КОД БЕЗОПАСНОСТИ

Secret Net Studio 8.5
для защиты данных и IT-инфраструктуры

ПРОБЛЕМЫ И СПЕЦИФИКА ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

УГРОЗЫ ДАННЫМ

- Кража данных внешним злоумышленником
- Потеря данных в результате атаки вируса-шифровальщика
- Утечка данных в результате действий внутреннего нарушителя

КОД БЕЗОПАСНОСТИ

УГРОЗЫ СИСТЕМЕ

- Заражение вредоносным ПО
- Закрепление злоумышленника в системе
- Несанкционированный доступ к конфиденциальным данным
- Несанкционированное изменение прикладного ПО

КОД БЕЗОПАСНОСТИ

УГРОЗЫ ЛОКАЛЬНОЙ СЕТИ

- Горизонтальное распространение злоумышленника
- Перехват трафика
- Распространение червей

О ПРОДУКТЕ
SECRET NET STUDIO 8.5

КОД БЕЗОПАСНОСТИ

Secret Net Studio 8.5

Защита рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийных устройств

Предназначен для решения следующих задач:

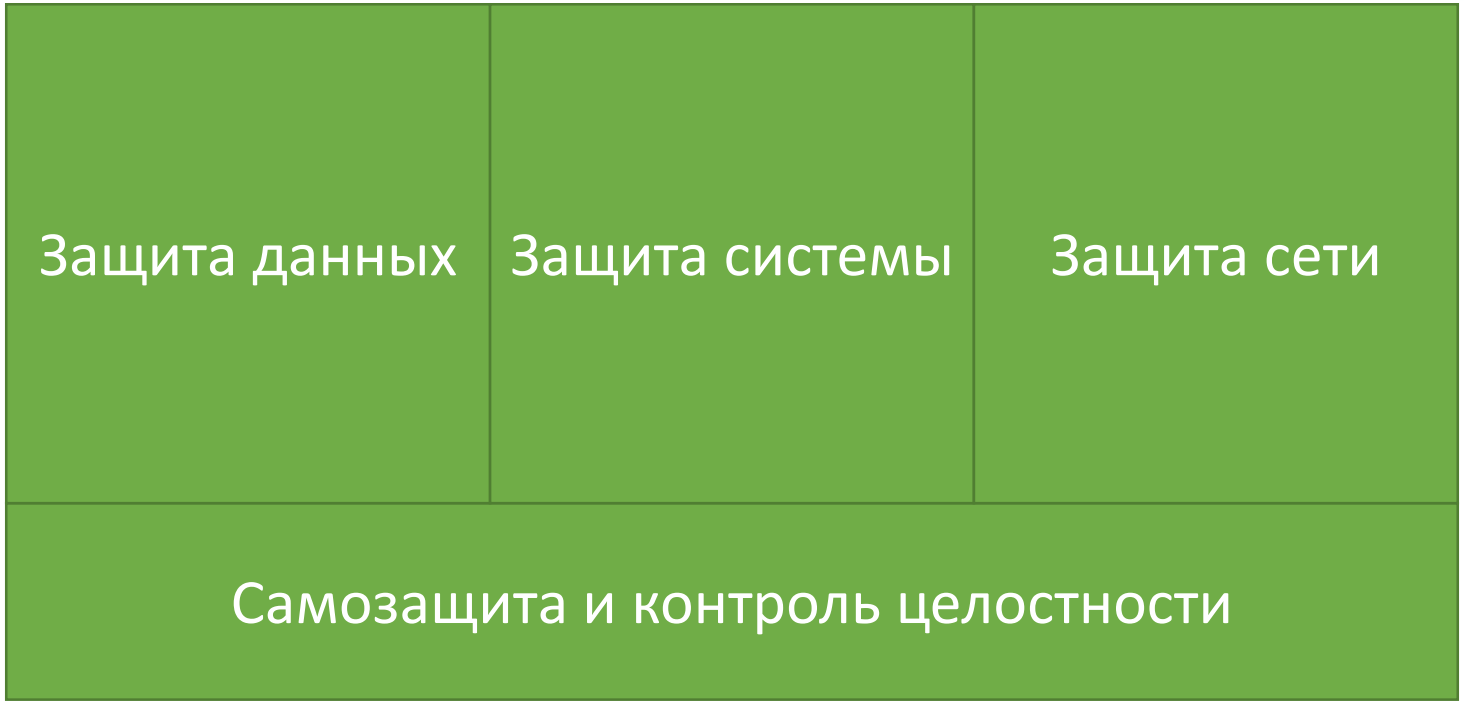
- **Защита конфиденциальной информации**
- **Защита от проникновения и несанкционированных действий злоумышленника внутри системы**
- **Выполнение требований и рекомендаций по защите конечных точек**

КОНЦЕПЦИЯ

Угрозы данным	Угрозы системе	Угрозы сети
• Утечки данных • Вымогательство за расшифровку • Кража данных	• Заражение вредоносным ПО • Закрепление в системе • Несанкционированный доступ к данным • Несанкционированное изменение прикладного ПО	• Горизонтальное распространение злоумышленника • Перехват трафика • Распространение червей

Угрозы средствам защиты
• Отключение пользователем • Отключение злоумышленником • Ограничение функциональности

КОНЦЕПЦИЯ


Защита данных
Защита системы
Защита сети
Самозащита и контроль целостности

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАЦИЯ

ФСТЭК России

Secret Net Studio 8.5

- 5 класс защищенности СВТ
- 4 уровень контроля НДВ
- 4 класс защиты СКН
- 4 класс защиты САВЗ
- 4 класс защиты СОВ
- 4 класс защиты МЭ тип “В”

Secret Net Studio-C 8.5

- 3 класс защищенности СВТ
- 2 уровень контроля НДВ
- 2 класс защиты МЭ тип “В”

Продукт сертифицирован для защиты

- значимых объектов критической информационной инфраструктуры (КИИ) до 1 категории включительно
- государственных информационных систем (ГИС) до К1 включительно
- информационных систем персональных данных (ИСПДн) до УЗ1 включительно
- автоматизированных систем управления технологическими процессами (АСУ ТП) до К1 включительно

SECURITY CODE

АРХИТЕКТУРА

КАК SNS 8.5 ЗАЩИЩАЕТ ДАННЫЕ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПОЛИТИКА РАЗГРАНИЧЕНИЯ ПРАВ

Прозрачная политика прав доступа с использованием меток конфиденциальности

- **Работа с конфиденциальными данными возможна только в соответствующей сессии (например, сессия гостайны)**
- **Информация не может быть скопирована в документ или хранилище более низкого уровня допуска**
- **Строгий запрет на вывод, изменение, удаление информации неавторизованными лицами**

КОД БЕЗОПАСНОСТИ

ПОЛИТИКА РАЗГРАНИЧЕНИЯ ПРАВ (2)

Права доступа распространяются на все ресурсы системы

- Выдача прав SNS в соответствии с корпоративными ролями/уровнями допуска

Многофакторная аутентификация

- Задание политики сложности паролей
- Вход по идентификатору/смарт-карте
- Совместный режим работы с ПАК «Соболь»

КОД БЕЗОПАСНОСТИ

МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

Метки назначаются на:

Сессия пользователя

Ресурсы системы
(физические и виртуальные)

Файлы и каталоги

Контроль доступа в систему

Контроль доступа к файлам и директориям

Контроль устройств

Контроль печати

Контроль NTFS-потоков

КОД БЕЗОПАСНОСТИ

ДОПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ

Шифрование контейнеров

- Данные на жестком диске и съемных носителях хранятся в зашифрованном контейнере
- Для пользователя контейнер отображается как подключаемый локальный диск

Контроль целостности данных

- Расчет контрольных сумм от данных и сравнение с эталонным значением
- Администратор Сервера Безопасности оперативно получает уведомление о нарушении целостности информации

Создание теневых копий

- При копировании информации на съемные носители, а также отправке документов на печать

Гарантированное удаление данных

- Уничтожение конфиденциальной информации без возможности последующего восстановления специализированными средствами

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА SECRET NET STUDIO 8.5

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ЭТАП ПРОНИКНОВЕНИЯ

Задачи:

Защита от проникновения во внутреннюю сеть

- Через атаку на сетевой сервис
- Через атаку с помощью USB-устройства

Механизмы SNS 8.5:

- Система обнаружения и предотвращения вторжений (СОВ)
- Контроль устройств

Система обнаружения и предотвращения вторжений

- **Защищает от проникновения злоумышленника во внутреннюю сеть организации через внешние каналы**

Контроль устройств

- **Запрещает использование неавторизованных съемных носителей информации, предотвращая занесение зловреда в систему с зараженных устройств**

КОД БЕЗОПАСНОСТИ

ЭТАП ВНУТРЕННЕГО РАСПРОСТРАНЕНИЯ

Задачи:

- Защита от распространения злоумышленника во внутренней сети
- Защита от перехвата трафика
- Защита от распространения вирусов во внутренней сети

Механизмы SNS 8.5:

- Межсетевой экран
- Авторизация сетевых соединений

Фильтрация трафика

- **На основе IP-Адресов и сетевых портов**
- **Имени пользователя**
- **Приложения**
- **Времени**

Виртуальная сегментация сети

- **Создание нескольких виртуальных сегментов в одной подсети**
- **Шифрование трафика при обмене между машинами виртуального сегмента**
- **Взаимная аутентификация машин в рамках одного виртуального сегмента**

Запрет доступа к серверному приложению до тех пор, пока не проведен ряд проверок

- **Проверка пользователя**
- **Взаимная аутентификация АРМ пользователя и сервера**
- **Проверка приложения, которое запрашивает доступ**

КОД БЕЗОПАСНОСТИ

КОНЕЧНЫЙ ЭТАП АТАКИ

Задачи:

- Защита от заражения вредоносным ПО
- Защита от несанкционированного изменения прикладного ПО
- Защита от закрепления злоумышленника в системе

Механизмы SNS 8.5:

- Замкнутая программная среда (ЗПС)
- Контроль целостности (КЦ)
- Антивирус
- Паспорт ПО

Замкнутая программная среда

- **Гарантирует запуск на компьютере только разрешенных приложений/скриптов из белого списка**

Контроль целостности

- **Контролирует неизменность файлов**

Антивирусный модуль

- **Обновляемая база доверенных сигнатур позволяет распознать вредоносную активность**

Паспорт ПО

- **Инструмент администратора ИБ для выявления новых исполняемых файлов и библиотек**

МОЖНО ЛИ ДОВЕРЯТЬ МЕХАНИЗМАМ SNS?

КОД БЕЗОПАСНОСТИ

МОЖНО!

ДОВЕРЕННАЯ СРЕДА – инструмент внешней защиты механизмов Secret Net Studio 8.5 от атак с любым уровнем прав.

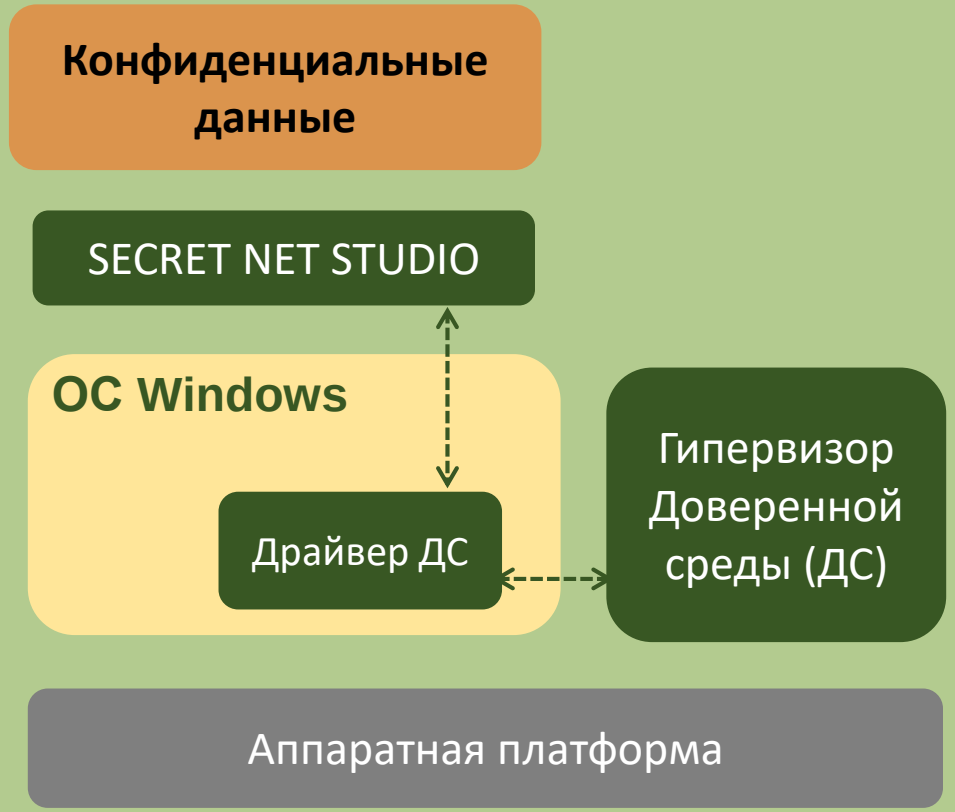
- На процессы SNS идет атака напрямую с системными правами?
  Доверенная среда это остановит!
- Злоумышленник пытается эксплуатировать уязвимость какого-либо драйвера на компьютере?
  Доверенная среда это остановит!

КОД БЕЗОПАСНОСТИ

КАК РАБОТАЕТ ДОВЕРЕННАЯ СРЕДА

- Загружается до операционной системы и работает параллельно
- Использует недоступные штатной ОС ресурсы:
  - Выделенное ядро процессора
  - Область оперативной памяти

- Доверенная среда “смотрит” внутрь ОС и реагирует на сигналы атак
- ОС и приложениям внутри **ничего о ДС не известно!**



УДОБСТВО ПРИМЕНЕНИЯ В ОРГАНИЗАЦИЯХ ЛЮБОГО РАЗМЕРА

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO 8.5 позволяет выполнить

Соответствие нормативным требованиям

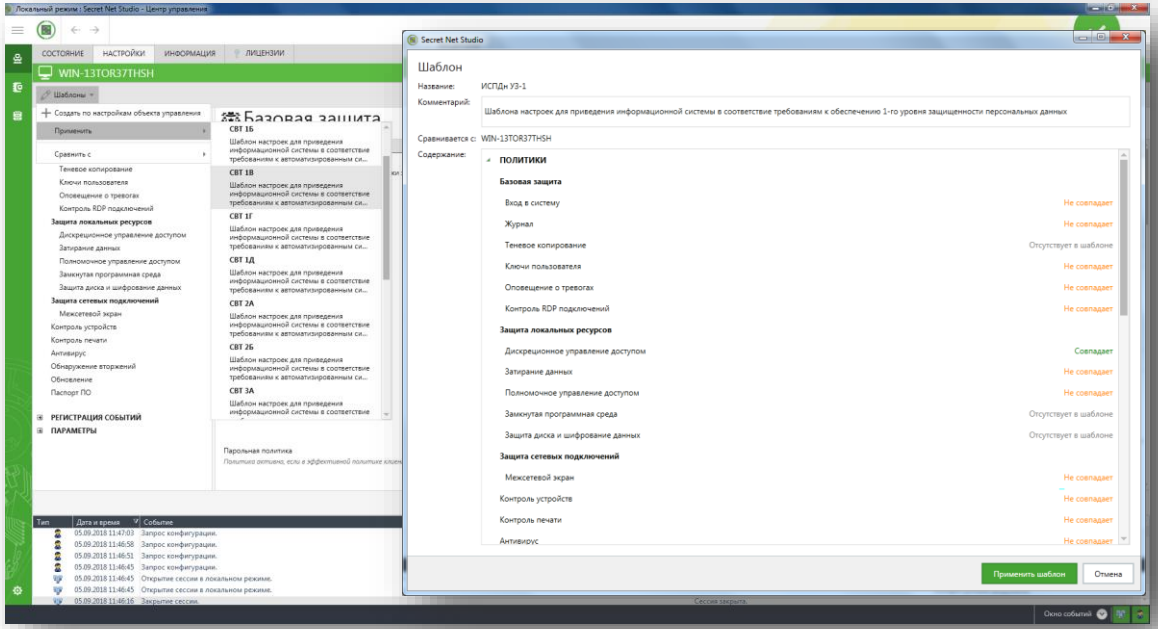
Более 60% всех мер защиты значимых объектов КИИ РФ из приказа ФСТЭК России № 239

Более 50% всех требований по защите ГИС из приказа ФСТЭК России № 17

Более 50% всех мер защиты ИСПДн из приказа ФСТЭК России № 21.

КОД БЕЗОПАСНОСТИ

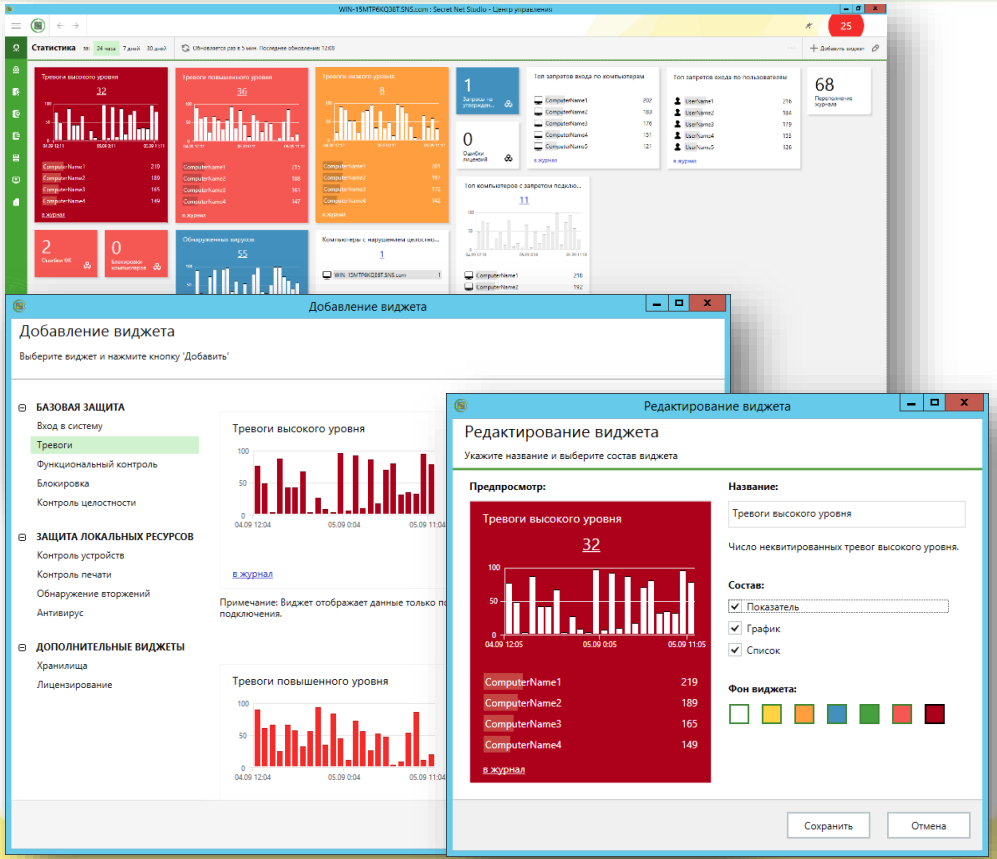
ШАБЛОНЫ ПОЛИТИК



- ✓ Преднастроенные шаблоны политик в соответствие с требованиями регуляторов
- ✓ Создание собственных шаблонов с настроенного АРМ
- ✓ Сравнение текущих настроек АРМ с шаблоном
- ✓ Централизованная рассылка шаблонов

КОД БЕЗОПАСНОСТИ

ЦЕНТРАЛИЗОВАННОЕ АДМИНИСТРИРОВАНИЕ

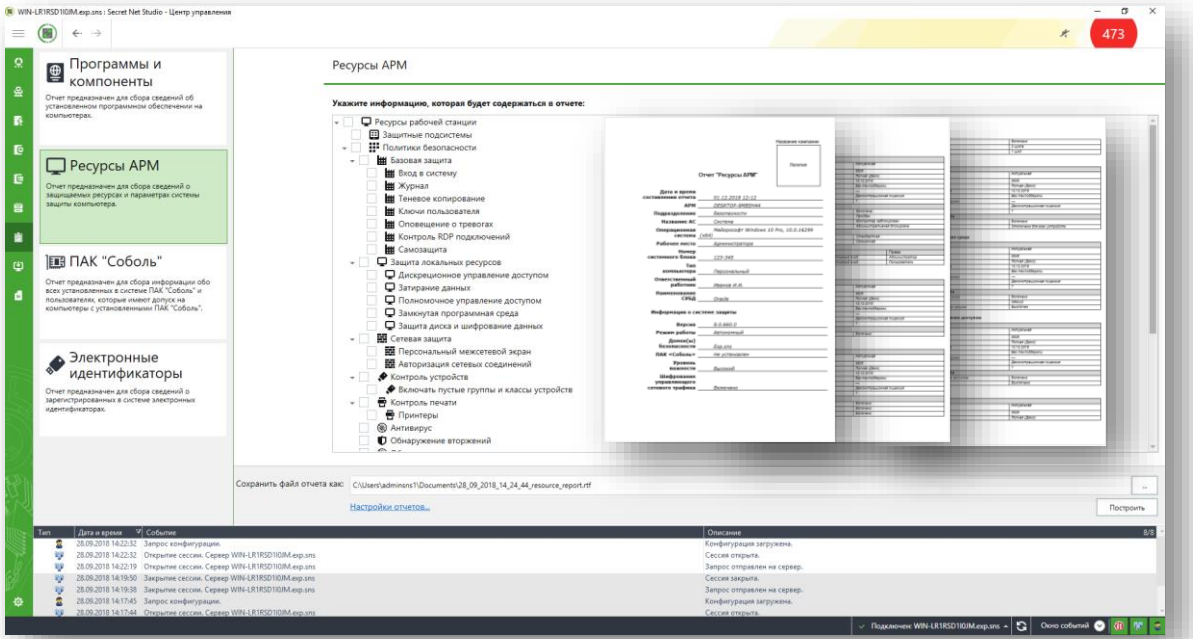


Администратору сервера безопасности доступно:

- ✓ Визуальное представление о всех тревогах на одном экране
- ✓ До 50 виджетов на одном экране, 20 типов настраиваемых виджетов
- ✓ Статистика тревог различных защитных подсистем
- ✓ Возможность создания групп мониторинга

КОД БЕЗОПАСНОСТИ

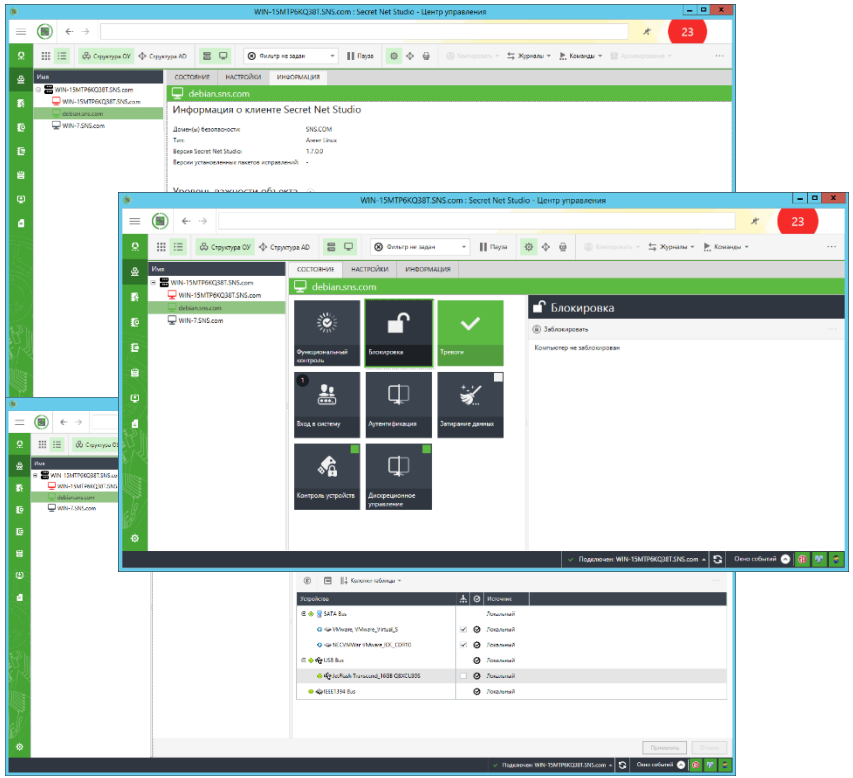
ГЕНЕРАЦИЯ ОТЧЕТОВ



- ✓ Отчет по установленному программному обеспечению на компьютере
- ✓ Отчет о защищаемых ресурсах, состоянии и настройках защитных компонентов
- ✓ Отчет о всех установленных в системе ПАК «Соболь» и пользователей с правом допуска
- ✓ Отчет о всех электронных идентификаторах, зарегистрированных в системе

КОД БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ КЛИЕНТАМИ SECRET NET LSP



Администратору безопасности Secret Net Studio 8.5 для агентов Linux доступны возможности:

- ✓ Отображение состояния компьютеров и событий НСД
- ✓ Получение журналов по расписанию и по команде
- ✓ Оперативное управление: блокировка, перезагрузка, выключение
- ✓ Управление защитными подсистемами (Вкл\Выкл)
- ✓ Управление контролем устройств

ИНТЕГРИРОВАННАЯ АРХИТЕКТУРА ЗАЩИТЫ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ИНТЕГРАЦИЯ С ПАК «СОБОЛЬ» И SECRET NET LSP

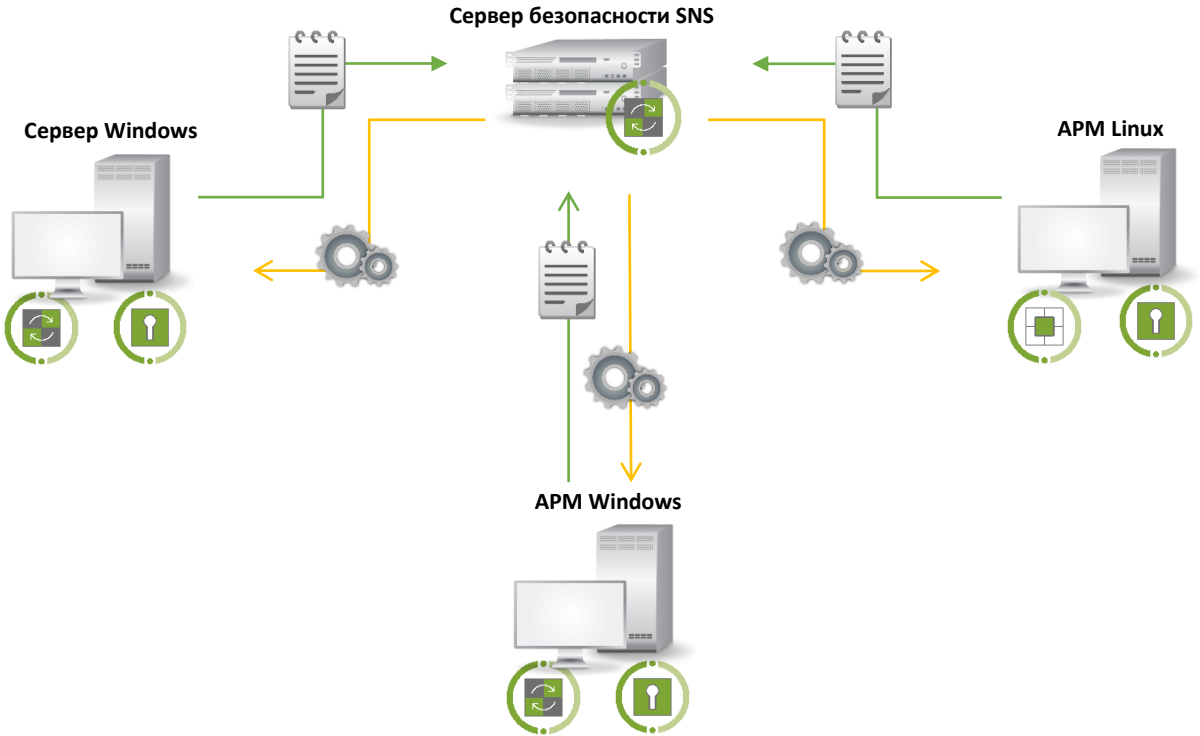
Единый идентификатор для:

- ПАК «Соболь» 4.2
- Secret Net Studio 8.5 / Secret Net LSP 1.9
- входа в операционную систему
- электронной подписи

КОД БЕЗОПАСНОСТИ

ИНТЕГРАЦИЯ С ПАК «СОБОЛЬ» И SECRET NET LSP

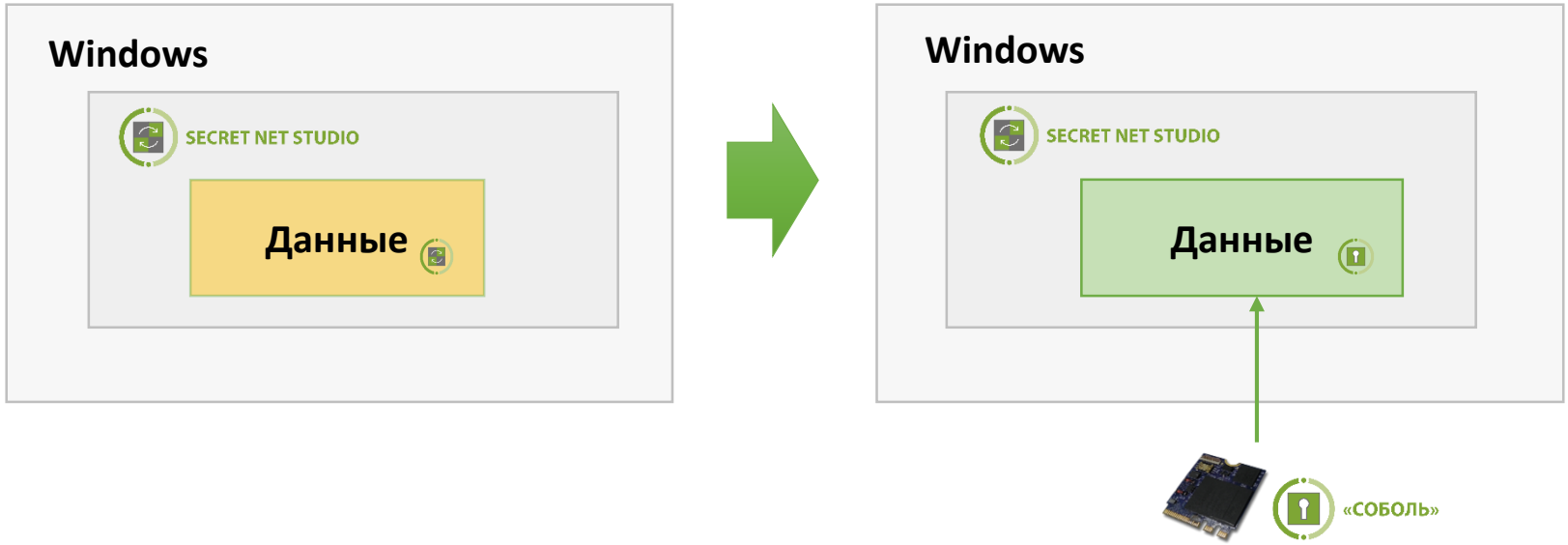
- Единые политики безопасности для ПАК «Соболь» и Secret Net Studio/Secret Net LSP
- Единый журнал событий безопасности



КОД БЕЗОПАСНОСТИ

ИНТЕГРАЦИЯ С ПАК «СОБОЛЬ»

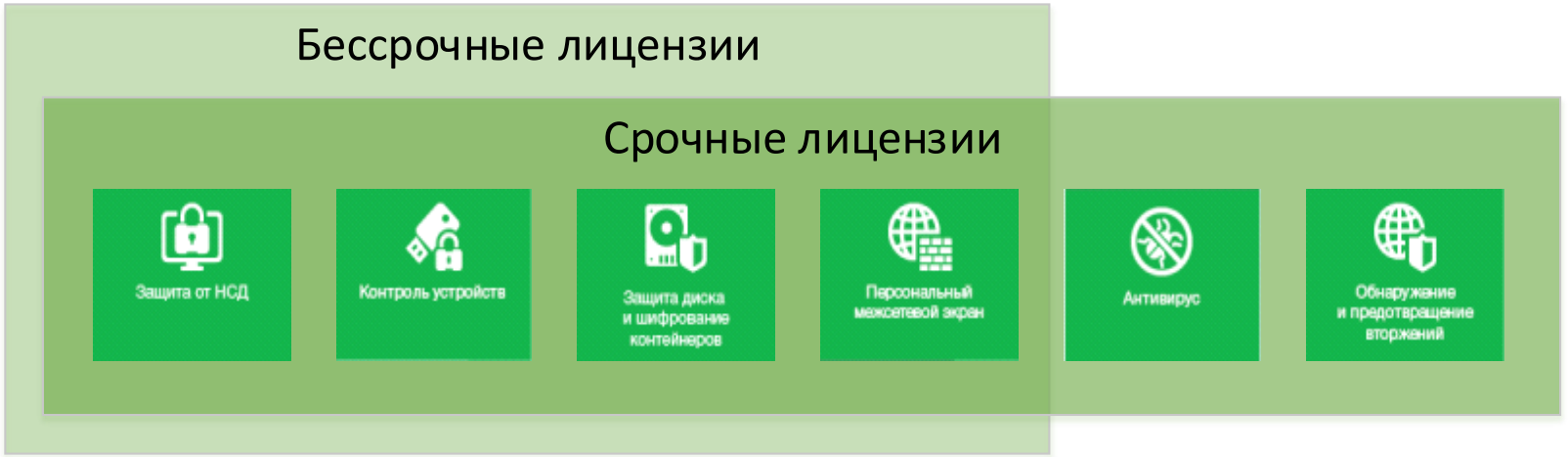
- Усиление контроля целостности на рабочих станциях и серверах под защитой Secret Net Studio 8.5 с помощью ПАК «Соболь»



КОД БЕЗОПАСНОСТИ

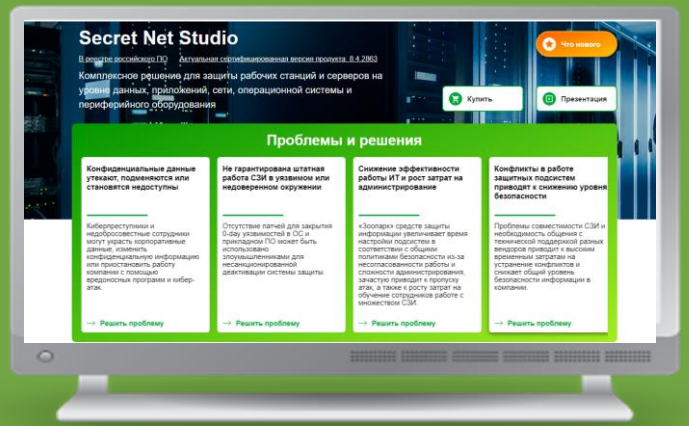
ЛИЦЕНЗИРОВАНИЕ SECRET NET STUDIO

- Лицензируются только защитные компоненты по количеству компьютеров.
- Нет дополнительных лицензий на сервер безопасности, терминальные подключения, централизованное управление и управление лицензиями.
- Срочные и бессрочные лицензии



КОД БЕЗОПАСНОСТИ

УЗНАТЬ ПОДРОБНЕЕ



https://www.securitycode.ru/products/secret-net-studio/

- Подробное описание продукта
- Техническая документация
- Листовки, презентации
- Сертификаты соответствия
- Онлайн-калькулятор для расчета стоимости
- Демоверсия

Для авторизованных партнеров компании «Код Безопасности» доступен закрытый раздел с дополнительными материалами

О КОМПАНИИ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ФАКТЫ О КОМПАНИИ

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

Более 20 лет на страже безопасности крупнейших предприятий России. Ведет свою деятельность на основании 9 лицензий ФСТЭК, ФСБ и Минобороны России.

Технологии защиты обеспечивают безопасность 1 200 000 компьютеров в 32 000 организаций.
3 центра разработки: Москва, Санкт-Петербург, Пенза.

Более 400 квалифицированных специалистов R&D, имеющих уникальные компетенции.

Более 50 разработанных СЗИ и СКЗИ.

Более 60 действующих сертификатов соответствия подтверждают высокое качество продуктов.

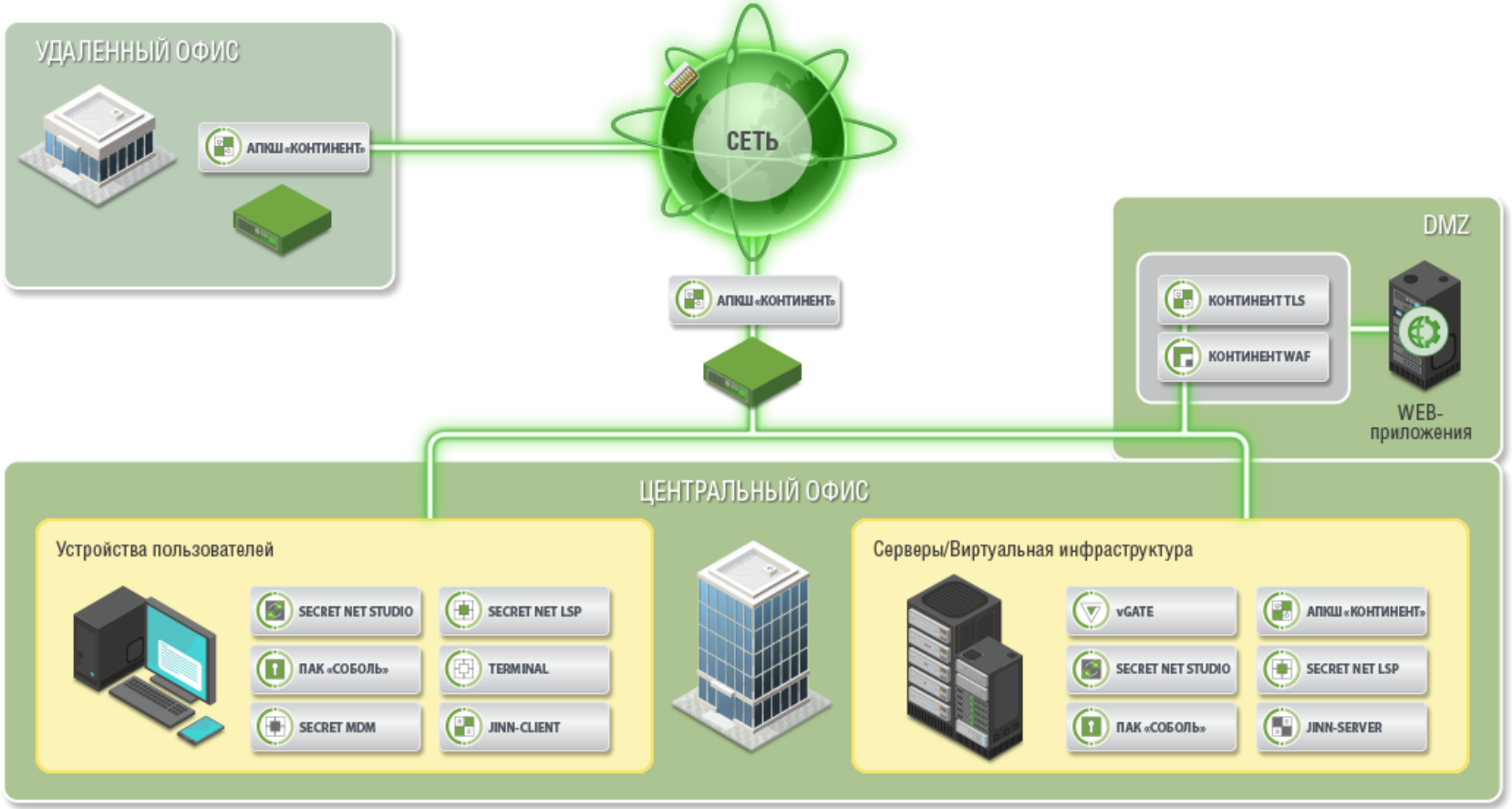
Партнерская сеть компании насчитывает более 900 авторизованных партнеров.

Компетентность «Кода Безопасности» подтверждена независимыми аналитиками:

- «Крупнейшие производители высокотехнологичного оборудования»: №1 («Эксперт РА»), №3 («Коммерсант»).
- «Крупнейшие разработчики программного обеспечения»: №7 («Эксперт РА»), №9 («Коммерсант»).
- «Крупнейшие ИТ-компании России»: №30 («Коммерсант»), №47 (TAdviser).

КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ИНФРАСТРУКТУРЫ



КОД БЕЗОПАСНОСТИ

НАМ ДОВЕРЯЮТ

ГОСУДАРСТВЕННЫЕ ОРГАНИЗАЦИИ:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

СИЛОВЫЕ СТРУКТУРЫ:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

ТЕЛЕКОММУНИКАЦИОННЫЕ КОМПАНИИ:

- ПАО «Ростелеком»
- ФГУП «Почта России»
- ГК «АКАДО Телеком»
- АО «Воентелеком»

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- АО «Страховая группа МСК»
- ПАО «ВТБ24»
- ПАО «Банк «Возрождение»

ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»
- ГКНПЦ им. М.В. Хруничева

ПРЕДПРИЯТИЯ ТЭК:

- Государственная корпорация по атомной энергии «Росатом»
- ПАО «Газпром»
- ОАО «АК «Транснефть»
- ОАО «НК «Роснефть»

Спасибо за внимание!

По вопросам стоимости и покупки продуктов:
buy@securitycode.ru
Служба технической поддержки:
support@securitycode.ru

КОД БЕЗОПАСНОСТИ

info@securitycode.ru
http://securitycode.ru