КОД безопасности

Secret Net LSP

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

- Удобство администрирования благодаря наличию графических и консольных средств управления
- Широкий список поддерживаемых дистрибутивов Linux
- Поддержка средств централизованного управления Secret Net Studio
- Формирование замкнутой среды для СКЗИ класса КС3
- Совместный режим работы с Соболем

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, IEEE 1394 и подключаемым к ним устройствам в целях предотвращения несанкционированной утечки информации с защищаемого компьютера.

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 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).

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.

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.
- Межсетевой экран уровня узла.

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. Запрет запуска модулей, явно не разрешенных администратором безопасности.

Аудит действий пользователей

- Аудит действий субъектов с защищаемыми объектами файловой системы и сетевых соединений, аудит отчуждения информации. 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 и мониторинг событий НСД через сервер безопасности Secret Net Studio.

Поддержка широкого списка дистрибутивов

- Astra Linux Common/Special edition
- Альт СП, Альт Рабочая станция
- РЕД ОС;
- CentOS;
- Debian
- Red Hat Enterprise Linux
- Лотос
- Ubuntu

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.

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.

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.

Защита гетерогенных сетей

Результат:

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

Сертификаты

Secret Net LSP
- 5-й класс защищенности СВТ
- 4-й класс защиты МЭ типа «В»
- 4-й уровень доверия
- Применяется для защиты значимых объектов КИИ 1 категории, ИМПДН до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно

Secret Net LSP-C
- 2-й уровень контроля отсутствия НДВ
- Технические условия
- Применяется для защиты АС, обрабатывающих государственную тайну до уровня «Совершенно секретно»

Техническая поддержка

Техническая поддержка Secret Net LSP может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Каталог услуг	Пакет поддержки			
	Базовый	Стандартный	Расширенный	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**