Эшелон
комплексная безопасность

СКАНЕР-ВС ИНСПЕКТОР

анализ защищенности и
проведение комплексных проверок

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 и контроль установки обновлений ПО;
- контроль состава технических средств и ПО;
- контроль реализации правил разграничения доступа;
- 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** контроля;
- технических условий, при выполнении указаний по эксплуатации, приведенных в формуляре на изделие.

Сертификат **Минобороны России №3873**, 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.

Сертифицированный программный комплекс, включающий систему тестирования защищенности **Сканер-ВС** и средство проведения комплексных проверок **Инспектор**, предназначен для анализа уязвимостей в программном обеспечении и в автоматизированных системах, контроля эффективности применения средств защиты информации, формирования и контроля полномочий доступа в автоматизированных системах, а также контроля целостности программ и программных комплексов.

Преимущества Сканера-ВС

- 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 позволяет получать короткие и информативные отчеты. Экспорт в различные форматы: HTML, PDF, DOC, CSV.
- Лицензия ограничивает количество IP-адресов, которые можно сканировать одновременно, отсутствует привязка к конкретным IP-адресам.

Преимущества Инспектора

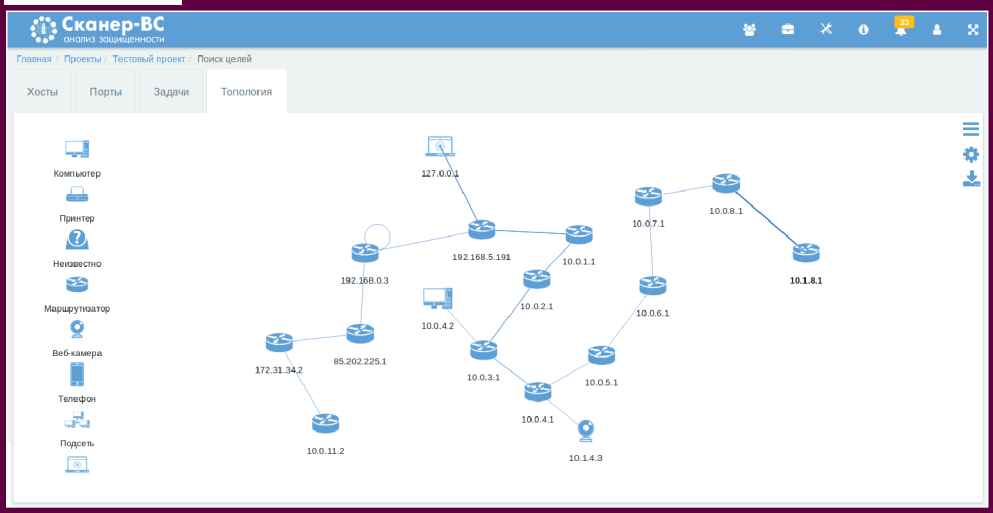
- Выполнение требований к программным (программно-техническим) средствам, необходимым для оказания услуг и выполнения работ, предусмотренных Положениями о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации и деятельности по технической защите конфиденциальной информации.
- Возможность сбора подробной информации об автоматизированной (информационной) системе (номера лицензий на некоторые виды ПО, идентификаторы подключавшихся внешних носителей и др.).
- Работа в режиме «переносимого» приложения – запуск непосредственно с носителя.
- Наличие простого пошагового мастера для проведения тестирования.
- Возможность формирования проекта в рамках проведения проверок и генерации единого отчета по их результатам;
- Совместимость с ОС Windows и Astra Linux SE.

Функциональные возможности Сканера-ВС

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.

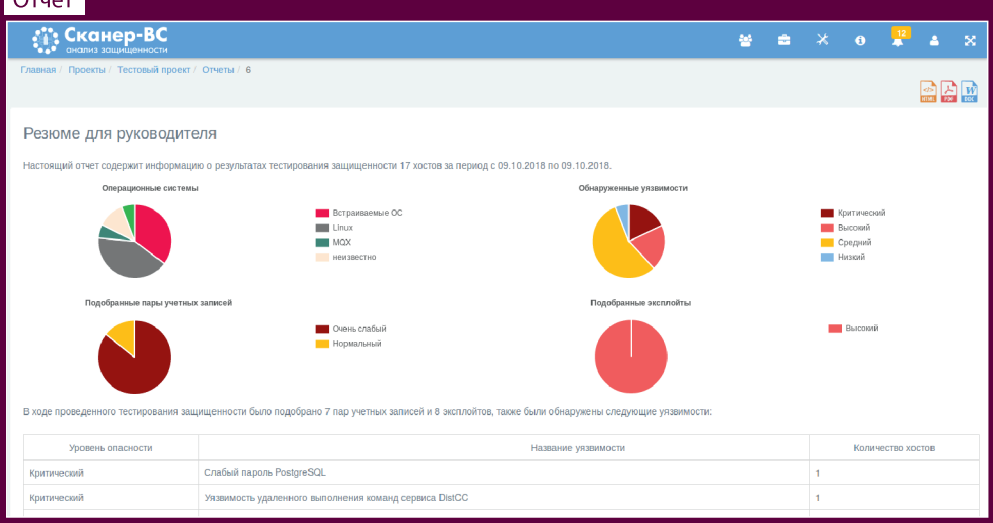
Топология сети



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.

Отчет

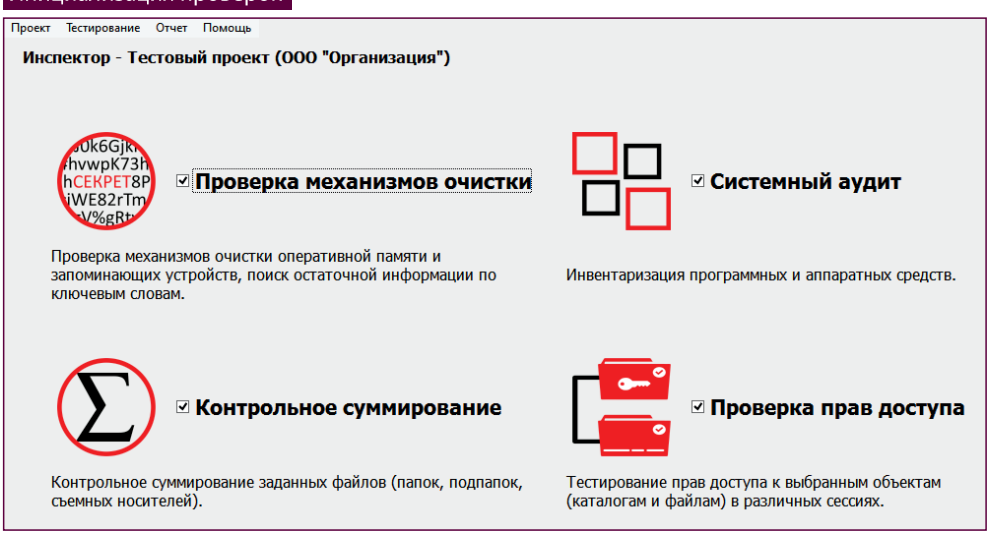


Функциональные возможности модуля Инспектор

Локальный аудит

- Формирование модели системы разграничения доступа пользователей к информационным ресурсам.
- Контроль дискреционных и мандатных полномочий доступа пользователей (локальных и доменных) к выбранным сетевым папкам и объектам файловой системы ОС семейства Windows, в том числе с учетом настроек СЗИ Secret Net Studio, СЗИ Secret Net Studio-C, СЗИ Secret Net 7, СЗИ НСД Dallas Lock 8.0-K, СЗИ НСД Dallas Lock 8.0-C.
- Контроль дискреционных и мандатных полномочий доступа локальных пользователей ОС специального назначения «Astra Linux Special Edition».
- Проверка механизмов очистки оперативной памяти и запоминающих устройств рабочей станции в автоматизированном режиме.
- Фиксация и контроль исходного состояния файлов и папок по контрольным суммам (поддерживается 16 алгоритмов).
- Инвентаризация программных и аппаратных средств: версия и тип операционной системы, перечень установленного программного обеспечения, лицензионные ключи, параметры монитора, информация о процессорах, дисковых устройствах, сетевых адаптерах, принтерах, устройствах ввода информации, перечень подключавшихся USB-накопителей, в том числе определение факта подключений телефонов и другого оборудования через USB-разъемы, возможность определения даты первого и последнего подключения USB-накопителя.
- Функция контроля изменений (сравнение целевых отчетов).
- Поиск остаточной информации по ключевым словам на запоминающих устройствах рабочей станции, в том числе поиск по документам форматов doc, docx, pdf, xlsx, pptx, odt, определение директории файла с найденной информацией, проверка физических дисков и всех разделов, функция ограничения области поиска, встроенные словари, возможность использования собственных словарей.
- Контроль работоспособности антивирусного ПО на основе EICAR-Test-File.

Инициализация проверок

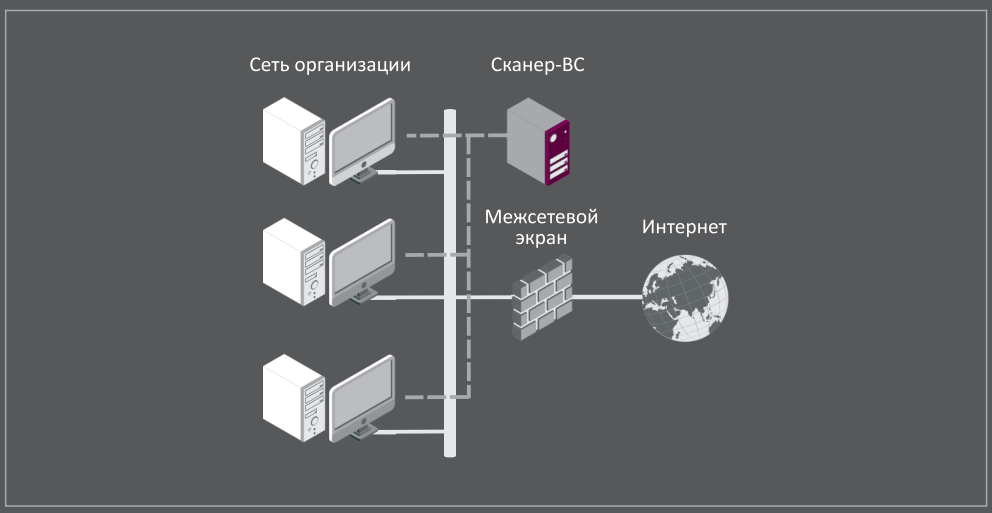


Операционные системы, поддерживаемые модулем «Инспектор»

- ОС семейства Microsoft® Windows®: Windows 7, 8.1, 10 .
- ОС семейства Linux/Unix: Astra Linux SE 1.4 - 1.6.

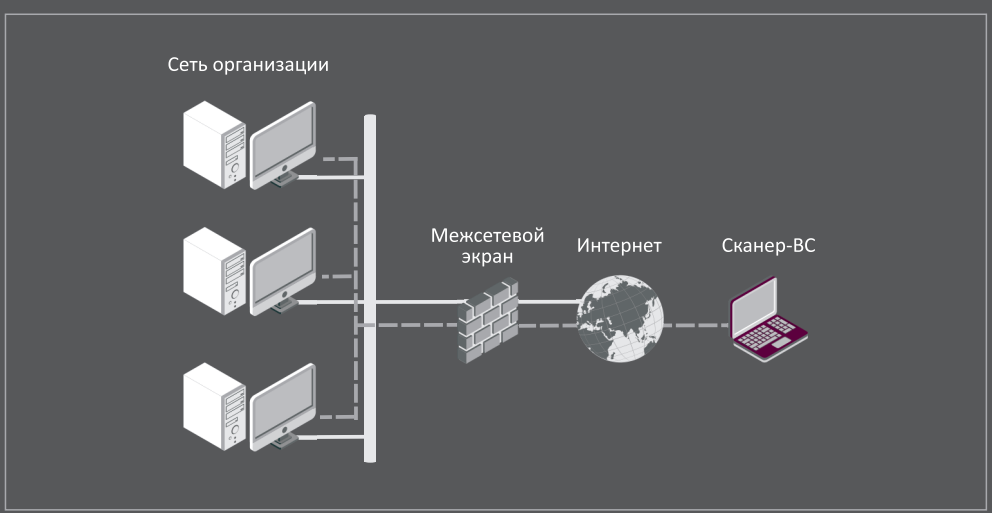
Внутреннее тестирование защищенности

Комплексный аудит защищенной локальной сети организации изнутри.



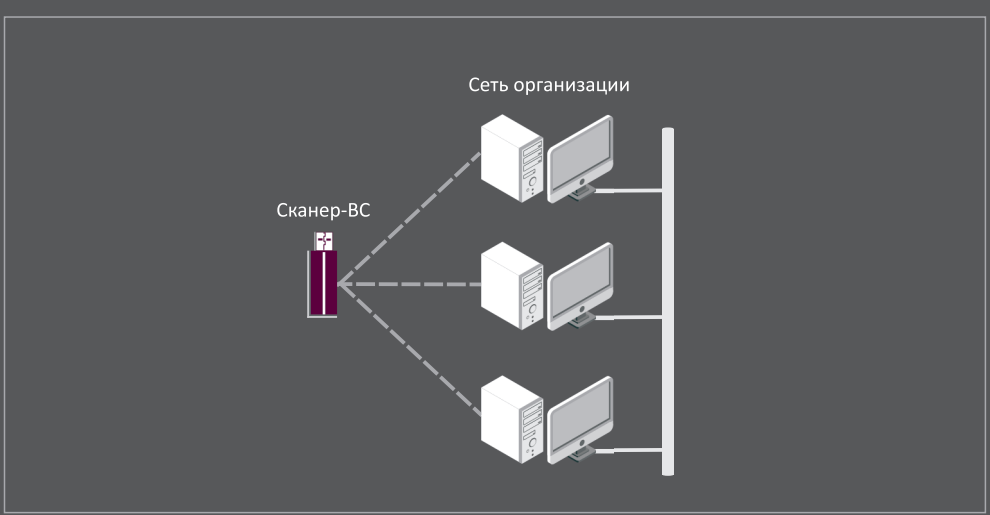
Внешнее тестирование защищенности

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

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
facebook.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