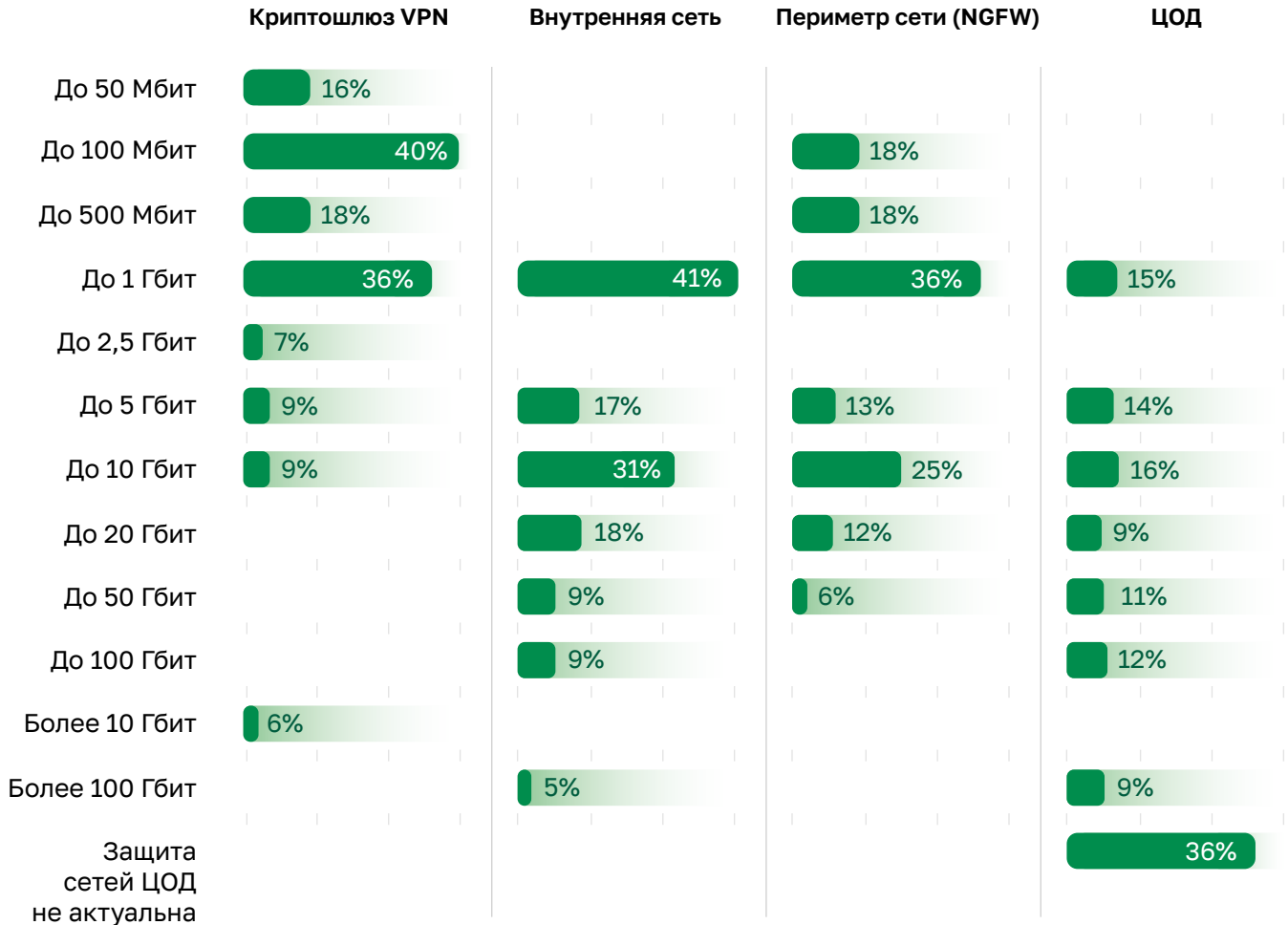
Другое

Производительность

- Выбор решений с производительностью до **1–10 Гбит/с** остаётся типичным. Не все сегменты нуждаются в высокопроизводительных решениях.

Следует отметить рост требований к производительности внутренних систем сегментации (**31% требуют 10 Гбит/с**), что превышает потребности периметровых решений и указывает на архитектурные изменения в подходах к безопасности.

- Ключевые тенденции:
 - Рост требований к внутренним сетям: 31% требуют 10 Гбит/с для сегментации.
 - Консервативные потребности VPN: 40% достаточно 100 Мбит/с для криптошлюзов.
 - Умеренные требования к периметру: 36% нуждаются в 1 Гбит/с для NGFW.
 - Дифференциация по уровням: Разные требования для разных уровней защиты.





г. Москва, 115230
1-й Нагатинский проезд, д. 10, стр. 1
+7 (495) 982-30-20
info@securitycode.ru
www.securitycode.ru