КОД безопасности

SECRET NET STUDIO

Комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования

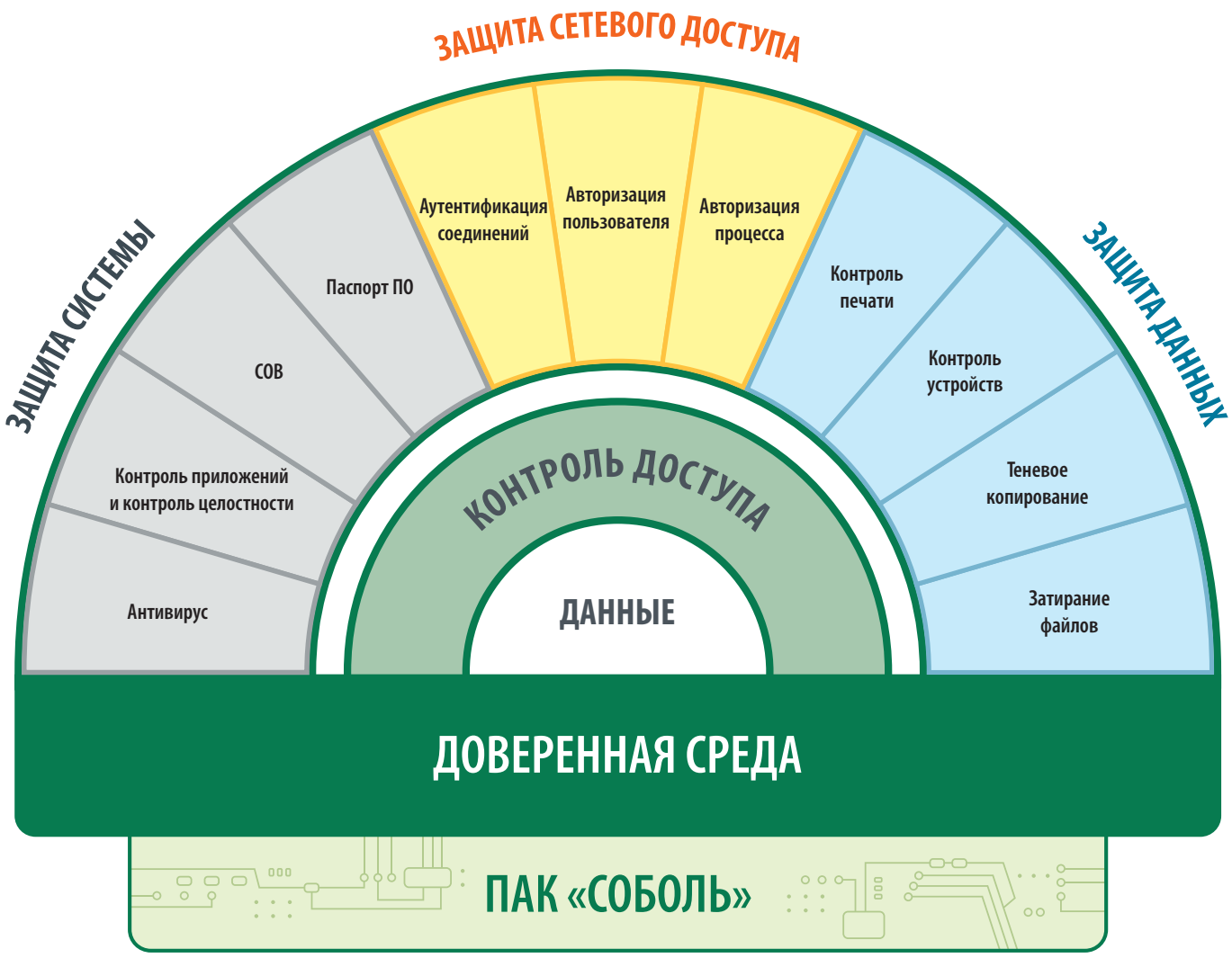
ПРЕИМУЩЕСТВА

- НИЗКАЯ НАГРУЗКА НА ЗАЩИЩАЕМЫЕ КОМПЬЮТЕРЫ
- 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
- ВНЕШНЯЯ ЗАЩИТА ПРОЦЕССОВ СЗИ И ДРАЙВЕРОВ

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 8.5



ЛИЦЕНЗИРОВАНИЕ

ПО РЕДАКЦИЯМ

Средство защиты информации Secret Net Studio представлено в двух редакциях:
- **Secret Net Studio;**
- **Secret Net Studio – C.**

Возможности Secret Net 7 и редакций Secret Net Studio:

ПОДСИСТЕМА	SECRET NET 7	SECRET NET STUDIO – C	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			●
Сертификат ФСТЭК России	3 СВТ, 2 НДВ	3 СВТ, 2 МЭ, 2 НДВ	5 СВТ, 4 СКН, 4 САВЗ, 4 МЭ, 4 СОВ, 4 НДВ

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	●	●		●
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 и других.
- 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».

Теневое копирование

- Создание теневых копий при копировании документов на съемные носители и выводе на печать.
- 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.
- 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.

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.

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.

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.

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.
- Настраиваемые сигналы тревоги, разделение событий по степени значимости.
- Группировка защищаемых компьютеров для наблюдения и раздельного отображения состояния.
- Получение журналов из ПАК «Соболь».
- Оповещение о событиях ИБ в панели управления и по e-mail.
- Квитирование событий.

УСТОЙЧИВОСТЬ К АТАКАМ

- Независимый от ОС модуль «Доверенная Среда»
- Внешний контроль целостности защитных процессов СЗИ.
- Внешний контроль целостности драйверов в системе.

СЕРТИФИКАТЫ

ФСТЭК России

Secret Net Studio – C
СВТ 3/МЭ 2/НДВ 2, для защиты АС до класса 1Б включительно (в т. ч. защита гостайны с грифом «совершенно секретно»), ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

Secret Net Studio
СВТ 5/СКН 4/САВЗ 4 (типы: «А», «Б», «В», «Г»)/МЭ 4/СОВ 4 (уровень узла)/НДВ 4, для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

ФСБ России

Защита по классу АК3 *(для Secret Net Studio 8.4)*

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.
Существует несколько пакетов технической поддержки:

Базовый | Стандартный | Расширенный | VIP

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