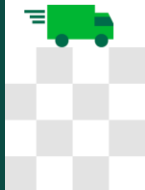




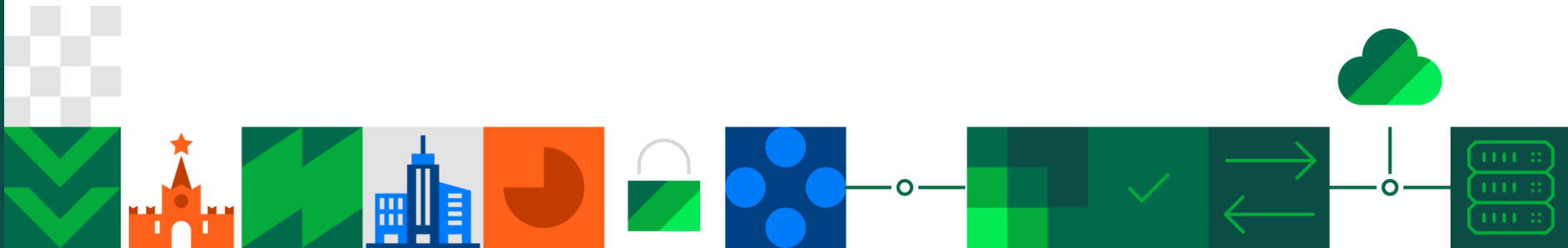
Соболь

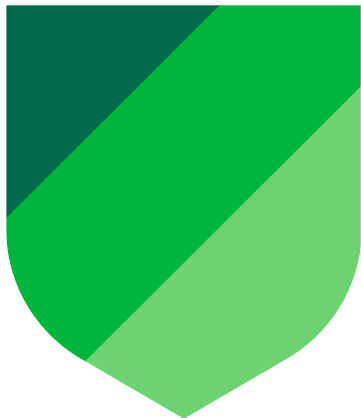
Версия 4.4





О продукте



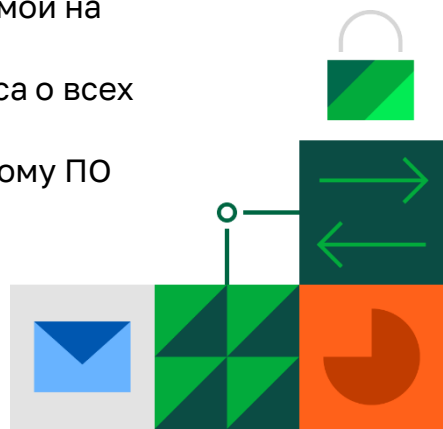


Соболь

Программный модуль доверенной загрузки, функционирующий в среде UEFI

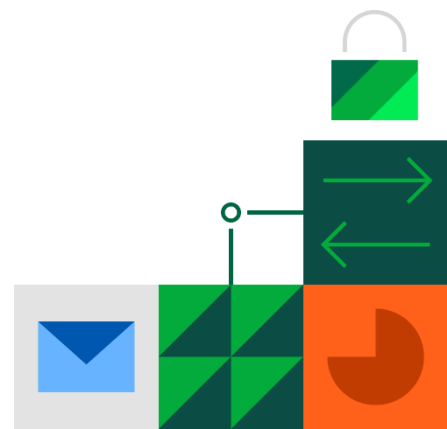
Предназначен для решения следующих задач:

- ✓ 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



ФСТЭК России:

- Средство доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты (СДЗ.УБ 2)
- 2 уровень доверия средств обеспечения безопасности (УД 2)



Контроль целостности системы осуществляется внутри ОС, поэтому при её взломе возможны:



отключение/обход программных СЗИ,



внесение изменений в реестр Windows,



скрытие действий злоумышленника.

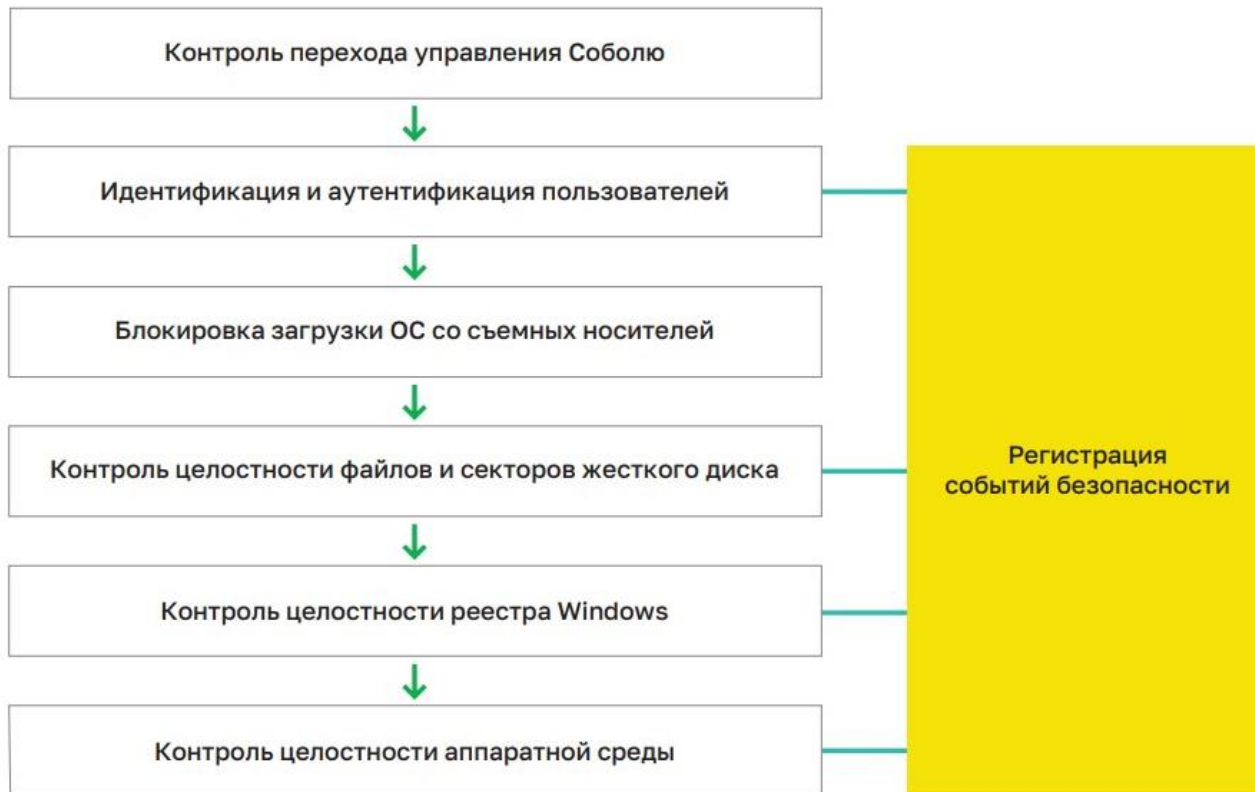
Требуется дополнительный контроль целостности до загрузки ОС.

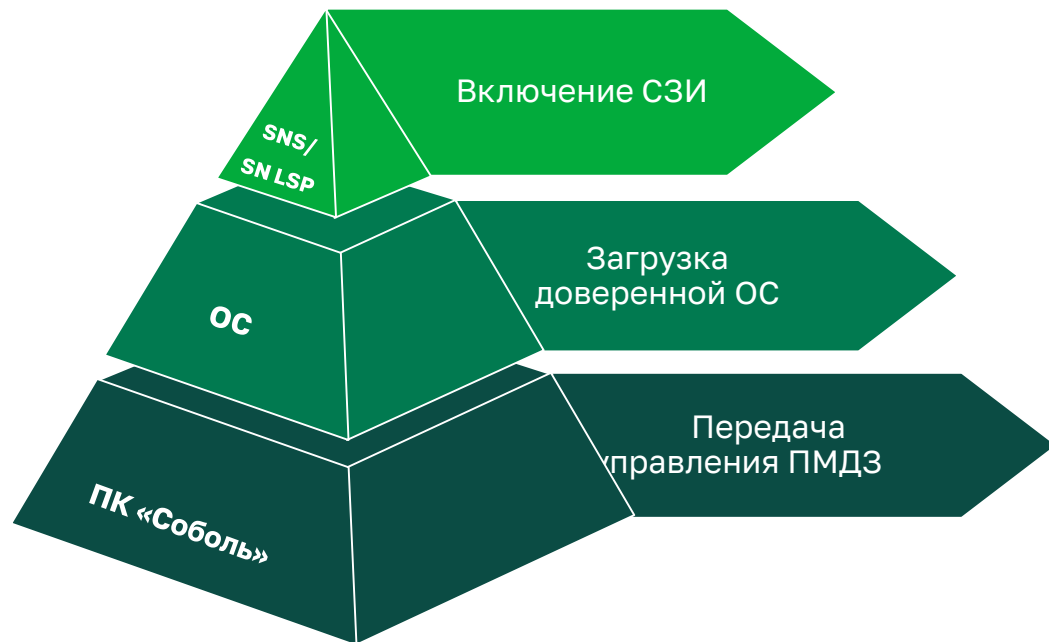
Другие средства доверенной загрузки

- Ограниченный выбор устройств, подходящих для обработки конфиденциальной информации и гостайны
- После сбоя ОС необходимо проводить вскрытие системного блока для переинициализации АПМДЗ или загрузки с внешнего устройства
- Расчёт контрольных сумм на ресурсах АПМДЗ замедляет загрузку компьютера

Соболь 4

- Поддержка современных устройств с UEFI
- Контроль целостности файлов и ключей реестра Windows
- Недоступность системы для неавторизованных пользователей и недоверенных устройств
- Блокировка доступа к компьютеру при несанкционированном изменении файлов
- Интеграция с Secret Net Studio/LSP обеспечивает комплексный подход к защите

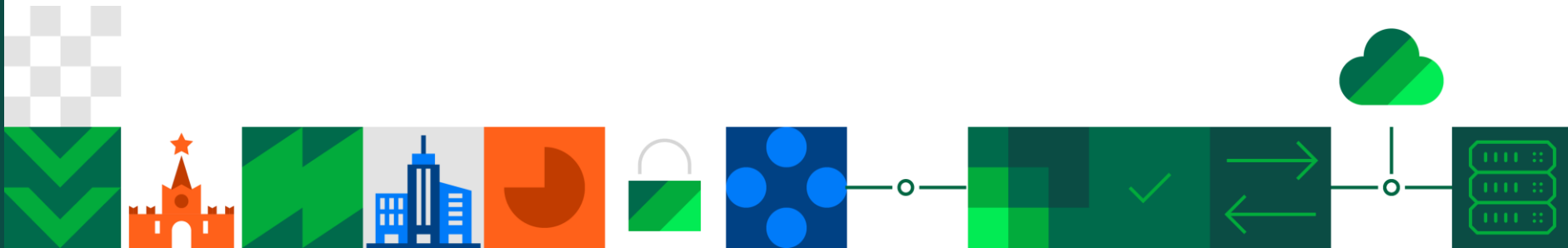




- Защита серверов или рабочих станций от атаки до загрузки ОС
- Интеграция с средствами защиты Secret Net Studio и Secret Net LSP
- Использование единого персонального идентификатора
- Блокировка несанкционированной загрузки ОС со съемных носителей



Возможности



Функционал Соболя



Контроль целостности аппаратной
конфигурации компьютера



Контроль целостности
файлов до загрузки ОС



Контроль целостности
реестра Windows

Результат использования



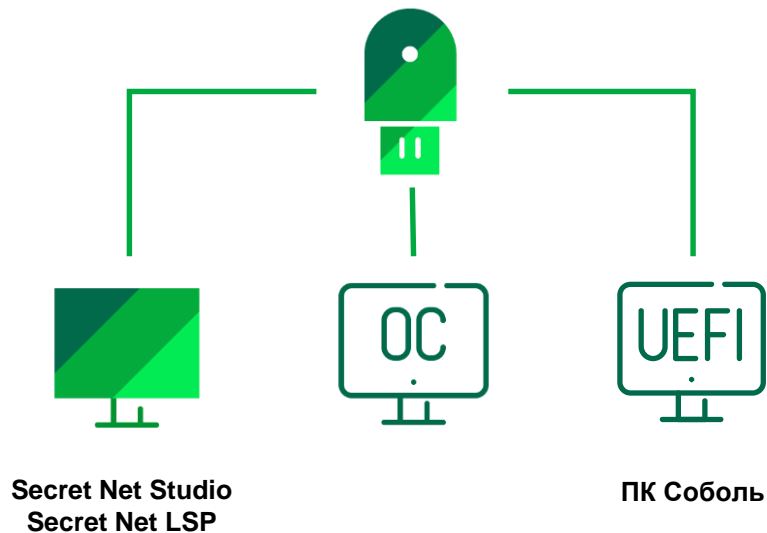
Обнаружение действий
продвинутого злоумышленника



Быстрая реакция на
инцидент безопасности

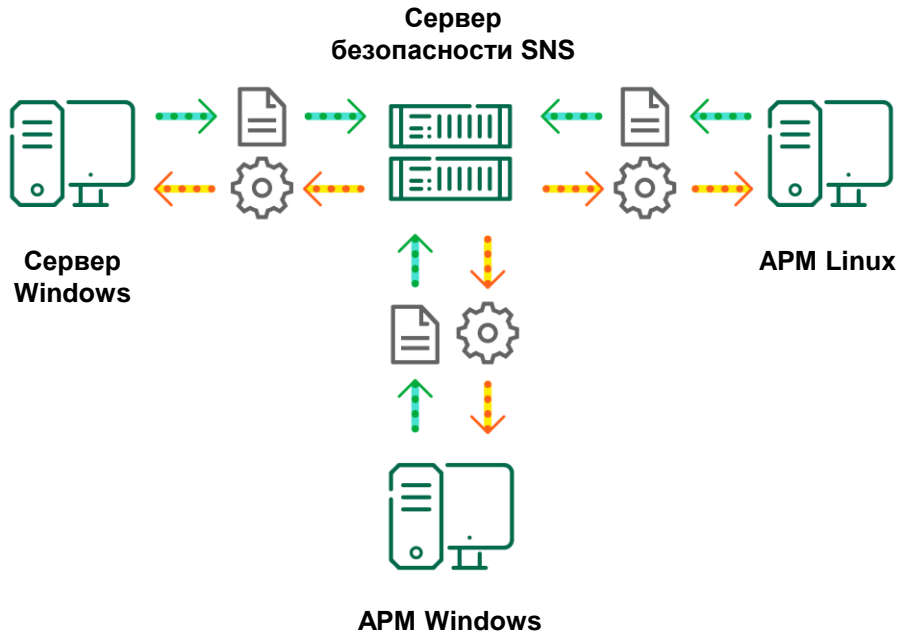


Сокращение ресурсов
на ликвидацию



Единый идентификатор для:

- Соболь
- Secret Net Studio/Secret Net LSP
- Входа в ОС
- Электронной подписи



- **Единые** политики безопасности
- **Единый** журнал событий безопасности

Windows



Secret Net
Studio

Данные



Windows



Secret Net
Studio

Данные



- **Усиление** контроля целостности на рабочих станциях и серверах
- **Совместное использование** с полнодисковым шифрованием

iButton	USB- ключи	Смарт-карты
DS1992	eToken: PRO, PRO (Java)	eToken: PRO, PRO (Java)
DS1993	vdToken	ESMART Token 64k
DS1994	ESMART Token 64k	JaCarta-2: ГОСТ, PKI/ГОСТ, PRO/ГОСТ
DS1995	JaCarta-2: ГОСТ, PKI/ГОСТ, PRO/ГОСТ	JaCarta: PKI, PRO
DS1996	JaCarta: SF/ГОСТ, PKI, PRO, PRO/ГОСТ	Рутокен: Lite (SC), ЭЦП 2.0, ЭЦП (SC), 2151
	Рутокен: S (RF), 2151 (RF), Lite (RF), ЭЦП 2.0 (RF), ЭЦП 2.0 2100 (RF)	ПЭК
	Guardant-ID	
	Форос R301	



Внешний считыватель



Внутренний считыватель

Блокировка загрузки ОС со съемных носителей

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

Снижение риска несанкционированного доступа к данным

Сторожевой таймер

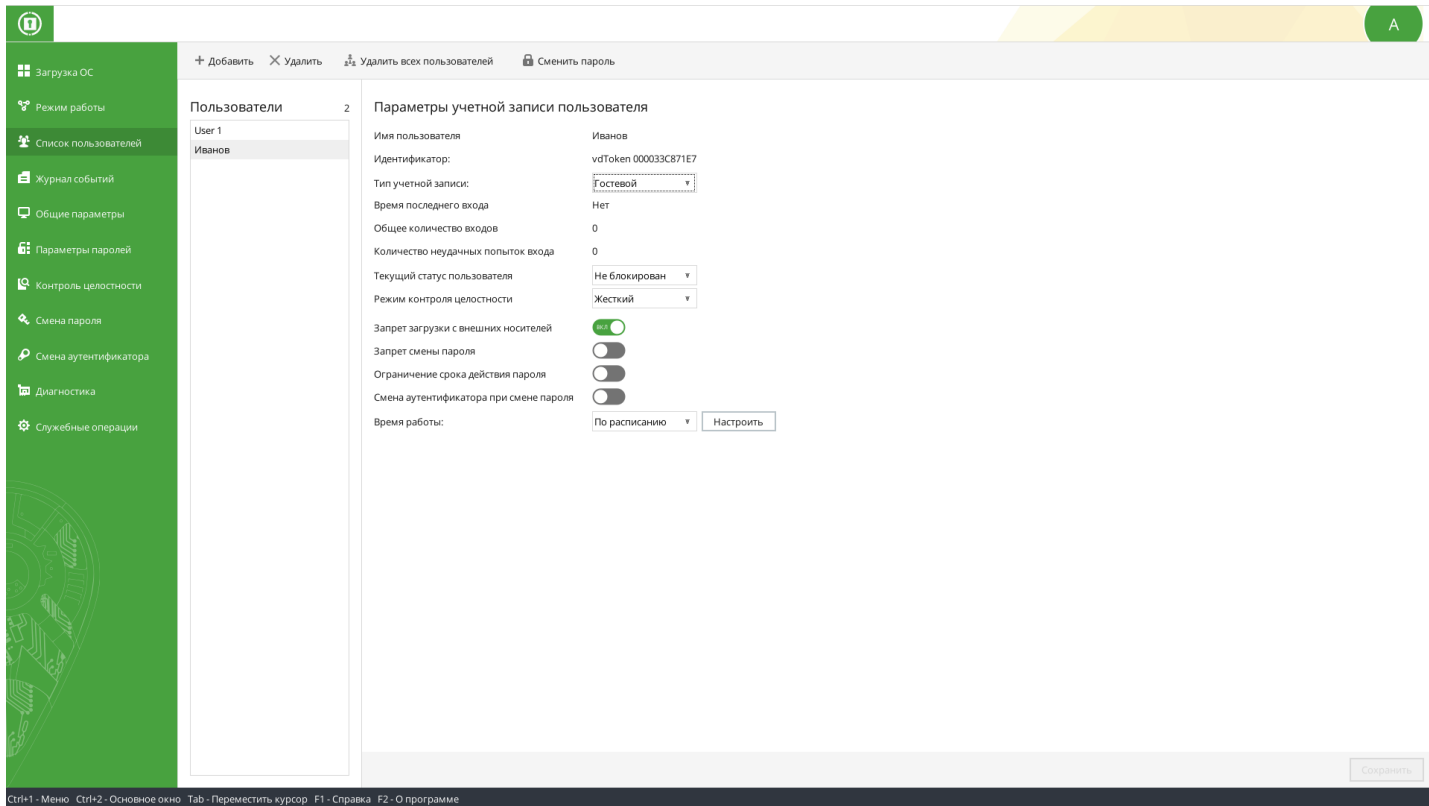
- Блокировка доступа к устройству при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано ПК «Соболь»

Предупреждение обхода комплекса злоумышленником

Системный журнал в энергонезависимой памяти

- Факт входа и имя пользователя
- Предъявление незарегистрированного идентификатора
- Ввод неправильного пароля
- Превышение числа попыток входа в систему
- Дата и время попыток НСД

Помощь в расследовании инцидентов



The screenshot shows a web-based user management interface. On the left is a green sidebar with navigation items: Загрузка ОС, Режим работы, Список пользователей, Журнал событий, Общие параметры, Параметры паролей, Контроль целостности, Смена пароля, Смена аутентификатора, Диагностика, and Служебные операции. The main area is divided into two panels. The left panel, titled 'Пользователи', shows a list with 'User 1' and 'Иванов'. The right panel, titled 'Параметры учетной записи пользователя', shows settings for 'Иванов', including fields for name, identifier, account type (Guest), last login time, failed login attempts, user status (Not blocked), and integrity control mode (Strict). There are also toggle switches for password change restrictions and a 'Настроить' button. A 'Сохранить' button is at the bottom right. A top navigation bar contains '+ Добавить', 'X Удалить', 'Удалить всех пользователей', and 'Сменить пароль'. A small 'A' icon is in the top right corner. At the bottom, a keyboard shortcut legend is visible: Ctrl+F1 - Меню, Ctrl+F2 - Основное окно, Tab - Переместить курсор, F1 - Справка, F2 - О программе.

Пользователи 2

Параметры учетной записи пользователя

Имя пользователя: Иванов

Идентификатор: vdToken 000033C871E7

Тип учетной записи: Гостевой

Время последнего входа: Нет

Общее количество входов: 0

Количество неудачных попыток входа: 0

Текущий статус пользователя: Не блокирован

Режим контроля целостности: Жесткий

Запрет загрузки с внешних носителей:

Запрет смены пароля:

Ограничение срока действия пароля:

Смена аутентификатора при смене пароля:

Время работы: По расписанию

Ctrl+F1 - Меню Ctrl+F2 - Основное окно Tab - Переместить курсор F1 - Справка F2 - О программе