КОД безопасности

Secret Net Studio 8.10

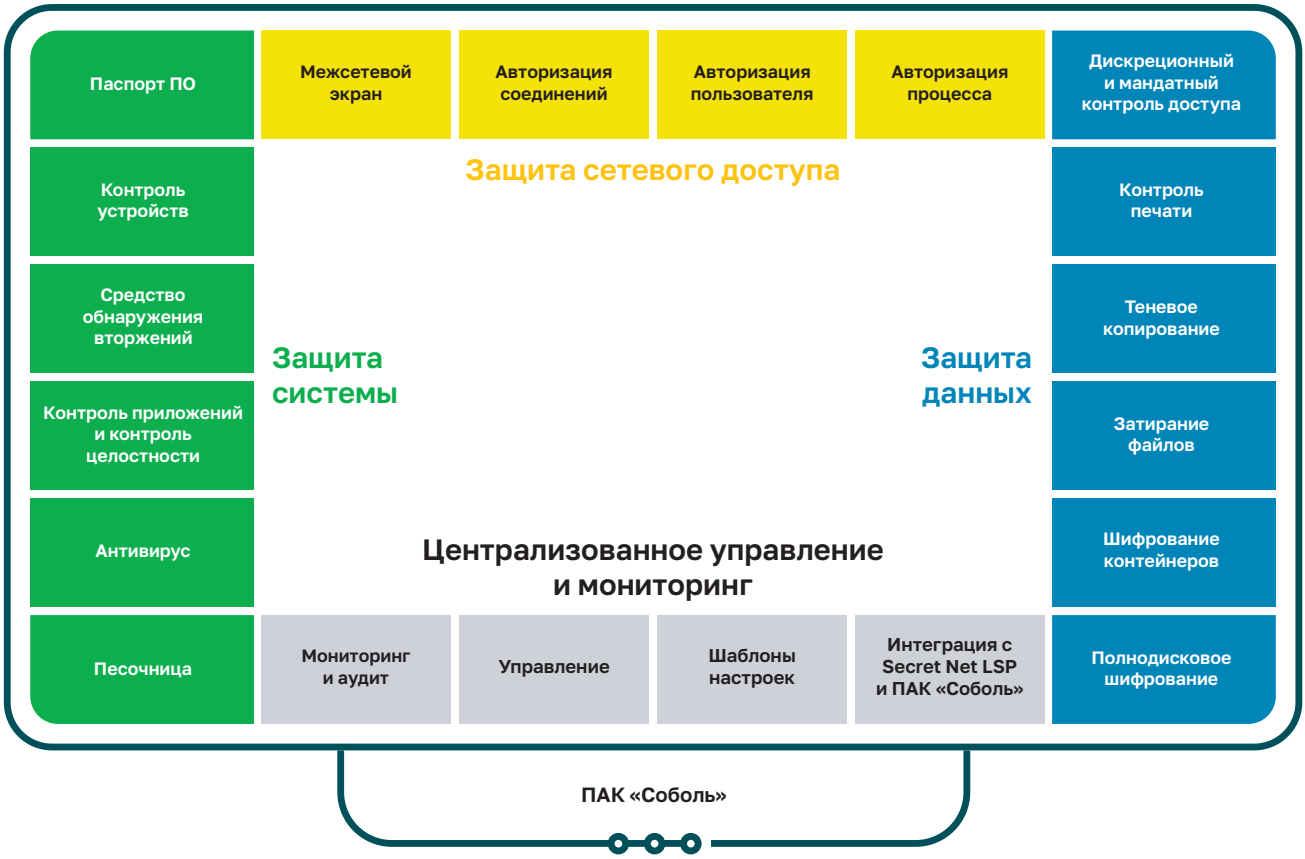
Средство защиты данных и контроля безопасности конечных точек

- Сокращение издержек на администрирование СЗИ и обучение персонала
- Высокая масштабируемость, поддержка распределенных инфраструктур
- Быстрая централизованная настройка защиты в соответствии 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



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, Форос, Guardant ID.
- 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».
- Возможность оффлайн присвоения токенов. new
- Опциональный модуль входа, который имеет три режима: жесткий, мягкий, выключен. new

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.
- 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.
- Защита от подмены VID и PID подключаемого устройства. new

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.
- Почтовый антивирус.
- Удаление вредоносных файлов, занятых другими процессами.

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.
- Совместимость с ПАК «Соболь».
- Регистрация изменений статусов защиты диска сторонними средствами.

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.
- Поддержка настройки SPI через Программу управления.

Авторизация сетевых соединений

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

Централизованное управление и мониторинг

- Шаблоны настроек для приведения системы в соответствие требованиям законодательства РФ.
- Централизованное развертывание, установка исправлений и обновлений.
- Централизованное управление клиентами Secret Net LSP через сервер безопасности SNS.
- Иерархические политики для управления настройками защитных компонентов.
- 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.
- Идентификация действий администратора в системе.
- Передача парольных политик в ПАК «Соболь».
- Поддержка экспорта/импорта списка рабочих станций.
- Централизованное управление сессиями пользователей и питанием компьютера.
- Возможность отправки журналов на сторонний syslog сервер. new
- Возможность создания и распространения легковесного автономного пакета развертывания. new

Лицензирование

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	●	-	●	-
Полнодисковое шифрование	●	-	●	-
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.

Сертификаты

ФСТЭК России
Secret Net Studio 8.10

- СВТ 5/СКН 4/САВЗ 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
Secret Net Studio 8.10

- СЗИ от НСД класса АК3/АК5

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**