



XSpider PRO

Зачем защищать инфраструктуру

Атак становится больше

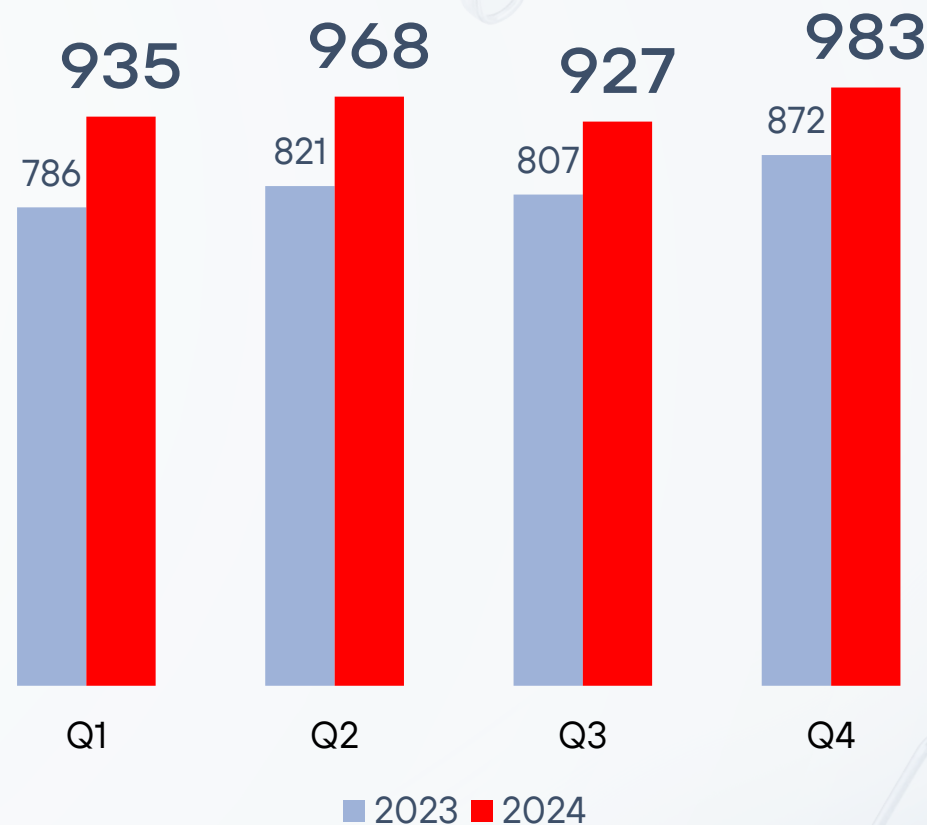
3800+

кибератак

выросло число атак за один год

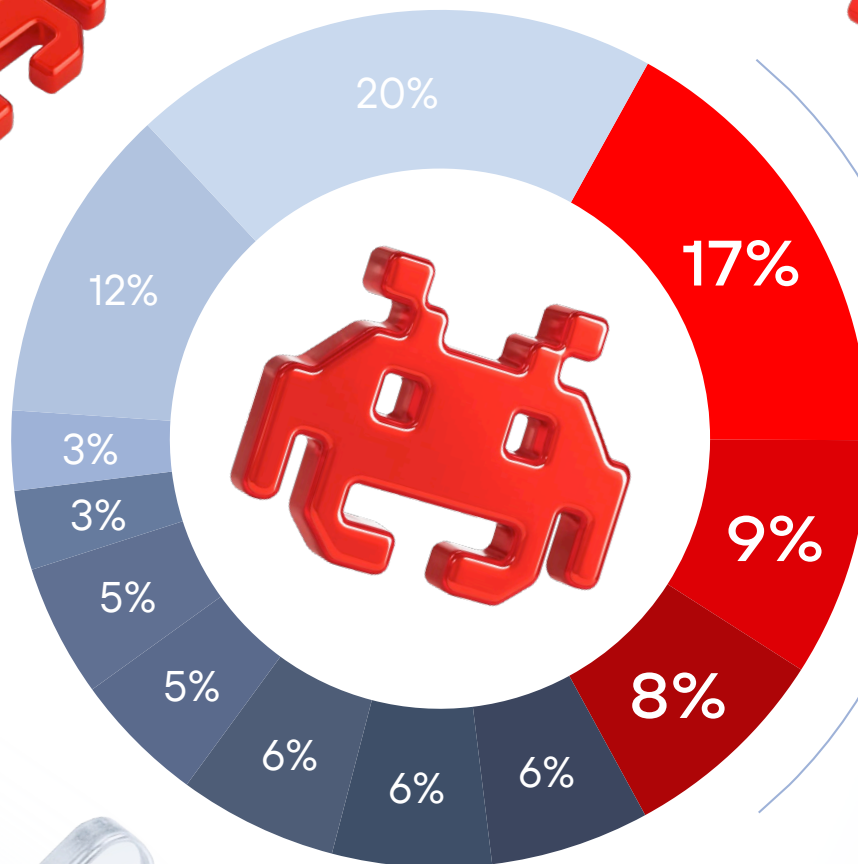
на 14%

выросло число атак за один год



Кто под угрозой

- Госучреждения
- Промышленность
- IT-компании
- Финансовые организации
- Медицинские учреждения
- Телекоммуникации
- Торговля
- Наука и образование
- Транспорт
- Сфера услуг
- Другие
- Без привязки к отрасли



**Госсектор,
промышленность
и IT-компании**

подвергались атакам
в 2024 году чаще всего

Уязвимости — угроза для компании



Использование ВПО



Социальная инженерия



Эксплуатация уязвимостей



Компрометация учетных данных



Компрометация цепочки поставок
или доверенных каналов связи



Другие



■ Организации ■ Частные лица

32%

атак

реализуются через
эксплуатацию
уязвимостей



К чему приводят атаки?

По данным аналитики от Positive Technologies за 2024 год



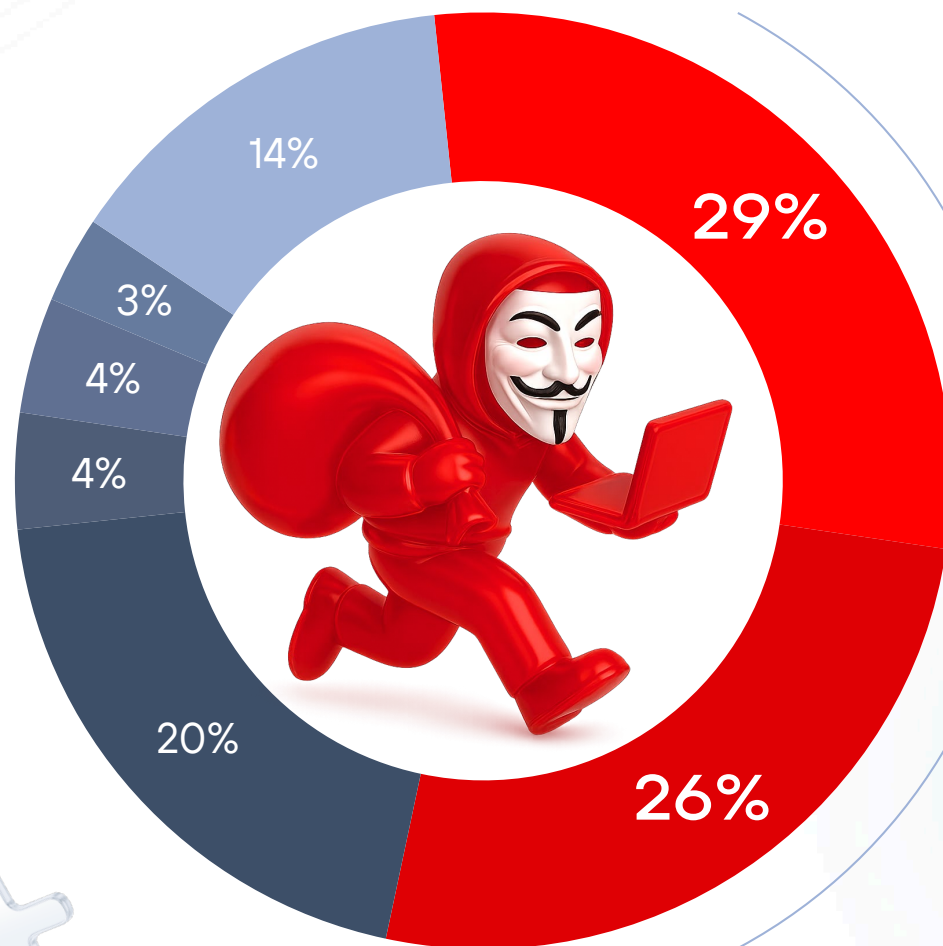
Чаще всего в 2024 году кибератаки оборачивались **утечкой конфиденциальных данных** и нарушением деятельности компании



Что крадут



- Персональные данные
- Учетные данные
- Коммерческая тайна
- Данные платежных карт
- Переписка
- Медицинская информация
- Другая информация



**Персональные
и учетные
данные,
коммерческая
тайна**

были в топе интересов
злоумышленников в 2024 году

Почему важно предотвратить утечку данных



Новый закон:

штрафы за утечку персональных данных

30 мая 2025 года

вступит в силу Федеральный закон от 30.11.2024 № 420-ФЗ

- ❗ **Оборотные штрафы до 500 млн руб.**
(до 3% от выручки)
- ❗ **Повторные утечки — штраф до 500 млн руб.**
- ❗ **Неуведомление Роскомнадзора — штраф до 3 млн руб.**
- ❗ **Юрлица, ИП, должностные лица — ответственность для всех**

Утечка персональных данных = серьезные финансовые потери

Требуются реальные меры для обеспечения информационной безопасности

Необходимо вовремя уведомлять об утечках Роскомнадзор

Как защититься — выявлять и устранять уязвимости



Контролировать безопасность систем

- + Своевременно обновлять используемое программное обеспечение по мере выхода патчей
- + Контролировать появление небезопасных ресурсов на периметре сети
- + Регулярно проводить инвентаризацию ресурсов, доступных для подключения из интернета

Защищать данные

- + Не допускать использование простых паролей
- + Использовать разные учетные записи и пароли для доступа к различным ресурсам

Использовать эффективные средства защиты

- + Регулярно проводить анализ защищенности инфраструктуры для выявления новых векторов атак и оценки эффективности мер защиты
- + Автоматизировать процесс выявления уязвимостей

Что мешает находить и устранять уязвимости



Ложные срабатывания

Множество сканеров уязвимостей часто ошибаются, поэтому обнаруживают несуществующие уязвимости или пропускают важные

Редко добавляется информация о новых уязвимостях

Часто обновления информации о новых угрозах происходит с большой задержкой

Ограниченное покрытие софта

Многие решения для сканирования не могут искать уязвимости в большом количестве ПО, что приводит к появлению «дыр» в инфраструктуре

Отсутствие понятной отчетности

Часто сканеры уязвимостей выдают плохо читаемые результаты, в которых сложно разобраться

Отсутствие приоритизации уязвимостей

Недостаточно получить информацию об уязвимостях, нужно оценивать их влияние на бизнес, чтобы устранять самые опасные в первую очередь

Неполное покрытие активов

Зачастую сканеры уязвимостей покрывают не всю инфраструктуру, из-за чего из процесса сканирования могут выпадать критически важные участки



Решение
Positive Technologies

XSpider PRO



Сканер безопасности нового поколения,
который покажет полную картину
уязвимостей в вашей инфраструктуре



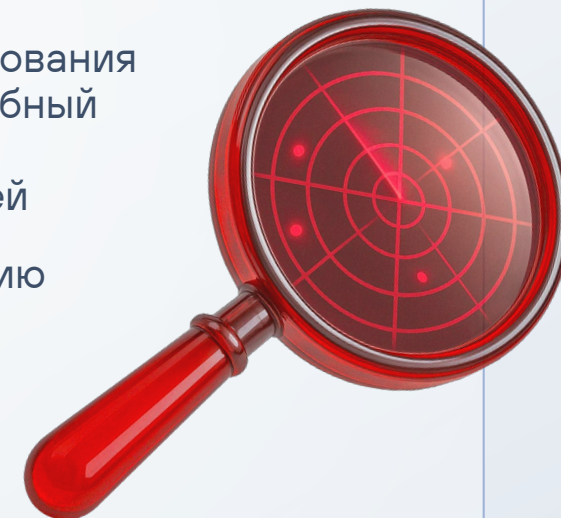
Обнаруживает уязвимости в сети и системах



- + Выявляет уязвимости на рабочих станциях, серверах и сетевых устройствах
- + Анализирует популярные ОС (Windows, Linux) на наличие известных уязвимостей
- + Сканирует веб-серверы и базы данных чтобы выявить уязвимости, связанные с некорректными настройками, устаревшими версиями ПО или избыточными правами доступа

Дает рекомендации по устранению

- + После завершения сканирования продукт генерирует подробный отчет с полным перечнем обнаруженных уязвимостей
- + Предоставляет информацию по всем уязвимостям и рекомендации по их устранению



Путь зрелости: от сканера к VM



XSpider

Базовый сетевой
сканер

1



XSpider PRO

Расширенный сканер
с элементами управления
уязвимостей

2



MaxPatrol VM

Система управления
уязвимостями

3

Преимущества XSpider PRO



Обширная база уязвимостей

Регулярно пополняем базу уязвимостей (БДУ ФСТЭК, CVE, OWASP Top 10, база Positive Technologies). Обнаруживаем уязвимости, в том числе в отечественных ОС и популярном ПО

Низкие аппаратные требования

Мы сделали «легкий» сканер, чтобы вы могли быстро и эффективно внедрять его в любую инфраструктуру без дополнительных затрат

Низкий уровень ложных срабатываний

Высокая точность и надежность результатов сканирования, чтобы не терять время на ошибочные срабатывания и сосредоточиться на исправлении реальных угроз

Несколько режимов работы

Продукт может работать в двух режимах: пентест и аудит, что позволяет оперативно оценить текущее состояние защищенности инфраструктуры

Работа на отечественных ОС

Сканер полностью адаптирован для работы на российских ОС. Это позволяет легко внедрять продукт в импортозамещенную инфраструктуру

Сканирование Docker-контейнеров и веб-приложений

Проверяет сайты и окружение, в котором они работают, чтобы найти и устранить уязвимости до того, как ими воспользуются злоумышленники

Что изменилось в продукте



	XSpider PRO	XSpider 7.8
Сканирование в режиме Pentest	+	+
Сканирование в режиме Audit	+	-
Поиск уязвимостей в веб-приложениях	+	-
Поиск уязвимостей в Docker-контейнерах	+	-
Актуализация информации о новых уязвимостях в поддерживаемом ПО	+	-
Поддержка нового ПО для поиска уязвимостей	+	-
Инвентаризация инфраструктуры	Выгрузка информации про инфраструктуру в отчет	Базовая инвентаризация
Консоль управления	Легкий веб-интерфейс	Тяжелый клиент
Поддержка ОС	Linux	Только Windows
Лицензирование	По сканируемым узлам и функциональности	По сканируемым IP-адресам
Сертификация ФСТЭК	Ожидаем к концу 2025 года	Заканчивается в конце 2025 года Техподдержка до конца 2030 года

Функциональные возможности Xspider PRO



XSpider PRO

Сканирование в режиме Pentest	Да
Сканирование в режиме Audit	Да
Поиск уязвимостей в веб-приложениях	Да
Поиск уязвимостей в Docker-контейнерах	Да
Актуализация информации о новых уязвимостях в поддерживаемом ПО	Да
Поддержка нового ПО для поиска уязвимостей	Да
Инвентаризация инфраструктуры	Выгрузка информации про инфраструктуру в отчет
Критерии приоритизации уязвимостей	CWE, CVSS, БДУ ФСТЭК, НКЦКИ
Консоль управления	Легкий веб-интерфейс
Поддержка ОС	Linux
Лицензирование	По сканируемым узлам и функциональности
Сертификация ФСТЭК	Ожидаем к концу 2025 года



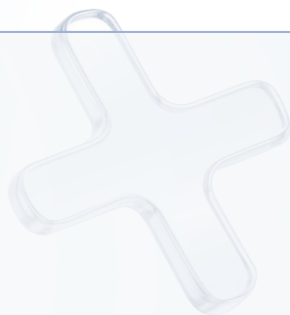
**Как это
работает**

Два режима работы



Pentest

- + Поиск уязвимостей
- + Сетевое сканирование
- + Сканирование веб-приложений
- + Инвентаризация



Audit

- + Системные проверки
- + Анализ ПО
- + Инвентаризация

Метод черного ящика



Метод белого ящика



Создавайте задачи на сканирование



XPro

Задачи

Отчеты

Параметры ▾

Создание задачи на сбор данных

Название

Pentest Scan 21.05

[Добавить описание](#)

Параметры сбора данных

Импорт

Экспорт

Профиль

Full PenTest ▾

PostgreSQL

SAP Sybase ASE

SAP через DIAG

SAP через RFC

Symantec pcAnywhere

Virtual Network Computing

VMware vSphere

Windows через Microsoft SQL S...

По протоколу FTP

По протоколу NetBIOS

По протоколу POP3

По протоколу RDP

Общие параметры сканирования

Метод сканирования портов

SYN-пакеты

Подключение

☒

Искать сетевые принтеры ⓘ

Сохранить

Сохранить и запустить ▾

Отмена

Создавайте задачи на сканирование



The screenshot shows the XPro web interface. The top navigation bar includes the XPro logo and links for 'Задачи' (Tasks), 'Отчеты' (Reports), and 'Параметры' (Parameters). The main content area is divided into two sections. The top section, 'Параметры сканирования' (Scanning Parameters), lists protocols: POP3, RDP, SIP, and SMTP, with a toggle for 'Показывать дополнительные параметры' (Show additional parameters). The bottom section, 'Цели сбора данных' (Data collection targets), provides examples of valid addresses (IP v4/v6, IP ranges, subnets, and FQDN) and includes input fields for 'Включить' (Include) and 'Исключить' (Exclude) targets. The 'Включить' field contains '192.168.0.0' and a dropdown arrow. Below it is a checkbox for 'Выполнить обнаружение узлов до начала сбора данных' (Perform node discovery before data collection). The 'Исключить' field is empty. At the bottom right, there are three buttons: 'Сохранить' (Save), 'Сохранить и запустить' (Save and run), and 'Отмена' (Cancel).

Параметры сканирования

По протоколу POP3
По протоколу RDP
По протоколу SIP
По протоколу SMTP

☐ Показывать дополнительные параметры

Цели сбора данных

Примеры допустимых адресов:

- IP-адрес v4 или v6 (192.168.0.0 или fe80::)
- диапазон IP-адресов (192.168.0.1-192.168.0.25)
- подсеть (192.168.0.0/24 или fe80::/10)
- FQDN (example.tuc.noao.ru)

Включить

☐ Выполнить обнаружение узлов до начала сбора данных

Исключить

Действия:

Отслеживайте статус задач



XPro

Задачи

Отчеты

Параметры

Задачи на сбор данных

+ Создать задачу

Копировать

Изменить

Расположение

Удалить

Запустить

Пауза

Остановить

Импорт

Группы задач

Root

Unmanaged Tasks

Все задачи

Статус	Название	Цели	Профиль
Завершена	bsvm3.mp10.ptsecurity.ru	bsvm3.mp10.ptsecurity.ru	Windows Audit
Не запускалась	XPro Test	11.11.11.11	Http Servers Disc
Не запускалась	Pentest Scan 21.05	192.168.0.0	Full PenTest

Всего 3 задачи, выбрана 1 задача

Pentest Scan 21.05

Создана 21 мая, 16:35

Статус Не запускалась

Цели сбора данных

Включить 192.168.0.0

Параметры сбора данных

Профиль Full PenTest

Модуль pentest

История запусков

Выпускайте отчеты по итогам сканирования



XPro

Задачи

Отчеты

Параметры

Отчеты

+ Создать отчет

Выпустить копию

Удалить

Прервать выпуск

Список отчетов

Статус отчета	Название	Задача	Тип	Формат	Д
✓ Выпущен	Уязвимости по узлам (през...	Задача сканирования 8ac9...	Уязвимости по узлам (през...	PDF	18 июл
Не выпущен	Уязвимости по узлам (09.0...	Задача сканирования 34e1...	Уязвимости по узлам	XLSX	9 июл
⌚ Ожидает выпуска	Уязвимости по узлам (през...	Задача сканирования 1c70...	Уязвимости по узлам (през...	HTML	2 июл
Не выпущен	Количество уязвимостей п...	Задача сканирования 7d6bf	Количество уязвимостей п...	XLSX	15 июл
Не выпущен	Количество уязвимостей п...	Задача сканирования 747f...	Количество уязвимостей п...	XLSX	20 июл
⌚ Выпускается	Инвентаризация узлов (04...	Задача сканирования 6914...	Инвентаризация узлов	XLSX	4 июл
⌚ Ожидает выпуска	Инвентаризация узлов (21...	Задача сканирования 8f4a0f	Инвентаризация узлов	XLSX	21 июл
Не выпущен	Количество уязвимостей п...	Задача сканирования 5c16...	Количество уязвимостей п...	XLSX	15 июл
⌚ Выпускается	Инвентаризация узлов (22...	Задача сканирования 36db...	Инвентаризация узлов	JSON	22 июл
✓ Выпущен	Операционные системы и ...	Задача сканирования 67ea...	Операционные системы и ...	XLSX	13 июл
Не выпущен	Дифференциальный отчет ...	Задача сканирования 12aa...	Дифференциальный отчет ...	XLSX	17 июл
✓ Выпущен	Количество уязвимостей п...	Задача сканирования 1966...	Количество уязвимостей п...	XLSX	12 июл
⌚ Выпускается	Операционные системы и ...	Задача сканирования 52e6...	Операционные системы и ...	XLSX	3 июл
Не выпущен	Уязвимости по узлам (01.0...	Задача сканирования 8e724	Уязвимости по узлам	XLSX	1 июл
⌚ Ожидает выпуска	Дифференциальный отчет ...	Задача сканирования 393f3f	Дифференциальный отчет ...	XLSX	19 июл
Не выпущен	Уязвимости по узлам (през...	Задача сканирования 3da6...	Уязвимости по узлам (през...	PDF	4 июл

Всего 50 отчетов, выбран 1 отчет

» Уязвимости по узлам (презентация) (18.07.20...

Скачать

Уязвимости по узлам (презентация) (18.07.2025).pdf

Статус

✓ Выпущен

Дата создания

18 июл., 13:00

Тип

Уязвимости по узлам (презентация)

Формат

pdf

Выбранные результаты

Задача

Задача сканирования 8ac970

Результат

2 июл., 13:00