КОД БЕЗОПАСНОСТИ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «СОБОЛЬ» 4.2

ДЛЯ ЧЕГО НУЖЕН МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ?

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

РИСКИ ПРИ ЗАЩИТЕ КОНЕЧНЫХ УСТРОЙСТВ ПРОГРАММНЫМИ СЗИ

Программные СЗИ осуществляют контроль целостности внутри операционной системы. И если ОС будет взломана:

- программные СЗИ можно будет обойти/отключить;
- в файлы и реестр Windows можно будет внести изменения;
- отследить действия злоумышленника будет невозможно.

Поэтому дополнительно требуется контроль целостности до загрузки ОС.

КОД БЕЗОПАСНОСТИ

С ЧЕМ ПРИХОДИТСЯ СТАЛКИВАТЬСЯ?

- Выбор средств вычислительной техники для АРМ, на которых обрабатывается конфиденциальная информация и гостайна, сильно ограничен
- Для восстановления работы после сбоя операционной системы компьютера необходимо вскрытие системного блока для переинициализации АПМДЗ или загрузки с внешнего устройства
- Процесс загрузки компьютера длится долго вследствие расчета контрольных сумм на ресурсах самого АПМДЗ

КОД БЕЗОПАСНОСТИ

ЧТО ДАЕТ ПАК «СОБОЛЬ» 4

- Возможность использовать для обработки конфиденциальных данных и гостайны современные компьютеры на базе UEFI
- Контроль целостности файлов и ключей реестра Windows
- Недоступность системы для неавторизованных пользователей и недоверенных устройств
- Блокировка доступа к компьютеру при обнаружении несанкционированного изменения файлов
- Комплексный подход к защите серверов и рабочих станций при использовании совместно с Secret Net Studio и Secret Net LSP

О ПРОДУКТЕ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ЧТО ТАКОЕ ПАК «СОБОЛЬ»?

ПАК «Соболь»

Сертифицированный аппаратно-программный модуль доверенной загрузки (АПМДЗ) с поддержкой UEFI

Предназначен для:

- защиты конфиденциальной информации, персональных данных, гостайны (гриф «Совершенно Секретно»);
- предотвращения доступа неавторизованных пользователей к информации, обрабатываемой на компьютере;
- информирования администратора комплекса о всех важных событиях ИБ;
- предоставления случайных чисел прикладному ПО.

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАТЫ ПАК «СОБОЛЬ»

ПАК «Соболь»

ФСТЭК России

- 2 класс СДЗ уровня платы расширения

Минобороны России

- НДВ2
- 2 класс СДЗ уровня платы расширения
- АС до 1Б включительно

Может применяться для защиты:

- АС до класса 1Б включительно (защита государственной тайны с грифом «сов. секретно»)
- ИСПДн до УЗ1 включительно
- ГИС до 1 класса включительно
- АСУ ТП до 1 класса включительно
- Значимых объектов КИИ до 1 кат. включительно

Планы по сертификации ФСБ России

- АПМДЗ 1Б

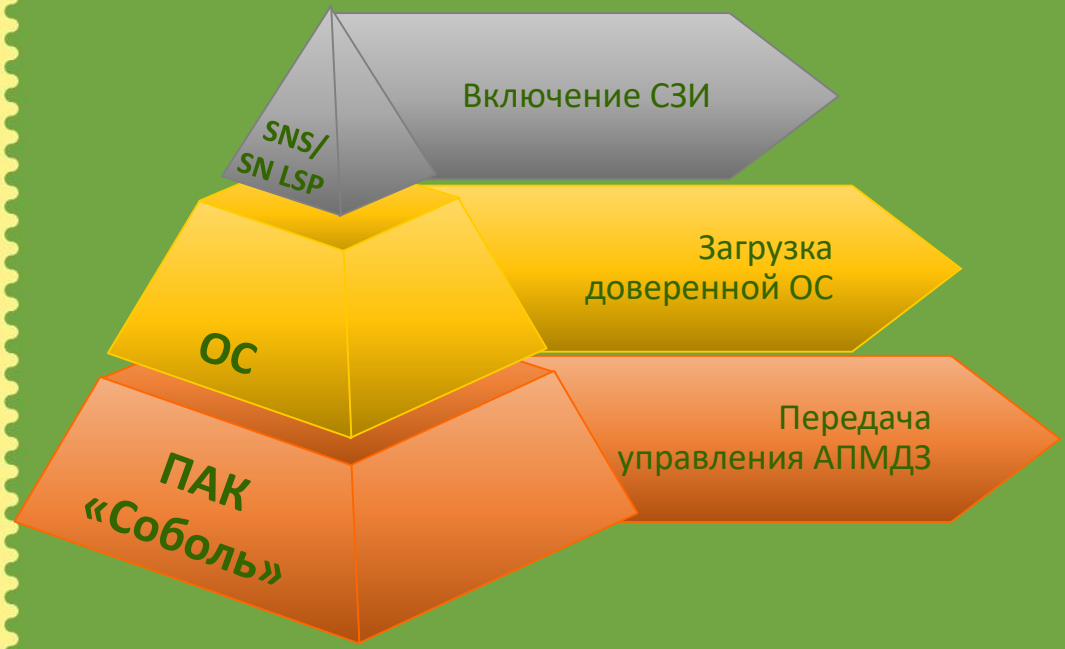
ВАРИАНТЫ ПРИМЕНЕНИЯ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

УСИЛЕНИЕ МЕХАНИЗМА ОБНАРУЖЕНИЯ АТАК

- Защита серверов или рабочих станций от атаки злоумышленника до загрузки ОС
- Интеграция с средствами защиты Secret Net Studio 8.5 и Secret Net LSP 1.9
- Использование единого персонального идентификатора при идентификации и двухфакторной аутентификации пользователей
- Блокировка несанкционированной загрузки ОС со съемных носителей



ВАРИАНТЫ ПРИМЕНЕНИЯ

ВОЗМОЖНОСТИ

КОД БЕЗОПАСНОСТИ

ПРИНЦИП РАБОТЫ

- КОНТРОЛЬ ПЕРЕХОДА УПРАВЛЕНИЯ «СОБОЛЮ»
- ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ
- БЛОКИРОВКА ЗАГРУЗКИ СО СЪЕМНЫХ НОСИТЕЛЕЙ
- КОНТРОЛЬ ЦЕЛОСТНОСТИ ФАЙЛОВ И СЕКТОРОВ ЖЕСТКОГО ДИСКА
- КОНТРОЛЬ ЦЕЛОСТНОСТИ РЕЕСТРА WINDOWS
- КОНТРОЛЬ ЦЕЛОСТНОСТИ АППАРАТНОЙ СРЕДЫ

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

КОНТРОЛЬ ЦЕЛОСТНОСТИ

ВОЗМОЖНОСТИ

Обнаружение действий продвинутого злоумышленника, быстрая реакция на инцидент безопасности и сокращение ресурсов, затрачиваемых на его ликвидацию последствий.

Все это обеспечивается с помощью следующих функций:

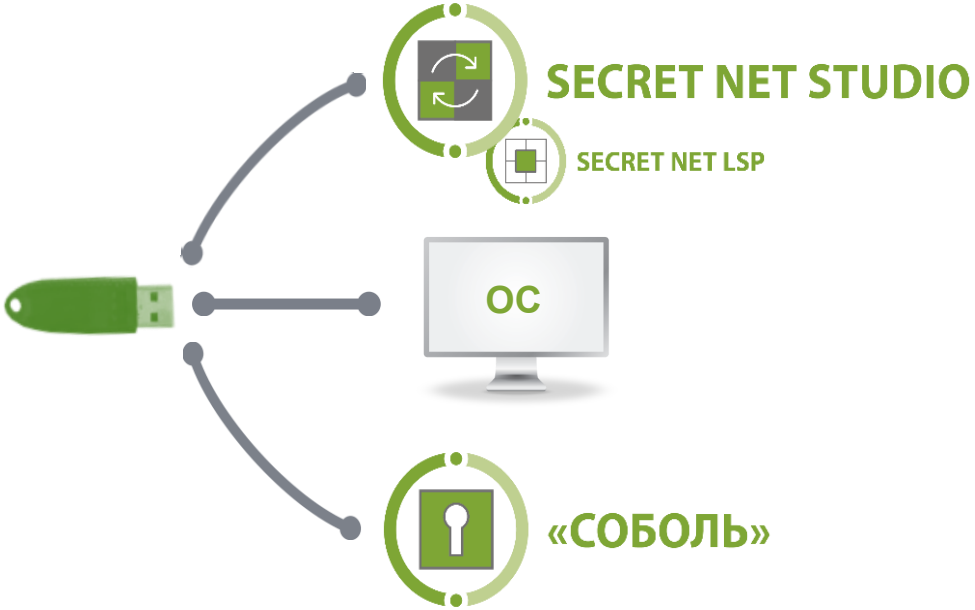
- Контроль целостности реестра Windows
- Контроль целостности файлов до загрузки ОС
- Контроль целостности аппаратной конфигурации компьютера

КОД БЕЗОПАСНОСТИ

ИНТЕГРАЦИЯ С SECRET NET STUDIO И SECRET NET LSP

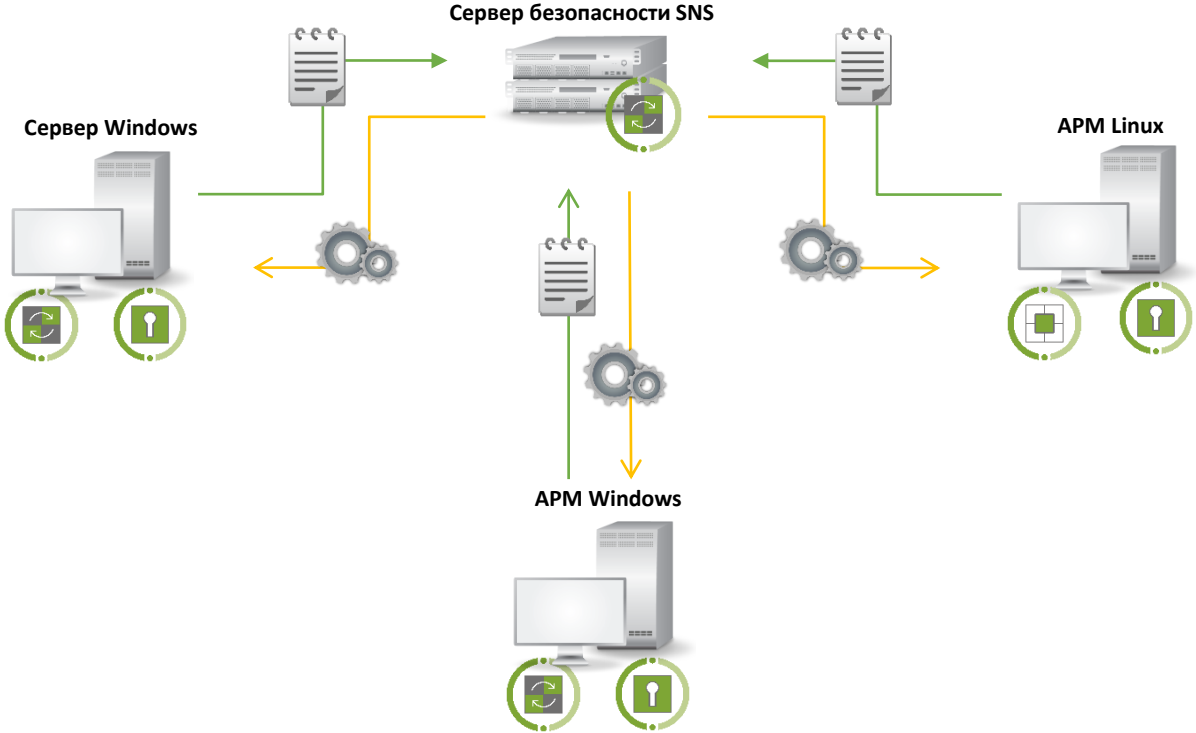
Единый идентификатор для:

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



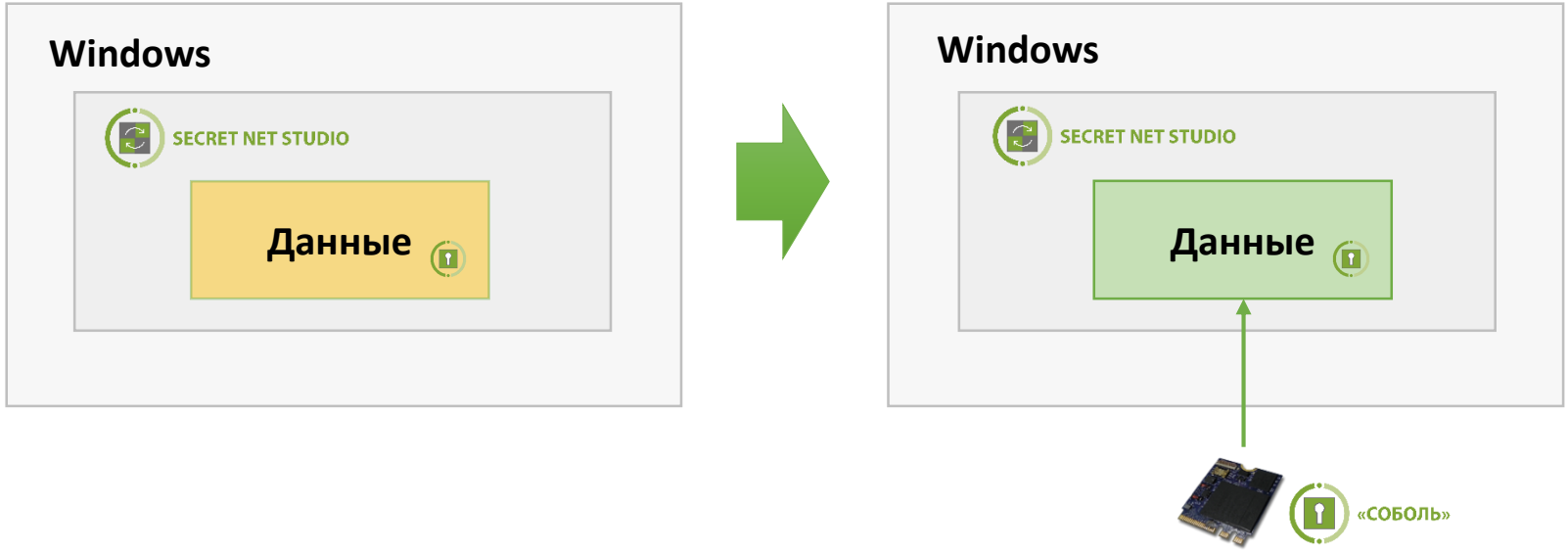
ИНТЕГРАЦИЯ С SECRET NET STUDIO И SECRET NET LSP

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



ИНТЕГРАЦИЯ С SECRET NET STUDIO 8.5

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



КОД БЕЗОПАСНОСТИ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

ВОЗМОЖНОСТИ

Усиление административных мер и снижение риска проникновения злоумышленника в систему благодаря совместной работе с идентификаторами:

iButton	USB-ключи	Смарт-карты
DS1996	JaCarta-2 ГОСТ	JaCarta-2 ГОСТ
DS1995	JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ
DS1994	JaCarta SF/ГОСТ	eToken PRO
DS1993	Рутокен Lite	eToken PRO (Java)
DS1992	Рутокен ЭЦП	Рутокен ЭЦП SC NEW
	Рутокен RF	Рутокен Lite NEW
	Рутокен	Персональная электронная карта (ПЭК) NEW
	eToken PRO	
	eToken PRO (Java)	
	Guardant ID NEW	

КОД БЕЗОПАСНОСТИ

ПРИМЕНЕНИЕ IBUTTON

СЧИТЫВАТЕЛИ

Применение идентификаторов типа iButton предполагает подключение считывателя:

Внешний считыватель

Внутренний считыватель

КОД БЕЗОПАСНОСТИ

ВСТРАИВАНИЕ В КОМПАКТНЫЕ УСТРОЙСТВА

АДАПТЕРЫ

При отсутствии в устройствах необходимых разъемов применяются адаптеры:

Адаптеры	Разъем RJ-12 (для подключения внешнего считывателя)	Разъем TM (для подключения внутреннего считывателя)	Разъем RST (для подключения кнопки Reset)	Разъем WD (для подключения сторожевого таймера)
Вариант 1 	✓	✓	✓	✓
Вариант 2 	✓			✓
Вариант 3 	✓			✓
Вариант 4 		✓		✓

КОД БЕЗОПАСНОСТИ

БЛОКИРОВКА ЗАГРУЗКИ ОС СО СЪЕМНЫХ НОСИТЕЛЕЙ

ВОЗМОЖНОСТИ

Снижение риска несанкционированного доступа к данным.

- Блокировка доступа к защищенным данным при загрузке с внешних устройств
- Запрет распространяется на всех пользователей компьютера, за исключением администратора.

КОД БЕЗОПАСНОСТИ

СТОРОЖЕВОЙ ТАЙМЕР

ВОЗМОЖНОСТИ

Предупреждение обхода комплекса злоумышленником.

Блокировка доступа к компьютеру при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано ПАК «Соболь».

КОД БЕЗОПАСНОСТИ

РЕГИСТРАЦИЯ ПОПЫТОК ДОСТУПА К ПЭВМ

ВОЗМОЖНОСТИ

Помощь в расследовании инцидентов.

Ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти.

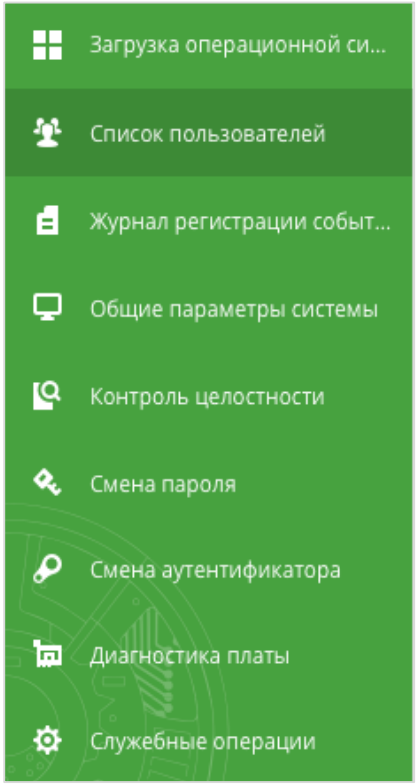
В журнал записывается:

- факт входа пользователя и имя пользователя;
- предъявление незарегистрированного идентификатора;
- ввод неправильного пароля;
- превышение числа попыток входа в систему;
- Регистрация даты и времени попыток НСД.

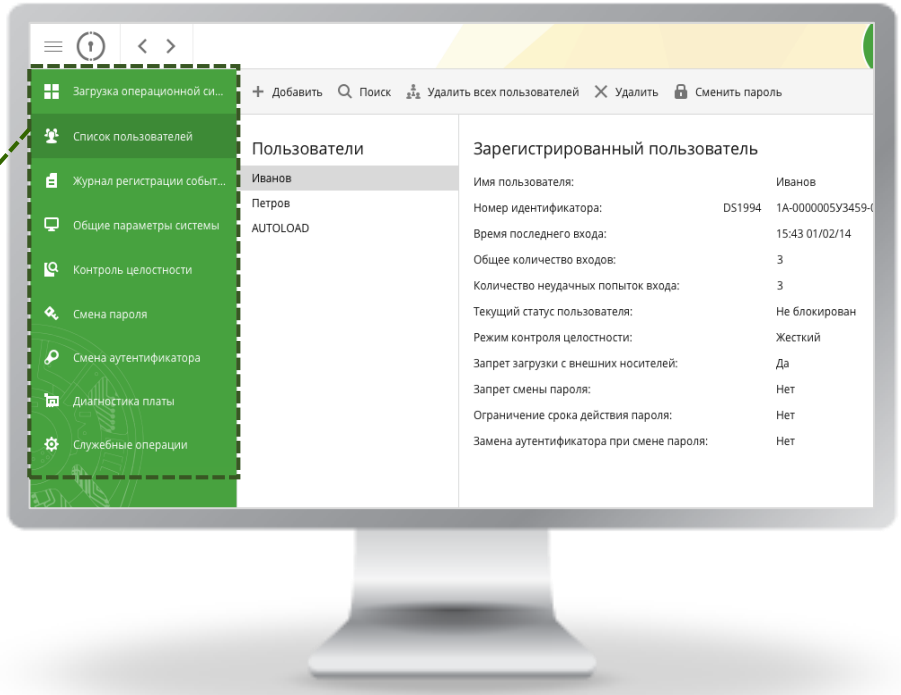
КОД БЕЗОПАСНОСТИ

НОВЫЙ ГРАФИЧЕСКИЙ ИНТЕРФЕЙС

- Преемственность логики интерфейса
- Возможность работы с мышкой



Меню



МОДЕЛЬНЫЙ РЯД

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПЛАТА PCI EXPRESS

PCI EXPRESS

Габариты: 57x 80 мм.
Интерфейс: PCI Express.
Комплект:

- Разъем RJ12 для подключения внешнего считывателя идентификатора iButton.
- Разъем для подключения внутреннего считывателя идентификатора iButton.
- Соединительный кабель для механизма сторожевого таймера.

Совместимые персональные идентификаторы:

iButton	USB-ключи	Смарт-карты
DS1996	JaCarta-2 ГОСТ	JaCarta-2 ГОСТ
DS1995	JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ
DS1994	JaCarta SF/ГОСТ	eToken PRO
DS1993	Rutoken ЭЦП	eToken PRO (Java)
DS1992	Rutoken Lite	Рутокен ЭЦП SC
	Rutoken RF	Рутокен Lite
	Rutoken	Персональная электронная карта (ПЭК)
	eToken PRO	
	eToken PRO (Java)	
	Guardant ID	

КОД БЕЗОПАСНОСТИ

ПЛАТА MINI PCI EXPRESS HALF SIZE

MINI PCI EXPRESS HALF SIZE

Габариты: 26 x 30 мм.

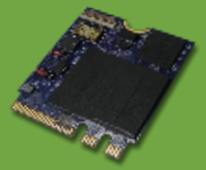
Интерфейс: Mini PCI Express.
С помощью дополнительного адаптера осуществляется подключение внутреннего или внешнего считывателя идентификаторов iButton и сторожевого таймера.

Совместимые персональные идентификаторы:

iButton	USB-ключи	Смарт-карты
DS1996	JaCarta-2 ГОСТ	JaCarta-2 ГОСТ
DS1995	JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ
DS1994	JaCarta SF/ГОСТ	eToken PRO
DS1993	Rutoken ЭЦП	eToken PRO (Java)
DS1992	Rutoken Lite	Рутокен ЭЦП SC
	Rutoken RF	Рутокен Lite
	Rutoken	Персональная электронная карта (ПЭК)
	eToken PRO	
	eToken PRO (Java)	
	Guardant ID	

КОД БЕЗОПАСНОСТИ

ПЛАТА M.2 A-E



M.2

Габариты: 30 x 22 мм.

Интерфейс: M.2 type 2230-D4-A-E.
С помощью дополнительного адаптера осуществляется подключение внутреннего или внешнего считывателя идентификаторов iButton и сторожевого таймера.

Совместимые персональные идентификаторы:

iButton	USB-ключи	Смарт-карты
DS1996	JaCarta-2 ГОСТ	JaCarta-2 ГОСТ
DS1995	JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ
DS1994	JaCarta SF/ГОСТ	eToken PRO
DS1993	Rutoken ЭЦП	eToken PRO (Java)
DS1992	Rutoken Lite	Рутокен ЭЦП SC
	Rutoken RF	Рутокен Lite
	Rutoken	Персональная электронная карта (ПЭК)
	eToken PRO	
	eToken PRO (Java)	
	Guardant ID	

КОД БЕЗОПАСНОСТИ

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ОС Windows:

- Windows 10 x64;
- Windows 8.1 x64;
- Windows 8 x64;
- Windows 7 x64 Edition;
- Windows Server 2012 R2;
- Windows Server 2016

ОС Linux:

- Astra Linux Special Edition 1.4; 1.5; 1.6;
- Astra Linux Common Edition 2.12;
- Альт Линукс СП 8; СП 8.1;
- CentOS 7.3.1611; 7.5.1804;
- ContinentOS 4.2;
- Debian 9.5;
- RHEL 6.8; 7.5;
- Oracle Linux 7.2; 7.3;
- РЕД ОС 7.1 Муром;
- SUSE Linux Enterprise 15;
- CentOS 7.3;
- Alt Linux 7.0 5 СПТ;
- Ubuntu 14.04;
- Лотос;
- ESXi 6 up2; 6.5a

Файловые системы: NTFS, FAT 16, FAT 32, EXT2, EXT3, EXT4

РЕЗЮМЕ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПРЕИМУЩЕСТВА ПАК «СОБОЛЬ»

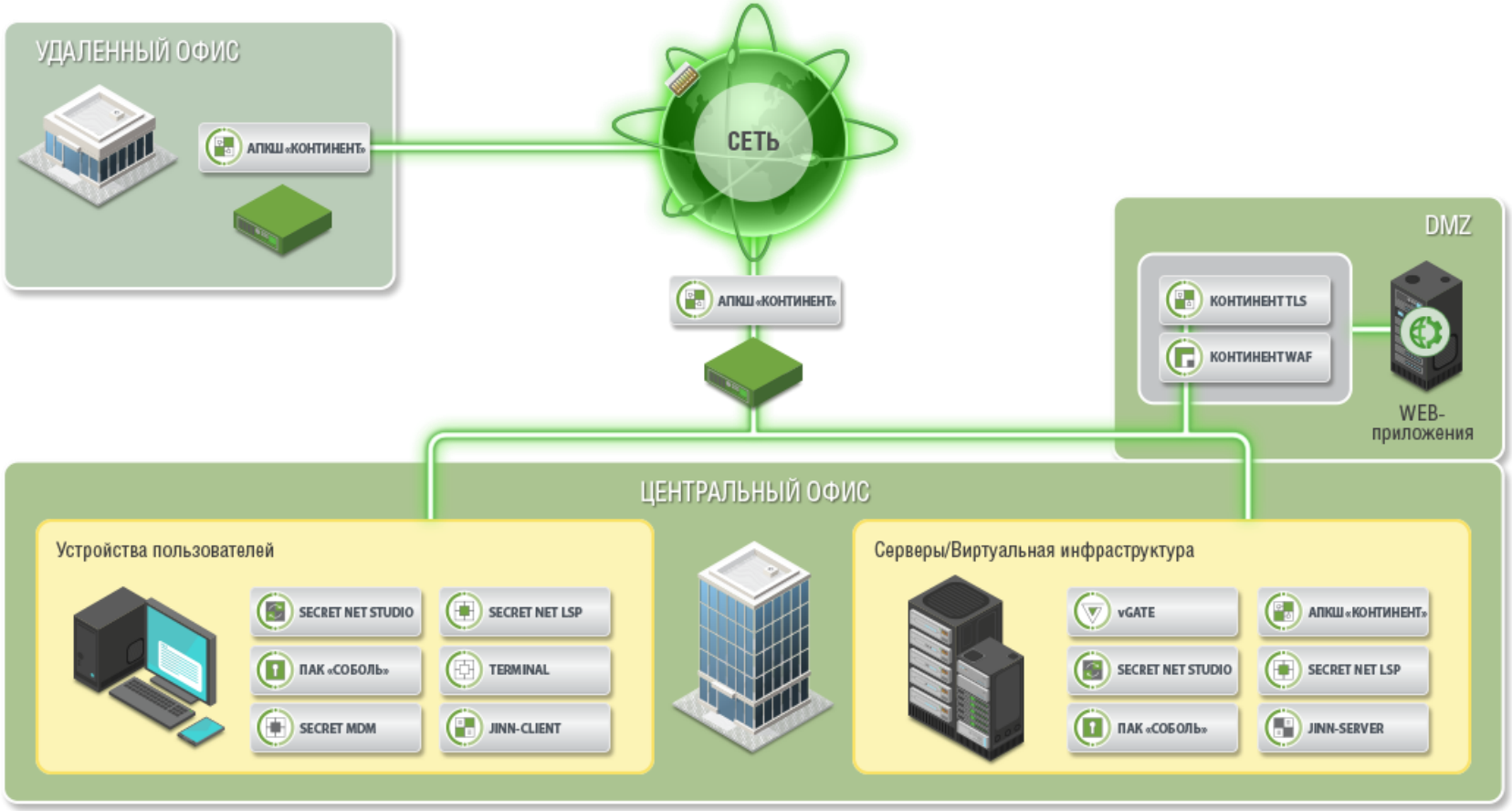
- Поддержка современных форматов плат с UEFI
- Интеграция с Secret Net Studio 8.5 и Secret Net LSP 1.9
- Простота установки, настройки и администрирования
- Возможность программной инициализации без вскрытия системного блока
- Аппаратный датчик случайных чисел
- Поддержка современных USB-токенов (USB 3.0) и смарт-карт

О КОМПАНИИ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ИНФРАСТРУКТУРЫ



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 1000 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

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!

Бурым Андрей

КОНТАКТЫ:

+7 (495) 982-30-20

info@securitycode.ru

www.securitycode.ru

КОД БЕЗОПАСНОСТИ