КОД безопасности

Secret Net LSP

Сертифицированное средство защиты от несанкционированного доступа для ОС семейства GNU/Linux

- Широкий список поддерживаемых дистрибутивов Linux
- Совместный режим работы с Соболем
- Поддержка средств централизованного управления Secret Net Studio

Сценарии применения

Защита конфиденциальной информации от внутренних угроз

Результат:

- Минимизация финансовых и репутационных рисков, связанных с утечкой конфиденциальной информации.
- Настроены политики безопасности для сотрудников различных служб при работе с конфиденциальной информацией:
  - с финансовыми документами;
  - с базой данных клиентов;
  - с интеллектуальной собственностью организации;
  - с банковской тайной;
  - с персональными данными.
- Сотрудники получают доступ только к своим рабочим данным, нивелирован риск финансовых и репутационных потерь из-за утечек конфиденциальной информации.

Защита гетерогенных сетей

Результат:

- Обеспечен централизованный мониторинг и управление защитой рабочих станций на базе ОС Windows и Linux.

Соответствие автоматизированных систем требованиям ФСТЭК России

Результат:

- Минимизация финансовых и репутационных рисков, связанных с невыполнением требований регуляторов.
- Информационная система приведена в соответствие требованиям нормативных документов.

Мониторинг событий безопасности для выявления угроз ИБ

Результат:

- Минимизированы финансовые потери от инцидентов, связанных с информационной безопасностью.
- Повышена скорость реакции на инцидент и оперативность расследования инцидентов ИБ.

Возможности

Идентификация и аутентификация пользователей

- Контроль входа пользователей в систему по логину/паролю или с использованием электронных идентификаторов.

Разграничение доступа к внешним устройствам

- Разграничение доступа пользователей и групп пользователей к шинам USB, SATA, сетевым интерфейсам и подключаемым к ним устройствам.
- Правила подключения задаются: new
  - на шину;
  - на классы устройств, связанные с шиной;
  - на конкретные модели и экземпляры устройств.

Регистрация событий ИБ и генерация отчетов

- Фиксация событий безопасности в журнале. Включает события, связанные с доступом пользователей к защищаемым файлам, устройствам и узлам вычислительной сети. Фильтрация событий безопасности, контекстный поиск в журнале событий безопасности.

Затирание остаточной информации

- Уничтожение (затирание) содержимого конфиденциальных файлов при их удалении пользователем. Очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств).

Разграничение доступа к ресурсам

- Механизм дискреционного разграничения доступа для контроля и управления правами доступа пользователей и групп пользователей к объектам файловой системы – файлам и каталогам.

Поддержка широкого списка дистрибутивов

- Astra Linux Common/Special edition; Альт; РЕД ОС; CentOS; Debian; Red Hat Enterprise Linux; Oracle Linux SUSE; Linux Enterprise Server; Ubuntu.

Расширение функциональности ОС

- Обновление общесистемного ПО и расширение функциональности системы без необходимости дожидаться сертификации обновления системных компонентов.
- Возможность создания различных по функциональности решений на базе дистрибутива Linux и защита этих решений с использованием Secret Net LSP.

Контроль целостности и замкнутая программная среда

- Контроль целостности ключевых компонентов Secret Net LSP и критических объектов файловой системы:
  - настройка режимов реакции на нарушение целостности объектов;
  - расписание запуска контроля целостности; new
  - поддержка полного контроля над объектами; new
  - поддержка контроля целостности в реальном времени. new
- Запрет запуска программ, явно не разрешенных администратором безопасности.

Аудит действий пользователей

- Аудит действий субъектов с защищаемыми объектами (файлами, каталогами, сетевыми соединениями, устройствами). Возможность автоматического построения отчетов по результатам аудита.

Интеграция со средствами управления Secret Net Studio

- СЗИ Secret Net LSP может использоваться совместно со средствами управления СЗИ Secret Net Studio. Контроль подключаемых устройств, управление защитными подсистемами, мониторинг событий НСД и поддержка централизованного управления лицензиями через сервер безопасности Secret Net Studio. new

Персональный межсетевой экран

- Контроль сетевого трафика.
- Нейтрализация угроз, связанных с сетевым взаимодействием.
- Разграничение сетевого доступа.
- Контроль папки общего доступа. new
- Контроль именованных файлов. new
- Контроль использования сети приложениями.
- Фильтрация входящих соединений с использованием данных отправителя пакетов.
- Принудительное завершение TCP-соединений.

Функции Secret Net LSP

Сертификаты

Secret Net LSP

- 5-й класс защищенности СВТ
- 4-й класс защиты МЭ типа «В»
- 4-й класс защиты СКН
- Применяется для защиты значимых объектов КИИ до 1 категории, ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно