КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

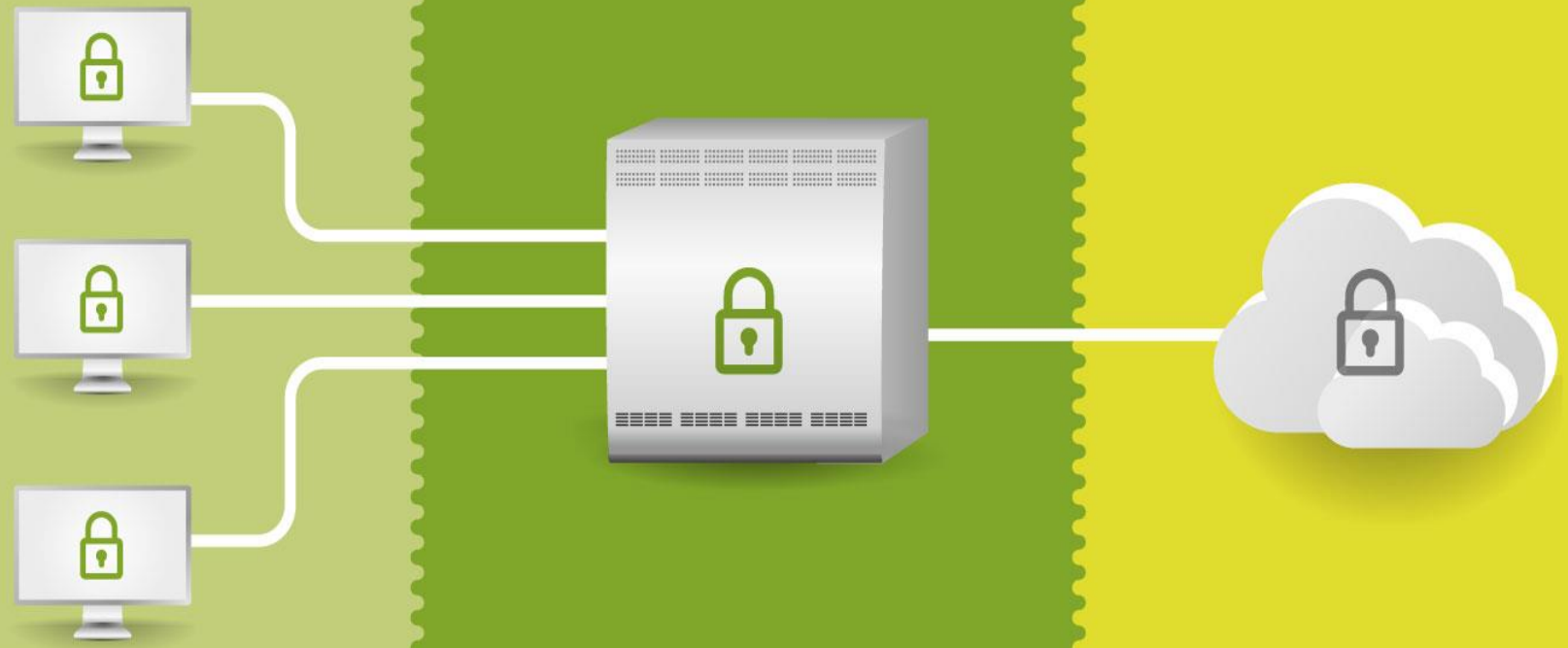
Ижевск 2019

КОД БЕЗОПАСНОСТИ

СЛОЖНОСТЬ УПРАВЛЕНИЯ И ОТСУТСТВИЕ СПЕЦИАЛИСТОВ

КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЕ РЕШЕНИЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД

- Secret Net Studio
- ПАК Соболь
- Terminal
- Jinn

Рабочие станции и сервера

- Secret MDM
- Secret Phone

Мобильные устройства

- АПКШ Континент L3VPN
- АПКШ Континент L2VPN
- АПКШ Континент СД
- Континент АП
- Континент TLS VPN
- Континент IDS/IPS
- Континент WAF

Локальные сети и межсетевое взаимодействие

- vGate (VMware)
- vGate (Hyper-V)

Виртуализация

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO

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

- Защита от НСД
- Контроль устройств
- Защита диска и шифрование контейнеров
- Персональный межсетевой экран
- Антивирус
- Обнаружение и предотвращение вторжений

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАТЫ SECRET NET STUDIO

SECRET NET STUDIO – C (версия 8.4.2863.0)

Сертификат соответствия ФСТЭК России № 3675, действителен до 12.12.2019

СВТ-3, МЭ-2 (тип «В»), НДВ-2

Может применяться в АС до класса 1Б включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

SECRET NET STUDIO (версия 8.4.2863.0)

Сертификат соответствия ФСТЭК России № 3745, действителен до 16.05.2020

СВТ-5, СКСН-4 (уровень подключения), МЭ-4 (тип «В»), СОВ-4 (уровень узла), САВЗ-4 (все типы), НДВ-4

Может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

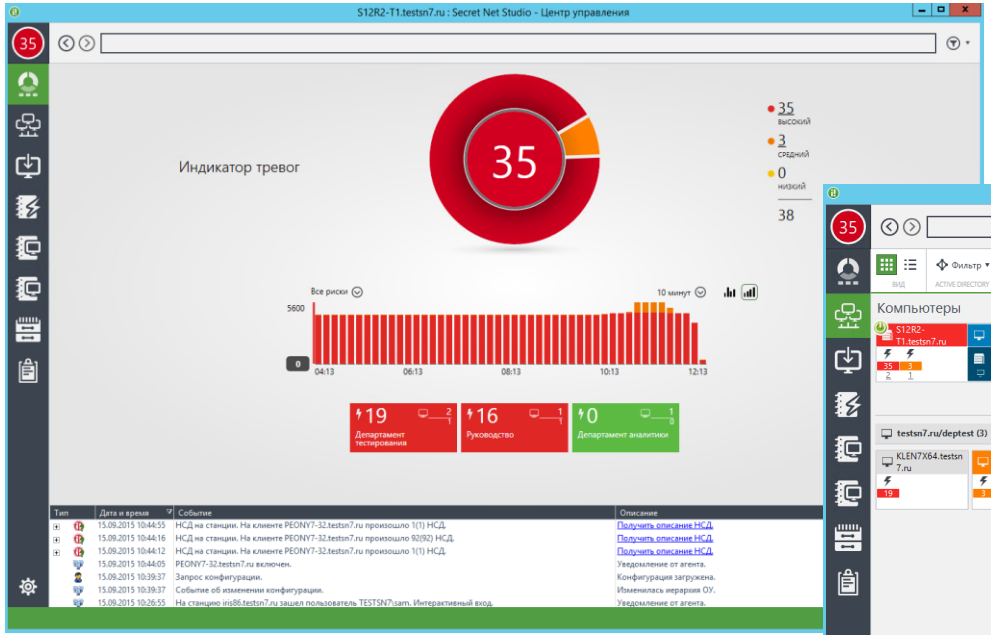
КОД БЕЗОПАСНОСТИ

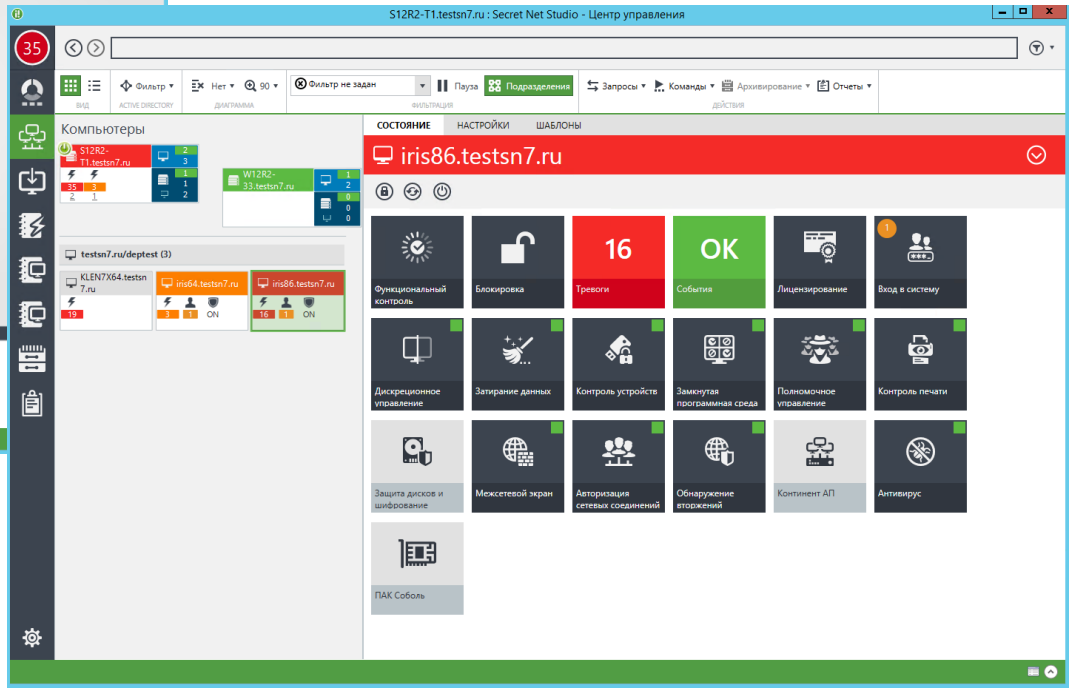
ЗАЩИТНЫЕ МЕХАНИЗМЫ

- Шифрование данных
- Теневое копирование
- Маркировка документов
- Замкнутая программная среда
- Межсетевой экран
- Авторизация сетевых соединений
- Защита от вторжений
- «Континент-АП» (VPN-клиент)
- Усиленный вход в систему
- Контроль целостности
- Антивирус
- Дискреционное управление доступом
- Мандатное управление доступом
- Затирание данных
- Контроль устройств
- Контроль печати
- Интеграция с ПАК «Соболь»

КОД БЕЗОПАСНОСТИ

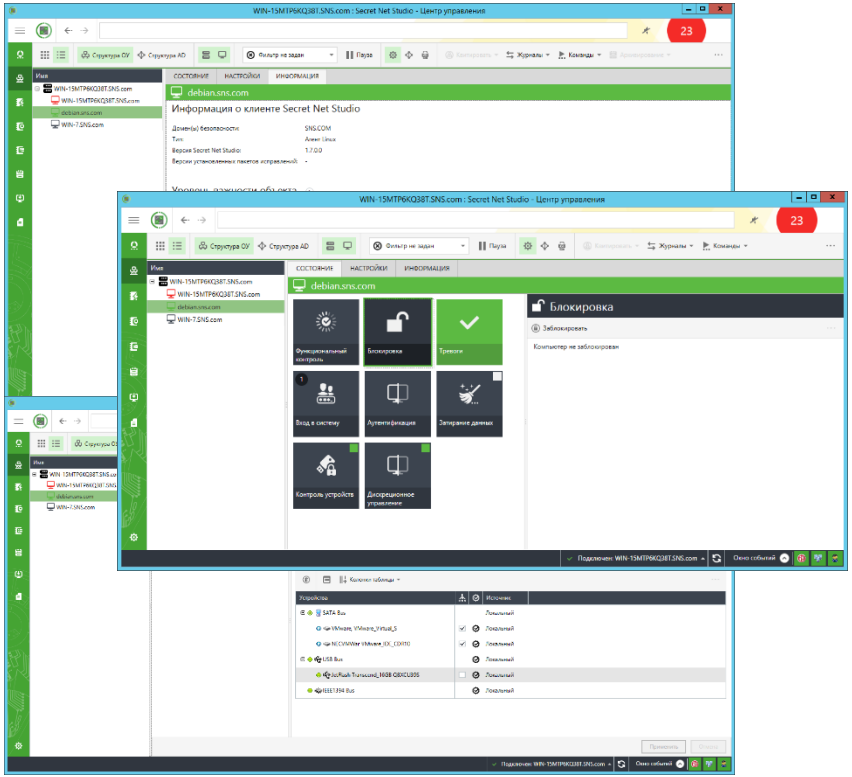
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИ





КОД БЕЗОПАСНОСТИ

Secret Net Studio
Централизованное управление клиентами Secret Net LSP

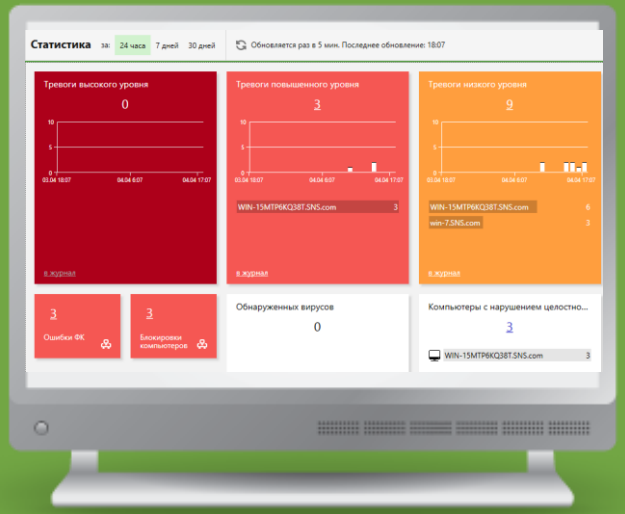


В программе управления Secret Net Studio 8.4 администратору безопасности для агентов Linux доступны возможности:

- ✓ 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

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO



МОНИТОРИНГ УГРОЗ

ГРАФИЧЕСКАЯ ПАНЕЛЬ

Позволяет осуществлять общий мониторинг защищенности системы

ПЕРЕДАЧА СОБЫТИЙ НА ПАНЕЛЬ, E-MAIL, SNMP

НАСТРАИВАЕМЫЕ СИГНАЛЫ ТРЕВОГИ

МОНИТОРИНГ ПО ГРУППАМ

Удобная группировка защищаемых компьютеров для наблюдения и раздельного отображения состояния

ПАСПОРТ ПО

ПЕЧАТНАЯ ФОРМА СВЕДЕНИЙ О КОМПЬЮТЕРАХ

Возможность печати и экспорта сведений о компьютерах, отображаемых в панели «Компьютеры» в режиме «Таблица»

КВИТИРОВАНИЕ СОБЫТИЙ

Проставление отметок о прочтении и добавление комментариев к событиям безопасности

КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO

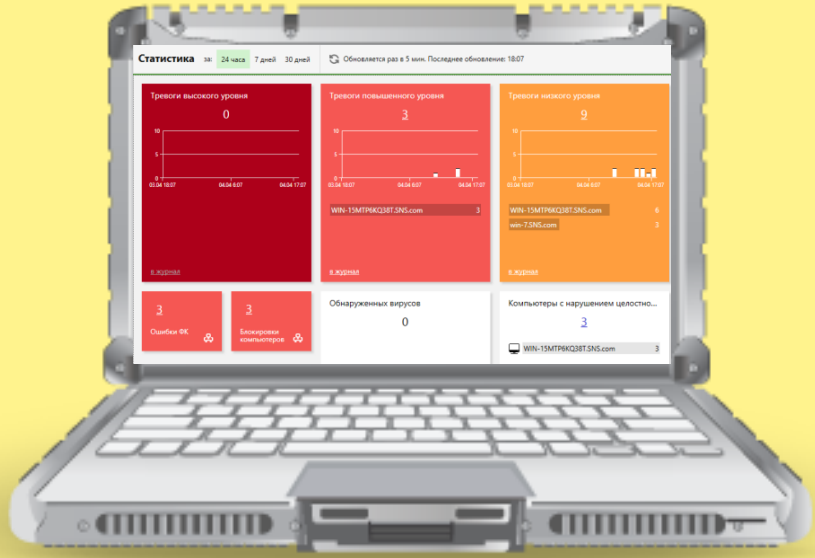
Высокий уровень

Повышенный уровень

Низкий уровень

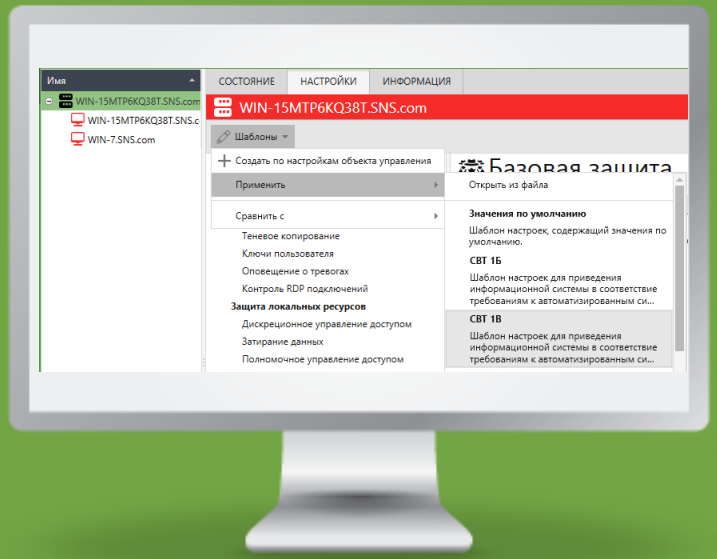
СТЕПЕНЬ ЗНАЧИМОСТИ

Тревоги - события, регистрируемые на защищаемых компьютерах в журнале Secret Net Studio или штатном журнале безопасности ОС и имеющие тип «Аудит отказов» или «Ошибки»



КОД БЕЗОПАСНОСТИ

SECRET NET STUDIO



ШАБЛОНЫ ПОЛИТИК

ПРЕДНАСТРОЕННЫЕ ШАБЛОНЫ ПОЛИТИК

Готовые шаблоны настроек для автоматизированного приведения в соответствие требованиям к АС (1Б, 1В, 1Г), ГИС (1, 2, 3 классы), ИС ПДн (1, 2, 3 уровни защищенности).

Возможность создания своих шаблонов, снятие снимка шаблона с настроенного АРМ

ВОЗМОЖНОСТЬ РАСПРОСТРАНЕНИЯ ШАБЛОНОВ

Распространение шаблона на все компьютеры или на выбранные компьютеры

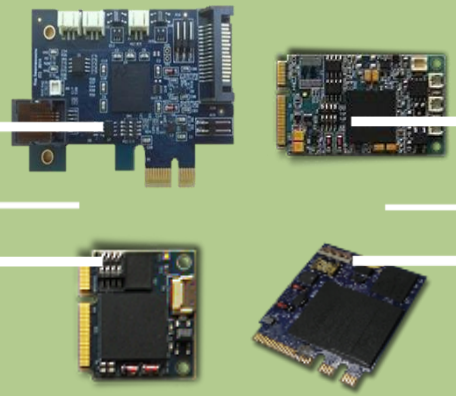
СРАВНЕНИЕ НАСТРОЕК АРМ С ШАБЛОНОМ

Возможность автоматизированного сравнения текущих настроек рабочей станции с настройками из эталонного шаблона

КОД БЕЗОПАСНОСТИ

НОВОЕ ПОКОЛЕНИЕ «СОБОЛЕЙ»

- Новая версия прошивки 4.0 с поддержкой новых моделей ПК и последних требований контролирующих органов.
- Новая плата в форм-факторе M.2 для ноутбуков, моноблоков и мини ПК. Поддержка идентификаторов JaCarta
- Функционирование в среде UEFI.
- Поддержка разметки дисков GPT и MBR
- Новая плата формата PCI-Express компактного размера, для установки в мини-корпусах.
- Наличие графического интерфейса, поддерживающего работу с мышью. Переработан процесс инициализации и обновления (без вскрытия корпуса)



КОД БЕЗОПАСНОСТИ

ЗАЩИЩЁННЫЙ ТЕРМИНАЛЬНЫЙ КЛИЕНТ

- Собственная ОС на базе Linux - «Continent OS».
- Доверенная загрузка.
- Защита от НСД и контроль подключения устройств.
- Криптографическая защита канала подключения.
- Централизованное управление и мониторинг.

КОД БЕЗОПАСНОСТИ

SECRET MDM

SECRET MDM
Управление корпоративной мобильностью и защита данных на мобильных устройствах

Предназначен для решения следующих задач:

- Комплексное управление корпоративной мобильностью
- Защита данных на мобильных устройствах
- Защита передаваемых сообщений и телефонии
- Организация защищенного доступа с мобильных устройств к корпоративным службам

Возможности продукта:

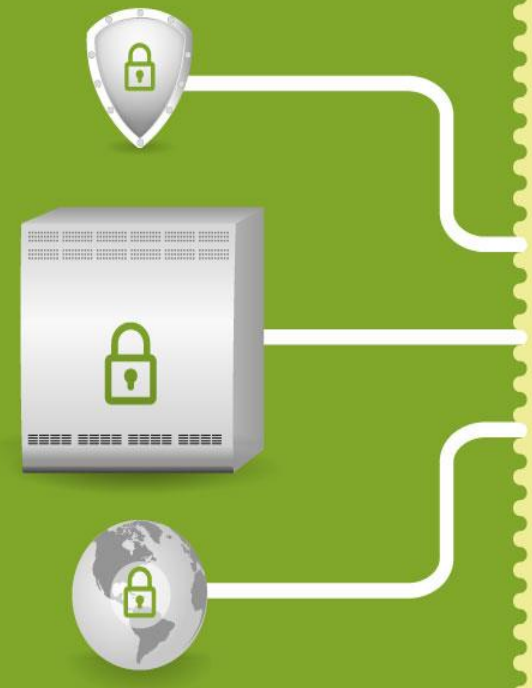
- Управление политиками блокировки, длиной и сложностью пароля
- Дистанционная блокировка и затирание данных (wipe при потере или краже устройства)
- Разрешения на использование встроенного
- микрофона, видеокамеры,
- Bluetooth, NFC
- Дистанционная установка и удаление приложений
- Запуск только разрешенных приложений
- Дистанционное распространение настроек для подключения к сервисам Exchange, WiFi точкам доступа
- Обнаружение действий злоумышленника при получении jailbreak и root доступа

КОНТИНЕНТ СОВ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ СОВ 4.0



ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

СОВ «КОНТИНЕНТ» 4.0

Система обнаружения и предотвращения вторжений (IDS/IPS) нового поколения «Континент» 4.0

Сертификаты

Продукт сертифицирован ФСТЭК России на СОВ 3/НДВ 2 для защиты АС до 1В включительно (гостайна с грифом «секретно»), ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно.

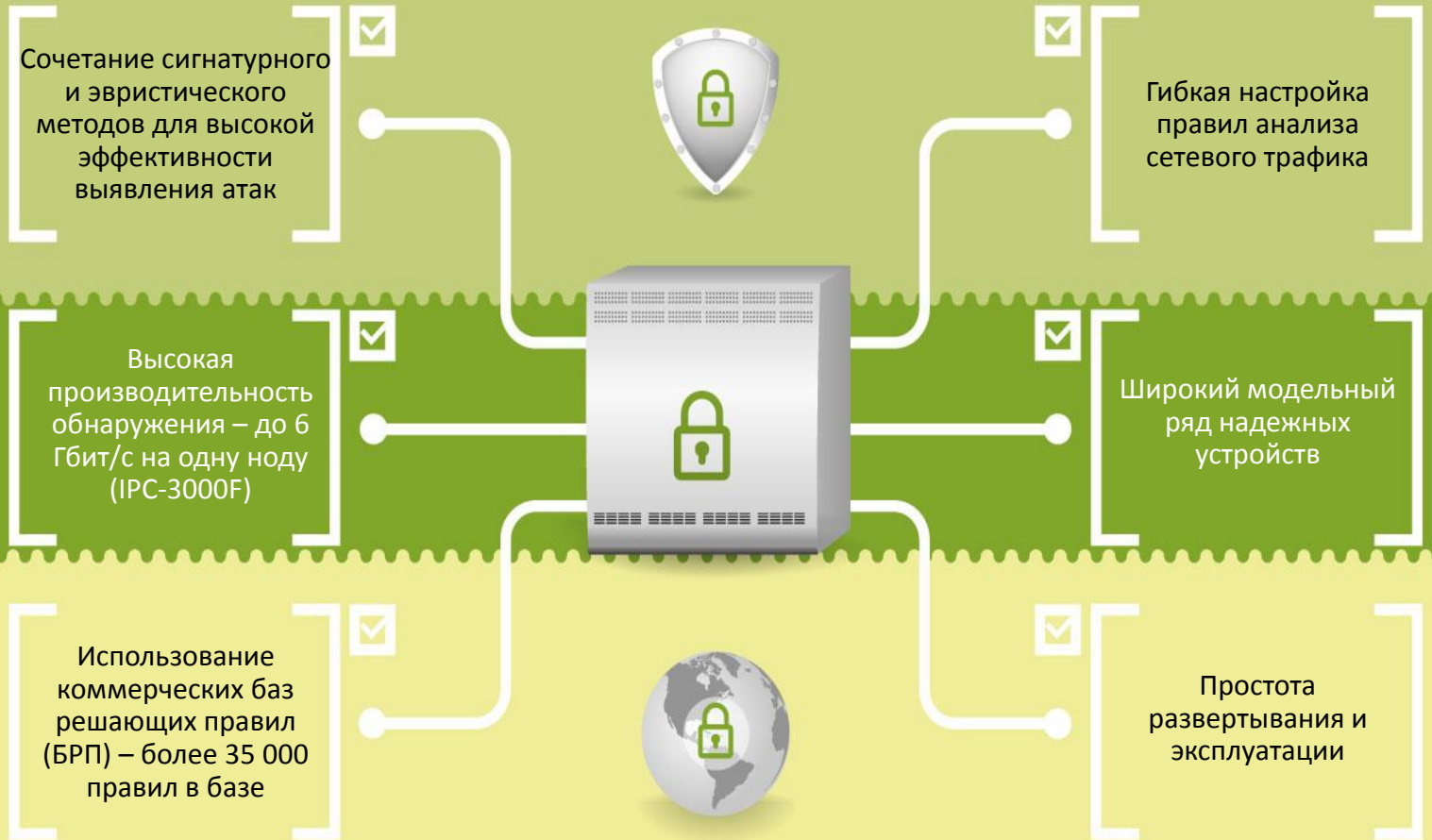
КОД БЕЗОПАСНОСТИ

ВОЗМОЖНОСТИ СОВ «КОНТИНЕНТ» 4.0

КОД БЕЗОПАСНОСТИ

ПРЕИМУЩЕСТВА СОВ «КОНТИНЕНТ» 4.0

- Сочетание сигнатурного и эвристического методов для высокой эффективности выявления атак
- Гибкая настройка правил анализа сетевого трафика
- Высокая производительность обнаружения – до 6 Гбит/с на одну ноду (IPC-3000F)
- Широкий модельный ряд надежных устройств
- Использование коммерческих баз решающих правил (БРП) – более 35 000 правил в базе
- Простота развертывания и эксплуатации



ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

УГРОЗЫ БЕЗОПАСНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

- Обработка информации разных уровней на одном сервере
- Отсутствие инструментов управления безопасностью виртуальной среды
- Появление суперпользователя – администратора виртуальной среды с неограниченными правами доступа ко всем виртуальным машинам (ВМ)

- Непригодность традиционных средств защиты для виртуализованной инфраструктуры
- Уязвимости платформ виртуализации
- Простота внесения изменений в образы ВМ и виртуальную инфраструктуру в целом

КОД БЕЗОПАСНОСТИ

ПРОДУКТ

ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

vGATE

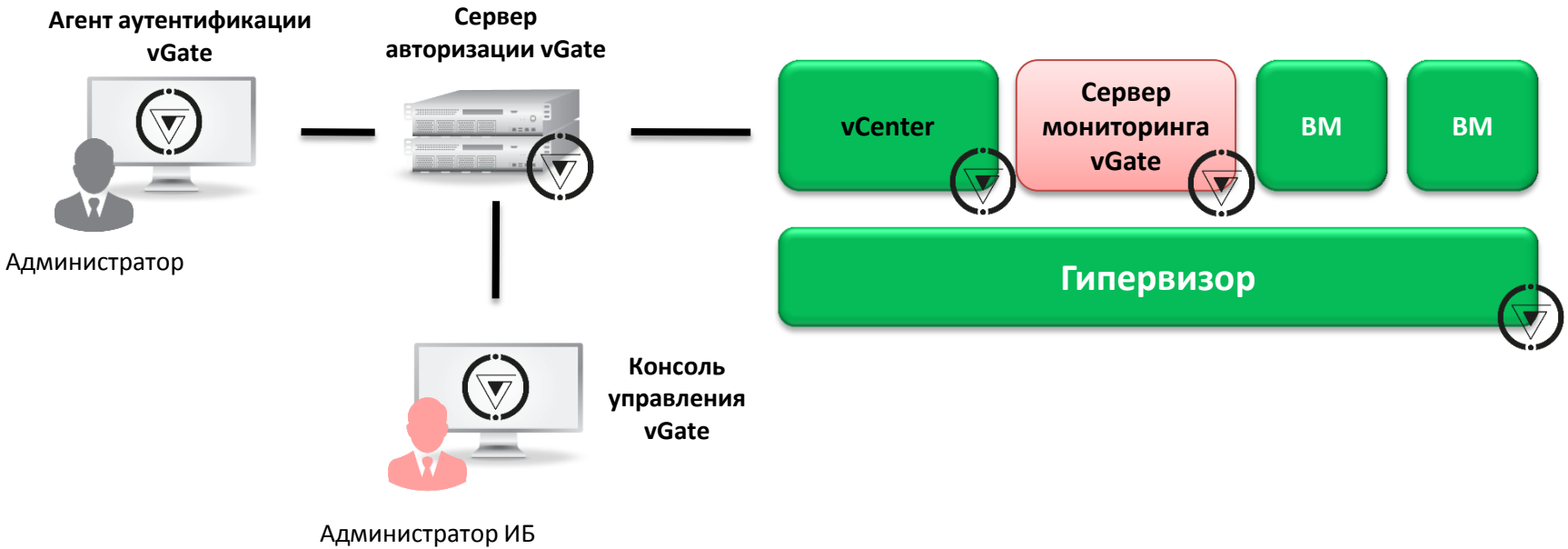
Сертифицированное средство защиты виртуальной инфраструктуры

Сертификаты

ФСТЭК России:
vGate R2: СВТ 5/НДВ 4, применяется для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до К1 и АСУ ТП до К1 включительно.
vGate-S R2: ТУ/НДВ 2, применяется для защиты АС до класса 1Б включительно и ИСПДн до УЗ1 включительно.

КОД БЕЗОПАСНОСТИ

АРХИТЕКТУРА vGATE



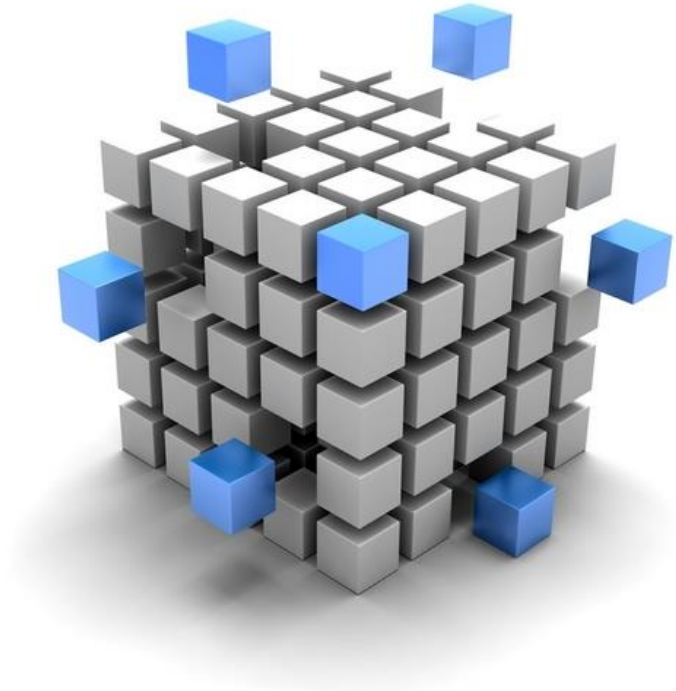
КОД БЕЗОПАСНОСТИ

ВОЗМОЖНОСТИ vGATE

КОД БЕЗОПАСНОСТИ

ЗАЩИТА ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ С VGATE 4.1

- Планируется межсетевой экран уровня гипервизора (аналог VMware NSX, Check Point vSEC)
  - ✓ Для микросегментации виртуализованных сред
  - ✓ Планируется сертификат по МЭ тип «Б» класс 4
- Поддержка Скала-Р
- Поддержка среды KVM



КОД БЕЗОПАСНОСТИ

ШАБЛОНЫ ПОЛИТИК БЕЗОПАСНОСТИ

- Приказ №17 (ГИС)
- Приказ №21 (ИСПДн)
- РД АС
- СТО БР ИББС
- PCI DSS
- VMware Hardening Guide
- CIS Benchmarks
- **ГОСТ Р 56938-2016 Защита информации при использовании технологий виртуализации** NEW
- **VMware vSphere 6.5 Security Configuration Guide** NEW

КОД БЕЗОПАСНОСТИ

Направления «Кода Безопасности» и требования ФСТЭК по защите КИИ

Направление	Endpoint	Network	Virtualization
Идентификация и аутентификация (ИАФ)	+	+	+
Управление доступом (УПД)	+	+	+
Ограничение программной среды (ОПС)	+		+
Защита машинных носителей информации (ЗНИ)	+		
Аудит безопасности (АУД)	+	+	+
Антивирусная защита (АВЗ)	+		
Предотвращение вторжений (компьютерных атак) (СОВ)	+	+	
Обеспечение целостности (ОЦЛ)	+	+	+
Обеспечение доступности информации (ОДТ)	+	+	+
Защита технических средств и систем (ЗТС)	Организационные меры		
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	+ (+Терминал, MDM)	+	+
Реагирование на инциденты информационной безопасности (ИНЦ)	+	+	+
Управление конфигурацией (УКФ)	+		+
Управление обновлениями программного обеспечения (ОПО)	+		+
Планирование мероприятий по обеспечению безопасности (ПЛН)	Организационные меры		
Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	+	+	+
Информирование и обучение персонала (ИПО)	Организационные меры		

Спасибо за внимание!

КОД БЕЗОПАСНОСТИ

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