Эшелон
комплексная безопасность

СКАНЕР-ВС

анализ защищенности

Сканер-ВС
анализ защищенности

Выполнение требований

Сканер-ВС реализует следующие меры ИБ:

Приказы ФСТЭК России
№ 17
№ 21
№ 31
№ 235
№ 239

- инвентаризация информационных ресурсов;
- анализ уязвимостей;
- контроль установки обновлений ПО;
- контроль состава технических средств и ПО;
- контроль целостности информации;
- учет носителей информации;
- уничтожение (стирание) информации на носителях;
- контроль и анализ сетевого трафика;
- контроль использования технологий беспроводного доступа.

Сертификаты

Сертификат **ФСТЭК России №2204**, подтверждающий выполнение требований:

- руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) — **по 4 уровню** доверия и технических условий;
- технических условий, при выполнении указаний по эксплуатации, приведенных в формуляре на изделие.

Сертификат **Минобороны России №3872**, подтверждающий выполнение требований Приказа МО РФ, в том числе:

- руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) — **по 2 уровню** контроля;
- требованиям по соответствию реальных и декларируемых в документации функциональных возможностей.

Реестр российского ПО

Сканер-ВС включен в **единый реестр российских программ** для электронных вычислительных машин и баз данных. Приказ Минкомсвязи России от 18.03.2016 г. №23.

Сканер-ВС — система комплексного анализа защищенности, позволяющая обеспечить своевременное выявление уязвимостей в ИТ-инфраструктуре организаций любого масштаба. С помощью Сканера-ВС можно проводить тестирование на проникновение, сканирование уязвимостей, а также анализ конфигурации, организовать непрерывный контроль защищенности.

Преимущества

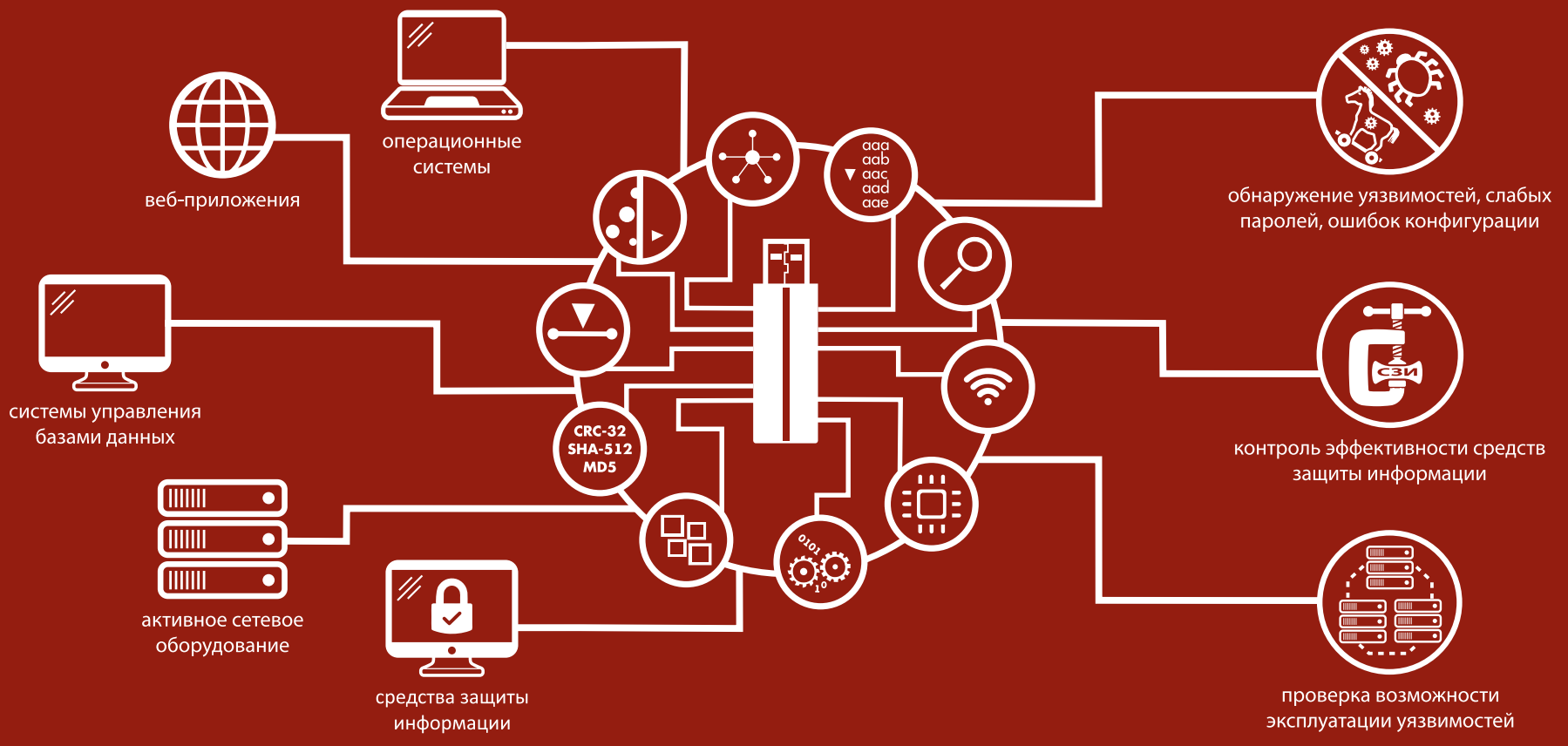
- Возможность работы в режиме Live USB, а также развертывания в ИТ-инфраструктуре предприятия с поддержкой одновременной удаленной работы пользователей.
- Еженедельно обновляемая база уязвимостей, совместимая с банком данных угроз безопасности информации (БДУ) ФСТЭК России, содержит более 45 000 проверок.
- Интуитивно понятный пользовательский интерфейс.
- Документированный программный интерфейс для интеграции с SIEM-системами.
- Гибкий конструктор отчетов, который позволяет получать короткие и информативные отчеты. Поддерживаются различные шаблоны отчетов: краткий (группировка по уязвимостям), полный (группировка по хостам), динамический (динамика изменения состояния хоста во времени), экспорт в различные форматы: HTML, PDF, DOC, CSV.
- Лицензия ограничивает количество IP-адресов, которые можно сканировать одновременно, отсутствует привязка к конкретным IP-адресам.
- Обучение по продукту в форме вебинаров и очных курсов повышения квалификации в учебном центре «Эшелон».
- Наличие сертификатов ФСТЭК России и Минобороны России.

Сетевой аудит

- **Инвентаризация ресурсов сети** — контроль появления новых сетевых узлов и сервисов, идентификация ОС и приложений, трассировка маршрутов передачи данных, построение топологии сети организации.
- **Поиск уязвимостей** — безагентное сканирование на наличие уязвимостей как с учетной записью администратора, так и без нее. Формирование отчета с техническими рекомендациями по устранению обнаруженных брешей в защите.
- **Сетевой аудит стойкости паролей** — проверка стойкости паролей практически всех сетевых сервисов, требующих авторизации (поддерживается более 20 протоколов: HTTP, SMTP, POP, FTP, SSH и др.). В комплексе предустановлены словари, содержащие самые распространенные пароли (имена, числовые, клавиатурные последовательности и т.д.).
- **Подбор эксплойтов** — поиск подходящих эксплойтов на основе собранной информации об узле.
- **Перехват и анализ сетевого трафика** — перехват и анализ трафика, фильтрация содержимого передаваемых данных, а также реализация атак типа MITM (Man In The Middle, «Человек посередине»).
- **Аудит беспроводных сетей** — обнаружение, сканирование и проведение активных и пассивных атак методом подбора паролей в беспроводных сетях с WEP, WPA и WPA-2 шифрованием.
- **Аудит обновлений ОС Windows** — аудит установленных обновлений для ОС Windows 7, 8.1, 10, Server 2012, 2012-R2 и 2016.
- **Аудит ОС «Astra Linux Special Edition»** — аудит настроек комплекса средств защиты ОС специального назначения «Astra Linux Special Edition» по требованиям безопасности.

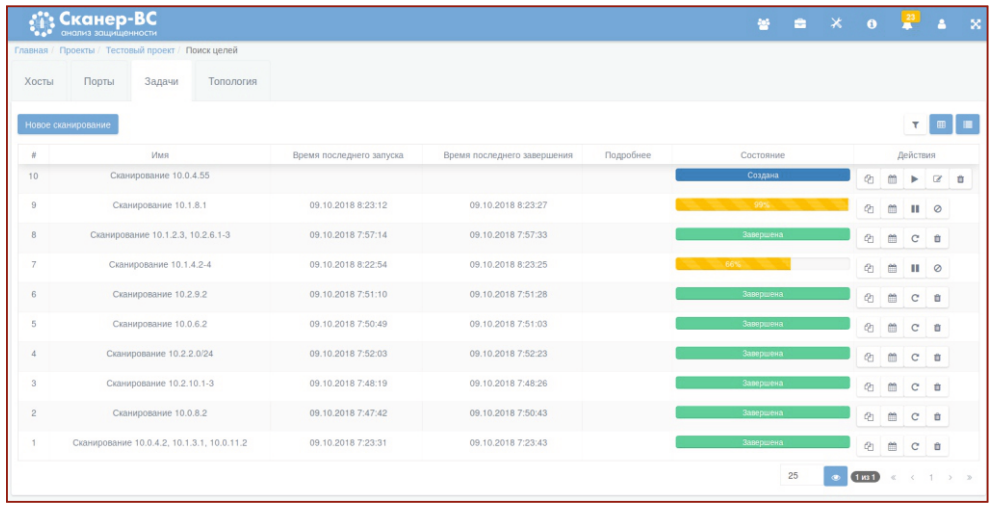
Локальный аудит

- **Локальный аудит стойкости паролей** — аудит стойкости паролей для операционных систем семейства Windows (7, 8.1, 10) и Linux (МСВС, Linux XP, Astra Linux и др.).
- **Поиск остаточной информации** — поиск остаточной информации по ключевым словам на носителях данных (жестких дисках, USB-устройствах, дискетах, оптических дисках) вне зависимости от файловой структуры.
- **Гарантированная очистка информации** — очистка информации на носителях данных путем многократного затирания файлов по стандартам ГОСТ, BSI, FIPS, DoD предотвращает восстановление информации. Также доступна функция безопасного затирания свободного места на носителях данных, предусмотрена защита от удаления системных файлов, совместимо с модулем поиска остаточной информации.
- **Аудит установленного аппаратного и программного обеспечения** — инвентаризация программных и аппаратных средств локальной системы, включая параметры установленных операционных систем, программное обеспечение, информацию о пользователях системы, историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств (центральный процессор, материнская плата, мост, оперативная память и др.), в том числе носителей информации и USB-устройств. Функция сравнения отчетов позволяет отслеживать изменения конфигурации системы.
- **Контроль целостности** — подсчет контрольных сумм заданных папок и файлов по 13 алгоритмам, включая алгоритмы высокой стойкости к атакам ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.



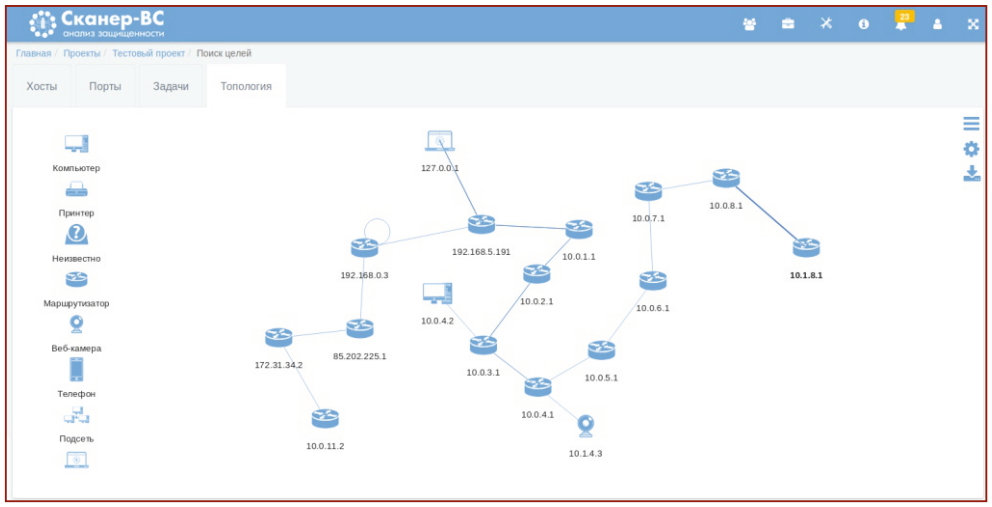
Управление задачами сканирования

Новый менеджер по работе с задачами сканирования позволяет эксперту эффективно управлять процессом аудита защищенности.



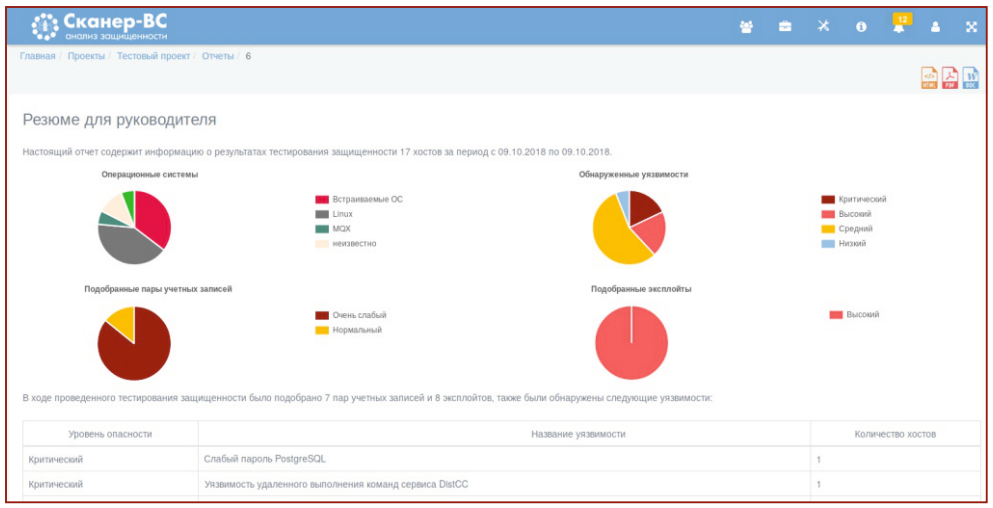
Топология сети

Инвентаризация ресурсов сети позволяет выявить хосты, запущенные сервисы, а также получить актуальную схему сети.



Подсистема отчетов

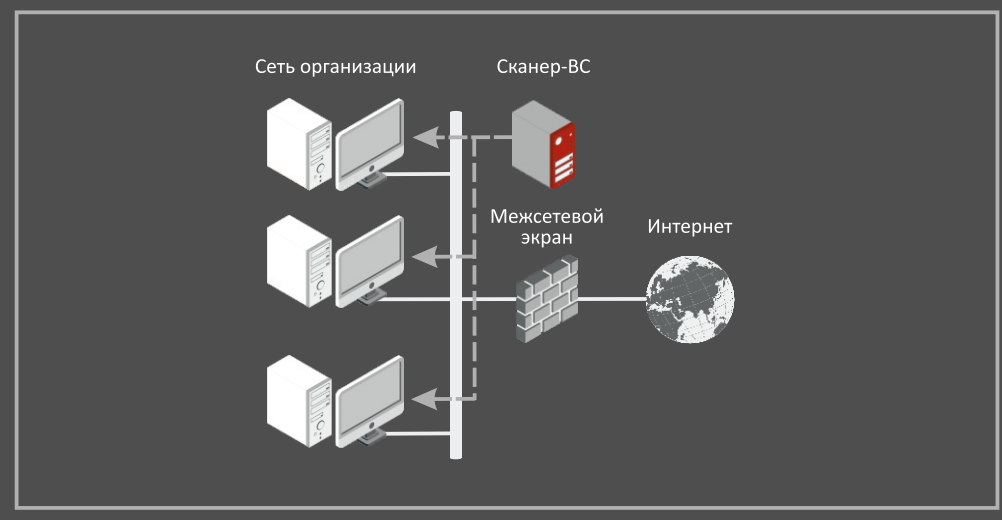
Отчеты содержат информацию об уязвимостях, включая идентификаторы BDU, CVE, оценку по CVSS 2.0, CVSS 3.0, описание методов устранения уязвимостей и ссылки на дополнительную информацию.



Сценарии применения

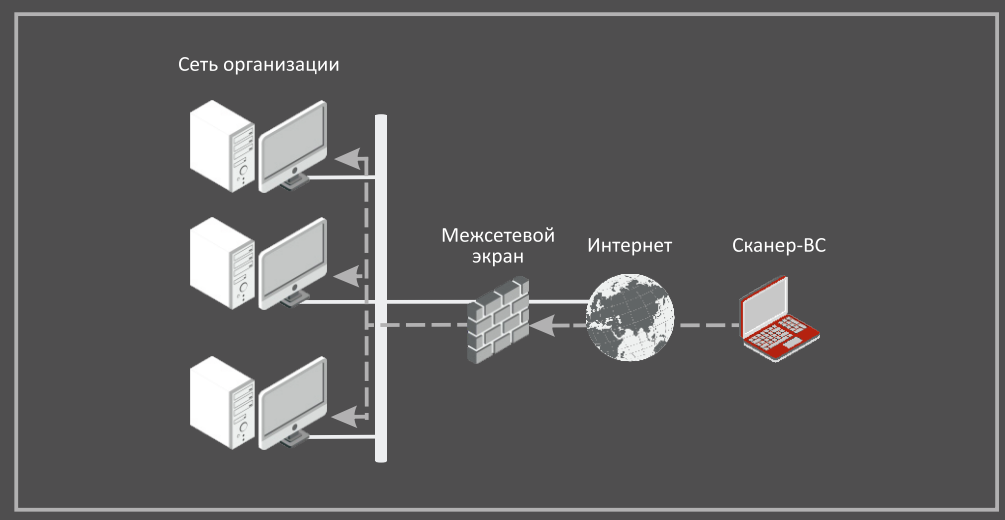
Внутреннее тестирование защищенности

Комплексный аудит защищенной локальной сети организации изнутри.



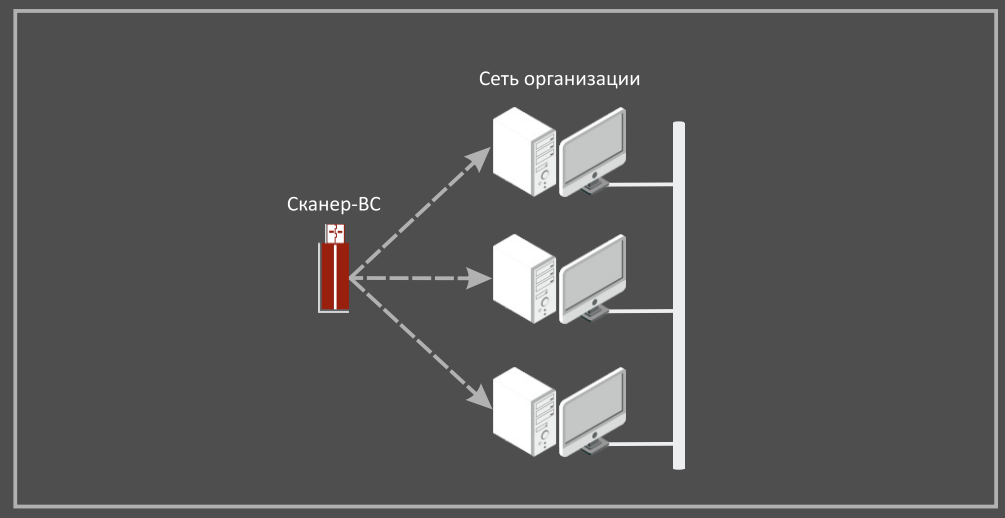
Внешнее тестирование защищенности

Комплексный аудит сети организации извне, проверка правил межсетевого экранирования, выявление узлов, доступных из сети Интернет и т.п.



Тестирование закрытого контура

Комплексный аудит СЗИ без внесения изменений в конфигурацию аттестованного рабочего места, запуск в режиме Live USB.



Эшелон
комплексная безопасность

Сканер-ВС
анализ защищенности

РУБИКОН
межсетевой экран и система обнаружения вторжений

{KOMRAD}
Enterprise SIEM

ПУЛЬСАР
генератор шума

ГЕНЕРАТОР
генерация и управление паролями

ПИК Эшелон
контроль целостности

АК-ВС²
анализ безопасности кода

AppChecker
анализ безопасности приложений

О компании

НПО «Эшелон» специализируется на разработке сертифицированных средств защиты информации и ведет свою деятельность на основании более 50 лицензий и аттестатов аккредитации ФСТЭК России, ФСБ России и Минобороны России. Компания регулярно занимает ведущие позиции в рейтингах CNews и «Эксперт РА».

Головной офис в Москве

107023, г. Москва, ул. Электрозаводская, д. 24
+7 (495) 223-23-92 (многоканальный)
npo-echelon.ru
sales@npo-echelon.ru
vk.com/npo_echelon

Офис в Санкт-Петербурге

199178, г. Санкт-Петербург, наб. реки Смоленки, д. 14
+7 (812) 635-89-04
npo-echelon.ru/spb/
mail@nwechelon.ru