XSpider

Выяви уязвимость в сетевых ресурсах до того,
как это будет сделано злоумышленниками

Обеспечиваем практическую кибербезопасность

20 лет

опыта исследований
и разработок

1500+ сотрудников

в компании: инженеров по ИБ,
разработчиков, аналитиков
и других специалистов

250+ экспертов

в нашем
исследовательском
центре безопасности

200+

обнаруженных
уязвимостей
нулевого дня в год

250+

аудитов безопасности
корпоративных систем
делаем ежегодно

50%

всех уязвимостей
в промышленности и телекомах
обнаружили наши эксперты

- Создаем продукты и решения
- Проводим аудиты безопасности
- Расследуем инциденты
- Исследуем угрозы

Нам доверяют

Экспертиза во всех областях кибербезопасности

200+

уязвимостей нулевого дня наши эксперты обнаруживают ежегодно

500+

уязвимостей нулевого дня в системах класса SCADA найдены нами

500+

работ по анализу безопасности мобильных и веб-приложений в год

30+

уязвимостей нулевого дня в mobile telecoms найдены нами

Наши проекты

sochi.ru 2014

2018 МАРТА ВЫБОРЫ ПРЕЗИДЕНТА РОССИИ

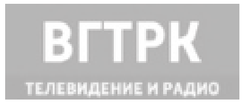
FIFA WORLD CUP RUSSIA 2018

Выпускаем более 20 исследований в год

Ежеквартальные отчеты об актуальных киберугрозах и трендах, прогнозы, расследования активности хакерских группировок, отраслевые исследования

Аналитические статьи

Наши клиенты



Наши проекты

STANDOFF

Самые крупные в мире открытые киберучения

Команды этичных хакеров атакуют виртуальное Государство F, находят уязвимости в корпоративных и промышленных IT-инфраструктурах, а специалисты по кибербезопасности выявляют и расследуют атаки. Участники киберучений SOC с помощью наших продуктов мониторят системы и выявляют атаки

standoff365.com

phd Positive Hack Days

Ежегодный международный форум по практической безопасности

Вас ждут выступления отечественных и зарубежных профессионалов в области информационной безопасности, закрытые и открытые круглые столы с участием лидеров мнений, мастер-классы и лабораторные практикумы известных экспертов

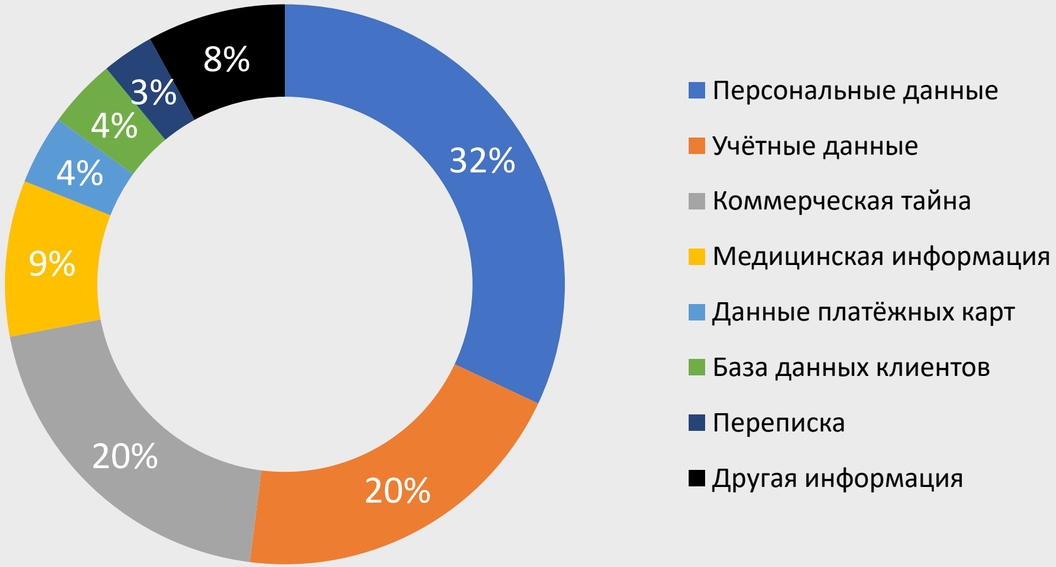
phdays.com

Как вовремя узнать об уязвимостях

и защитить свою компанию

Наши клиенты

Название диаграммы



2400+

Кибератак зафиксировали в 2021 году

Кого атакуют чаще всего*

16%
Государственный сектор

10%
Промышленные компании

11%
Медицинские учреждения

9%
Наука и образование

5%
Финансовая отрасль

7%
IT–компании

5%
Сфера услуг

5%
Телекоммуникации

* «Актуальные киберугрозы: итоги 2021», Positive Technologies

Как злоумышленник может проникнуть в компанию

Расцвет хакинка

Все больше преступников стремятся воспользоваться уязвимостями в ПО

Веб–уязвимости

Позволяет получить контроль над веб-приложением, а также провести атаку и на локальную сеть

Подбор учёток

Большинство паролей составлены предсказуемо

Уязвимости в ПО

Использование устаревших версий ПО является серьезным риском

Ошибки в настройках

Злоумышленники используют ошибки, которые допускают администраторы ИС

Социальная инженерия

Применяется для получения информации от клиента/ сотрудника компании или для доставки ВПО в инфраструктуру

* «Актуальные киберугрозы: итоги 2021», Positive Technologies

Как защититься

Выявлять и устранять уязвимости

Контролировать безопасность систем

- Своевременно обновлять используемое ПО 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 эффективностей мер защиты;
- Автоматизировать процесс выявления уязвимостей.

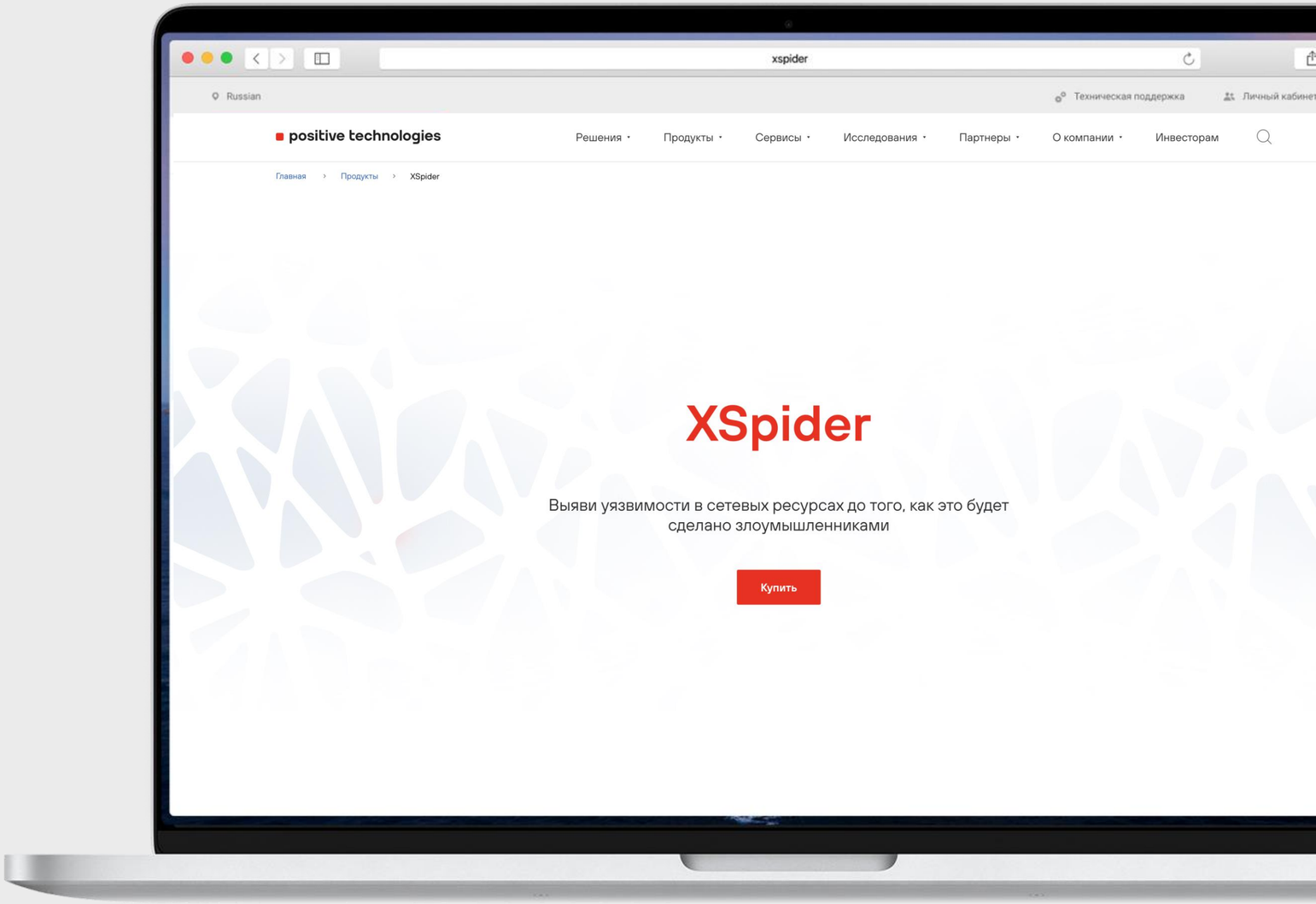
Наше решение

XSpider

Профессиональный
сканер уязвимостей

1. Быстро и точно определяет компоненты сети
2. Сканирует сетевые ресурсы на уязвимости
3. Выдает рекомендации по устранению уязвимостей

20+ лет **XSpider** является признанным лидером среди сканеров безопасности в России



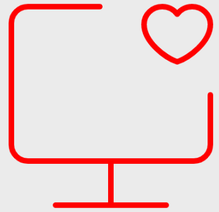
Возможности XSpider

Проведёт инвентаризацию

Определит сетевые узлы, открытые порты, идентифицирует операционную систему и серверные приложения, а также отследит изменения в состоянии информационной системы.

Выявит уязвимости

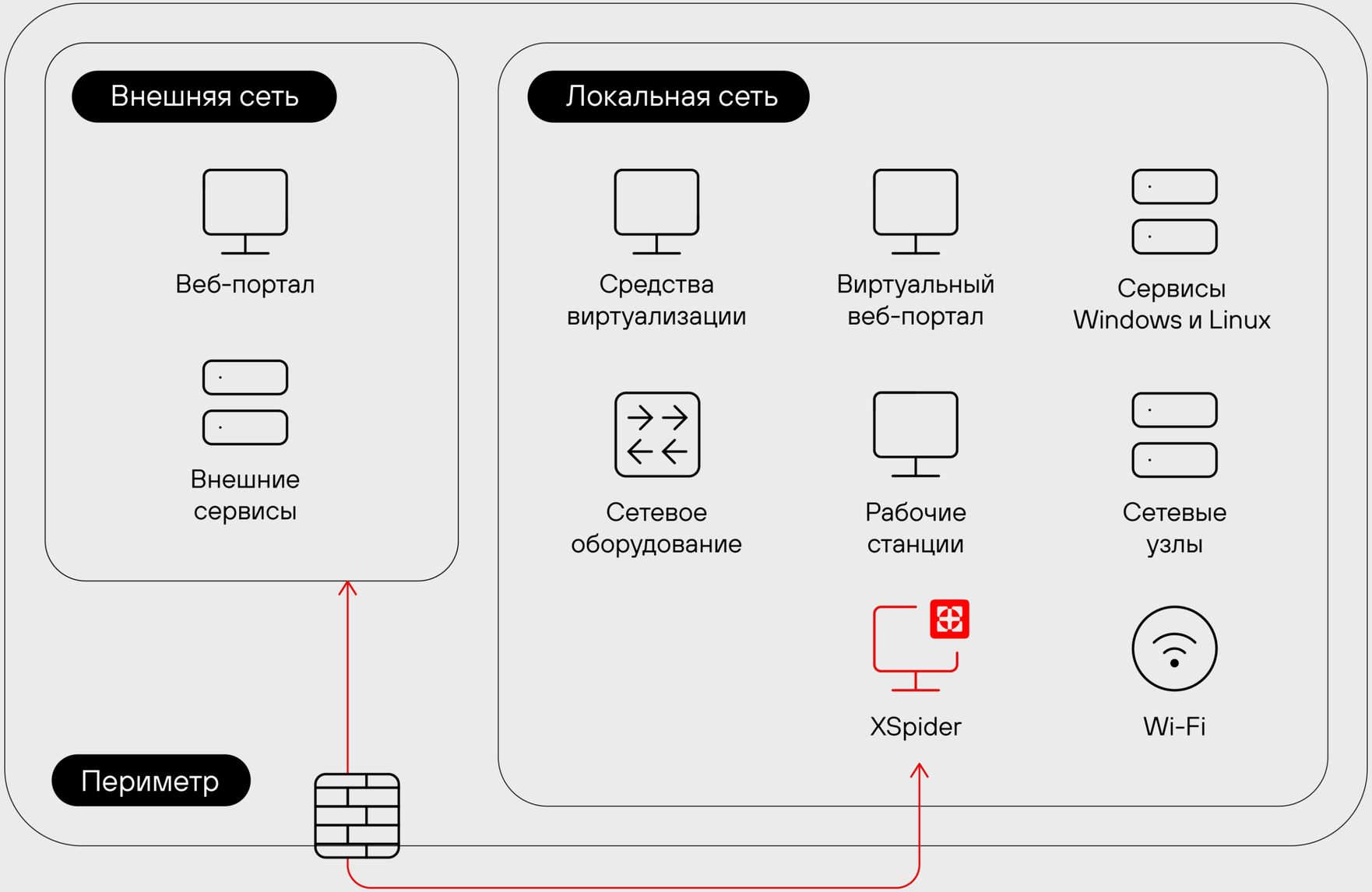
Найдет уязвимости на рабочих станциях, серверах, сетевом оборудовании, проведёт глубокий анализ веб-ресурсов. Проверит стойкость паролей для сервисов, требующих аутентификации. Позволит автоматизировать процесс поиска уязвимостей.



Подскажет решение

По всем обнаруженным уязвимостям XSpider даст подробную информацию и четкие и понятные рекомендации по их устранению.
Также сформирует отчеты по результатам сканирования.

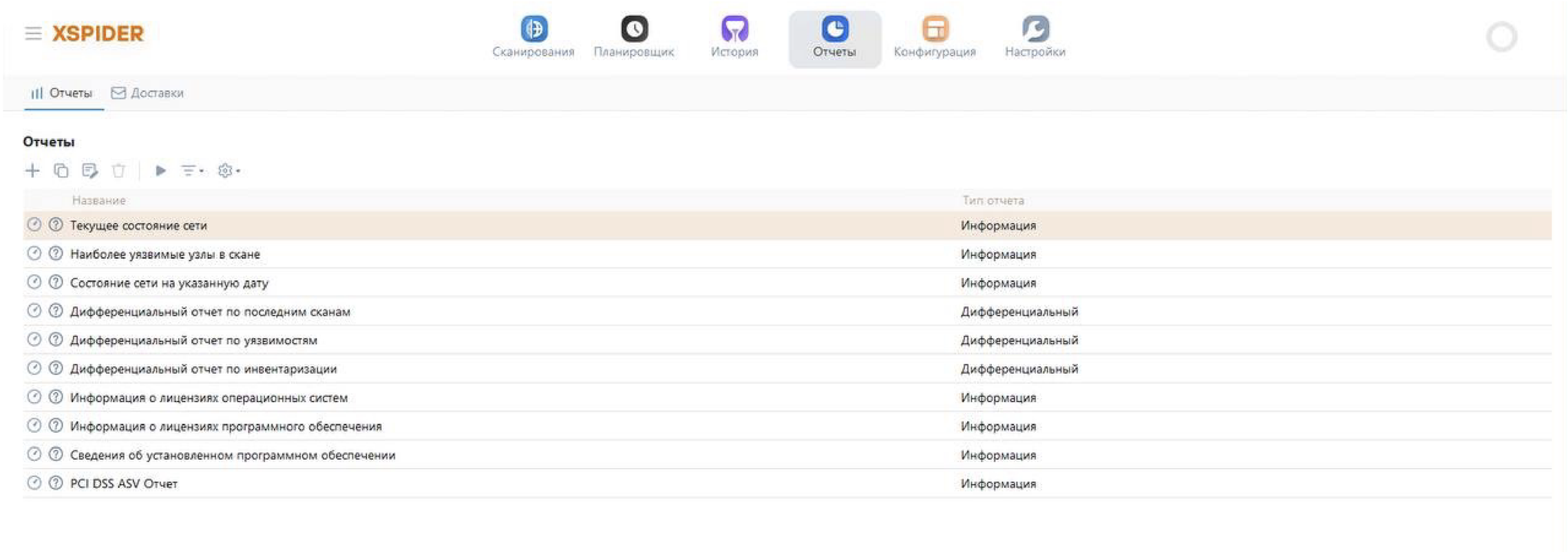
Как работает



Преимущества

- Обширная база уязвимостей с регулярными пополнениями
- Поддержка уязвимостей из БДУ ФСТЭК России
- Анализ веб-приложений по OWASP Top 10
- Русскоязычная техническая поддержка
- Автоматический запуск задач сканирования и выпуска отчета
- Качественная проверка парольной защиты
- Низкий уровень ложных срабатываний
- Низкие аппаратные требования
- Не требует установки дополнительного ПО и агентов

Понятный и современный интрефейс



Помогает выполнять требования регуляторов

Сертификат ФСТЭК России №3247

подтверждает соответствие средствам контроля (анализа) защищенности и требованиям по 4 уровню отсутствия НДВ

Сканер может использоваться в составе автоматизированных систем, а также:

- в ИСПДн (закон № 152-ФЗ, приказ ФСТЭК № 21),
- ГИС (приказ ФСТЭК № 17),
- АСУ ТП КВО (приказ ФСТЭК №31),
- для защиты ЗО КИИ (приказ ФСТЭК №239).

Минкомсвязь России

Входит в реестр российского ПО

с 16 мая 2016 года, рег. номер 786

Сертификат соответствия МО РФ № 2910

позволяет применять XSpider для сканирования на уязвимости в сетях Минобороны

Банк России

Обеспечение соответствия требованиям PCI DSS

Варианты поставки и модель лицензирования

Поставка

Сертифицированная актуальная версия

Поставляются по одной цене

Поддержка

Включена в стоимость

- оперативная техническая поддержка по телефону: +7(495)744-01-44, с 9:00 до 19:00
- портал технической поддержки: support.ptsecurity.com

Годовое лицензирование

Базовая лицензия

по проверяемым хостам (любое оборудование подключенное к локальной или глобальной сети, имеющее ip-адрес или DNS имя)

Продление

- по истечению срока базовой лицензии, но не позднее 12 месяцев
- продление лицензии составляет 40% от стоимости покупки

xspider@ptsecurity.com

ptsecurity.com