## СЗИ от НСД Secret Net

Более 15 лет является одним из лучших средств защиты информации от несанкционированного доступа к информационным ресурсам рабочих станций и серверов.

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующих документов:

- №152-ФЗ ("О персональных данных");
- №98-ФЗ ("О коммерческой тайне");
- №5485-1-ФЗ ("О государственной тайне");
- СТО БР ИББС (Стандарт Банка России).

Сертификаты ФСТЭК и Министерства обороны России позволяют использовать СЗИ от НСД Secret Net для защиты:

- конфиденциальной информации и государственной тайны в автоматизированных системах (АС) до класса 1Б включительно;
- информационных систем персональных данных (ИСПДн) до класса У31 включительно;
- государственных информационных систем (ГИС) до 1 класса защищенности включительно.

**Обновленная версия Secret Net 7**
**Включает множество улучшений и новых возможностей**
Что нового?
Скачать демоверсию

**Ключевые возможности СЗИ от НСД Secret Net:**

- Аутентификация пользователей.
- Разграничение доступа пользователей к информации и ресурсам автоматизированной системы.
- Доверенная информационная среда.
- Контроль утечек и каналов распространения конфиденциальной информации.
- Контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации.
- Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.
- Масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов.
- Защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI).

## СЗИ от НСД Secret Net LSP

Secret Net LSP является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы на платформе Linux в соответствие требованиям регулирующих документов:

- №152-ФЗ ("О персональных данных");
- №98-ФЗ ("О коммерческой тайне");
- СТО БР ИББС (Стандарт Банка России).

Сертификат ФСТЭК России позволяет использовать СЗИ от НСД Secret Net LSP для защиты:

- конфиденциальной информации в автоматизированных системах до класса 1Г включительно;
- информационных систем обработки персональных данных до класса К1 включительно.

**Ключевые возможности Secret Net LSP:**

- Контроль входа пользователей в систему, как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации.
- Разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера.
- Разграничение доступа пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам.
- Уничтожение (затирание) содержимого конфиденциальных файлов при их удалении пользователем.
- Очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств).
- Контроль целостности ключевых компонентов Secret Net LSP и критических объектов файловой системы.
- Регистрация событий безопасности в журнале безопасности. Фильтрация событий безопасности, контекстный поиск в журнале безопасности.
- Контроль действий пользователей: доступ к защищаемым файлам, устройствам и узлам вычислительной сети.
- Аудит действий субъектов с объектами файловой системы и сетевых соединений, аудит отчуждения информации.
- Управление СЗИ - с помощью графического интерфейса и командной строки.
- Возможна установка на тонкие клиенты, работающие под ОС Linux, и совместная работа с СЗИ Secret Net (для ОС Windows), установленным на терминальном сервере.

## Электронный замок «Соболь».

Это аппаратно-программное средство защиты компьютера от несанкционированного доступа (аппаратно-программный модуль доверенной загрузки).

Электронный замок «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

**Возможности электронного замка «Соболь»**

- Аутентификация пользователей.
- Блокировка загрузки ОС со съемных носителей.
- Контроль целостности программной среды.
- Контроль целостности системного реестра Windows.
- Контроль конфигурации компьютера (PCI-устройств, ACPI, SMBIOS).
- Сторожевой таймер.
- Регистрация попыток доступа к ПЭВМ.

Подробнее о возможностях электронного замка «Соболь».

**Достоинства электронного замка «Соболь»**

- Наличие сертификатов ФСБ и ФСТЭК России.
- Защита информации, составляющей государственную тайну.
- Помощь в построении прикладных криптографических приложений.
- Простота в установке, настройке и эксплуатации.
- Поддержка 64-битных операционных систем Windows (в том числе Windows 8 и Windows server 2012).
- Поддержка идентификаторов iButton, iKey 2032, eToken PRO, eToken PRO (Java), Rutoken, Rutoken RF.

- Гибкий выбор форматов исполнения платы (PCI, PCI-E, Mini PCI-E) и вариантов комплектации.
- Поддержка файловой системы EXT 4 в ОС семейства Linux.
- Поддержка высокоскоростного режима USB 2.0/3.0 для усиленной идентификации пользователей.

## АПКШ «Континент» 3.6

Сертифицированный ФСБ и ФСТЭК России аппаратно-программный комплекс шифрования «Континент» 3.6 является средством построения виртуальных частных сетей (VPN) на основе глобальных сетей общего пользования, использующих протоколы семейства TCP/IP.

**Применение АПКШ "Континент" 3.6**

АПКШ «Континент» 3.6 обладает всеми необходимыми возможностями, чтобы обеспечить:

- объединение через Интернет территориально распределенных локальных сетей предприятия в единую сеть VPN;
- возможность удаленного защищенного доступа к информационным ресурсами предприятия для мобильных пользователей, посредством VPN соединения;
- разделение прав доступа между информационными подсистемами организации на сетевом уровне;
- сегментирование ЛВС организации;
- организация защищенного взаимодействия со сторонними организациями;
- безопасное удаленное управление маршрутизаторами.

**Достоинства АПКШ «Континент» 3.6**

- Высокая надежность и отказоустойчивость
- Простота внедрения и обслуживания
- Удобство управления и поддержки
- Высокая пропускная способность
- Высокая масштабируемость
- Поддержка всех современных протоколов и технологий

## vGate

vGate – сертифицированное средство защиты информации для виртуальной инфраструктуры на базе систем VMware vSphere 4, 5, 5.5.

- Позволяет автоматизировать работу администраторов по конфигурированию и эксплуатации системы безопасности.
- Способствует противодействию ошибкам и злоупотреблениям при управлении виртуальной инфраструктурой.
- Позволяет привести виртуальную инфраструктуру в соответствие законодательству, отраслевым стандартам и лучшим мировым практикам.

**Возможности vGate 2.5**

- Усиленная аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности.
- Защита средств управления виртуальной инфраструктурой от НСД.
- Защита ESX-серверов от НСД.
- Поддержка распределенных инфраструктур.
- Мандатное управление доступом.
- Контроль целостности конфигурации виртуальных машин и доверенная загрузка.
- Контроль доступа администраторов ВИ к данным виртуальных машин.
- Регистрация событий, связанных с информационной безопасностью.
- Контроль целостности и доверенная загрузка ESX-серверов и виртуальных машин.
- Контроль целостности и защита от НСД компонентов СЗИ.
- Централизованное управление и мониторинг.

## TrustAccess

TrustAccess — распределенный межсетевой экран высокого класса защиты с централизованным управлением и аудитом для защиты ключевых ресурсов сети от НСД и разграничения доступа к информационным системам.

Внедрение TrustAccess не требует реконфигурирования существующей сетевой инфраструктуры. Продукт пригоден для защиты физических и виртуальных машин, может использоваться как в сетях с доменной организацией, так и в одноранговых сетях.

TrustAccess позволяет управлять доступом к сетевым службам в условиях работы в терминальной среде, разграничить доступ к сетевым ресурсам на основе уровней допуска или должностей пользователей.

**Возможности TrustAccess**

- Аутентификация сетевых соединений на уровне пользователей и компьютеров;
- Фильтрация сетевых соединений;
- Защита сетевых соединений;
- Регистрация событий, связанных с информационной безопасностью;
- Контроль целостности и защита от НСД компонентов СЗИ;
- Централизованное управление;
- Централизованный сбор и отображение данных аудита, связанных с информационной безопасностью;
- Построение отчетов по событиям ИБ, происходящих на защищаемых компьютерах;
- Интеграция с Secret Net 7 (сетевой вариант).