

Secret Net Studio 8.8

Средство защиты данных и контроля безопасности
конечных точек



Сокращение издержек
на администрирование
СЗИ и обучение персонала



Высокая масштабируе-
мость, поддержка распре-
деленных инфраструктур



Быстрая централизованная
настройка защиты в соот-
ветствии с требованиями
законодательства РФ



Централизованное
управление клиентами
Secret Net LSP
на платформе Linux



Решаемые задачи

- Защита рабочих станций и серверов от вирусов и вредоносных программ.
- Защита от сетевых атак.
- Защита от подделки и перехвата сетевого трафика внутри локальной сети.
- Защита информации от несанкционированного доступа.
- Контроль утечек и каналов распространения защищаемой информации.
- Защита от действий инсайдеров.
- Разграничение доступа к конфиденциальной информации и ресурсам.
- Защита от кражи информации при утере носителей.
- Соответствие требованиям регуляторов к защите персональных данных, государственных информационных систем, автоматизированных систем управления и государственной тайны.
- Защита объектов критической информационной инфраструктуры (КИИ).

Возможности Secret Net Studio



Лицензирование

По редакциям

Средство защиты информации Secret Net Studio представлено в двух редакциях:

- Secret Net Studio
- Secret Net Studio – С

Возможности Secret Net 7 и редакций Secret Net Studio:

| Подсистема | Secret Net 7 | Secret Net Studio – С* | Secret Net Studio |
|--|--------------|------------------------|-------------------|
| Защита от НСД | ● | ● | ● |
| Контроль устройств | ● | ● | ● |
| Защита диска и шифрование контейнеров | - | ● | ● |
| Персональный межсетевой экран и система авторизации сетевых соединений | - | ● | ● |
| Антивирус | - | - | ● |
| Обнаружение и предотвращение вторжений | - | - | ● |
| Песочница ^{new} | - | - | ● |
| Полнодисковое шифрование ^{new} | - | - | ● |

* Для защиты гостайны.

По уровню защиты

| Подсистема | Максимальная защита | Оптимальная защита | Постоянная защита | Дополнительная защита* |
|---|---------------------|--------------------|-------------------|------------------------|
| Защита от НСД | ● | ● | ● | - |
| Контроль устройств | ● | ● | ● | - |
| Защита диска и шифрование контейнеров | ● | - | ● | - |
| Персональный межсетевой экран | ● | - | ● | - |
| Антивирус | ● | ● | - | ● |
| Обнаружение и предотвращение вторжений | ● | ● | - | ● |
| Песочница ^{new} | ● | - | ● | - |
| Полнодисковое шифрование ^{new} | ● | - | ● | - |
| Срок лицензии | 1 или 3 года | 1 или 3 года | Бессрочно | 1 или 3 года |

* Пакет «Дополнительная защита» может быть приобретен только в дополнение к другому набору лицензий.

Возможности

Защита от несанкционированного доступа

Дискреционное и мандатное управление доступом к файлам

- Работа в любой файловой системе, поддерживаемой Windows, включая FAT
- Назначение меток конфиденциальности через свойства папок и директорий
- Контроль потоков, возможность строгого контроля терминальных подключений
- Выбор уровня конфиденциальности сессии при входе в систему или автоматическое назначение максимального уровня конфиденциальности

Усиленный вход в систему

- Поддержка двухфакторной аутентификации и электронных идентификаторов eToken, Rutoken, ESMART, JaCarta, iButton, Guardant ID 2.0 ^{new} и других
- Поддержка аппаратных ключей JaCarta PKI/ BIO, Форос
- Собственная усиленная парольная аутентификация и парольные политики
- Политики блокировки сеанса при неактивности или изъятии идентификатора
- Работа с локальными и доменными пользователями
- Поддержка терминальных серверов и VDI
- Гибкие настройки ограничения доступа
- Сквозная аутентификация пользователя при использовании ПАК «Соболь»
- Работа с идентификаторами iButton, подключенными к ПАК «Соболь»

Поддержка схем аутентификации пользователя

- Пароль
- Токен
- Windows Live ID
- Графический пароль
- Indeed AM
- Indeed SSO

Теневое копирование

- Создание теневых копий при копировании документов на съемные носители и выводе на печать
- API для автоматизированного доступа в хранилище теневых копий ^{new}
- Защищенное хранилище для теневых копий
- Локальное управление теневыми копиями
- Контроль заполнения хранилища

Контроль печати

- Настройка отдельных принтеров и правил для всех подключенных устройств
- Дискреционное и полномочное управление доступом к принтерам
- Поддержка виртуальных принтеров
- Ограничение печати документов в зависимости от уровня конфиденциальности
- Маркировка документов

Затирание данных

- Настройка количества циклов затирания
- Поддержка FAT, NTFS и REFS
- Затирание данных на локальных и сменных носителях

Замкнутая программная среда и контроль целостности данных

- Создание списка разрешенных к запуску приложений
- Автопостроение зависимостей приложений
- Контроль файлов, директорий и реестра
- Настройка времени контроля
- Выбор варианта реакции на события ИБ
- Управление контролем целостности файлов с помощью ПАК «Соболь»

Контроль устройств

- Дискреционное и полномочное управление доступом к устройствам
- Контроль по группам, классам, моделям и отдельным устройствам
- Иерархическое наследование настроек
- Контроль подключения и отключения устройств
- Управление перенаправлением устройств в терминальных подключениях



Антивирусная защита и обнаружение вторжений

- Сигнатурные и эвристические методы поиска вредоносного ПО
- Постоянная защита, сканирование из контекстного меню и по расписанию
- «Белые» списки директорий и файлов
- Выбор профилей сканирования
- Локальные серверы обновлений
- Эвристический и сигнатурный анализ входящего сетевого трафика
- Автоматическая временная блокировка атакующих хостов
- Команда оперативного снятия блокировки
- Песочница ^{new}
- Почтовый антивирус ^{new}
- Удаление вредоносных файлов, занятых другими процессами ^{new}

Шифрование данных

- Шифрование контейнеров произвольного размера
- Хранение ключевой информации на электронных ключах или съемных дисках
- Резервное копирование ключей
- Настраиваемые права доступа к данным в контейнере
- Полнодисковое шифрование ^{new}
- Совместимость с ПАК «Соболь» ^{new}
- Регистрация изменений статусов защиты диска сторонними средствами ^{new}

Устойчивость к атакам

- Независимый от ОС модуль «Доверенная Среда»
- Внешний контроль целостности защитных процессов СЗИ
- Внешний контроль целостности драйверов в системе
- Защита системы управления от действий локального администратора

Защита сетевого взаимодействия

Межсетевой экран

- Фильтрация трафика на L3, L4 и L7
- Настройка реакции на срабатывание правил
- Возможность задать действие правил по дням недели и времени суток
- Шаблоны для различных сетевых служб
- Добавление возможности экспортировать/импортировать правила МЭ ^{new}
- Поддержка настройки SPI через Программу управления ^{new}

Авторизация сетевых соединений

- Разграничение доступа для терминальных серверов
- Защита от атак Man-in-the-middle
- Программная сегментация сети без изменения сетевой топологии
- Скрытие сетевого трафика

Централизованное управление и мониторинг

- Централизованное управление клиентами Secret Net LSP
- Шаблоны настроек для приведения системы в соответствие требованиям законодательства РФ
- Централизованное развертывание, установка исправлений и обновлений
- Иерархические политики для управления настройками защитных компонентов
- Настраиваемая регистрация событий, разделение событий по степени значимости
- Группировка защищаемых компьютеров для наблюдения и отдельного отображения состояния
- Получение журналов из ПАК «Соболь»
- Оповещение о событиях ИБ в панели управления и по e-mail
- Централизованное управление безопасностью в несвязанных доменах Active Directory
- Детализированный аудит применения эффективных политик безопасности ^{new}
- Идентификация действий администратора в системе ^{new}
- Передача парольных политик в ПАК «Соболь» ^{new}
- Централизованная активация механизма защиты дисков ^{new}
- Выделенный сервер аутентификации ^{new}
- Поддержка экспорта/импорта списка рабочих станций ^{new}
- Централизованное управление сессиями пользователей и питанием компьютера ^{new}
- Кумулятивные пакеты исправлений ^{new}



Планы по сертификации



ФСТЭК России

Secret Net Studio – С (Сертификат получен)

- УД 2/СВТ 3/МЭ В2, для защиты АС до класса 1Б включительно (в т. ч. защита гостайны с грифом «совершенно секретно»), защита ЗОКИИ до 1 категории включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

Secret Net Studio

- СВТ 5/СКН 4/СВЗ 4 (типы: «А», «Б», «В», «Г»)/МЭ В4/СОВ 4 (уровень узла)/УД 4, для защиты АС до класса 1Г включительно, защита ЗОКИИ до 1 категории включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

ФСБ России

- Защита по классу АК5

Техническая поддержка

Техническая поддержка продуктов линейки Secret Net Studio 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 международным и отраслевым стандартам.