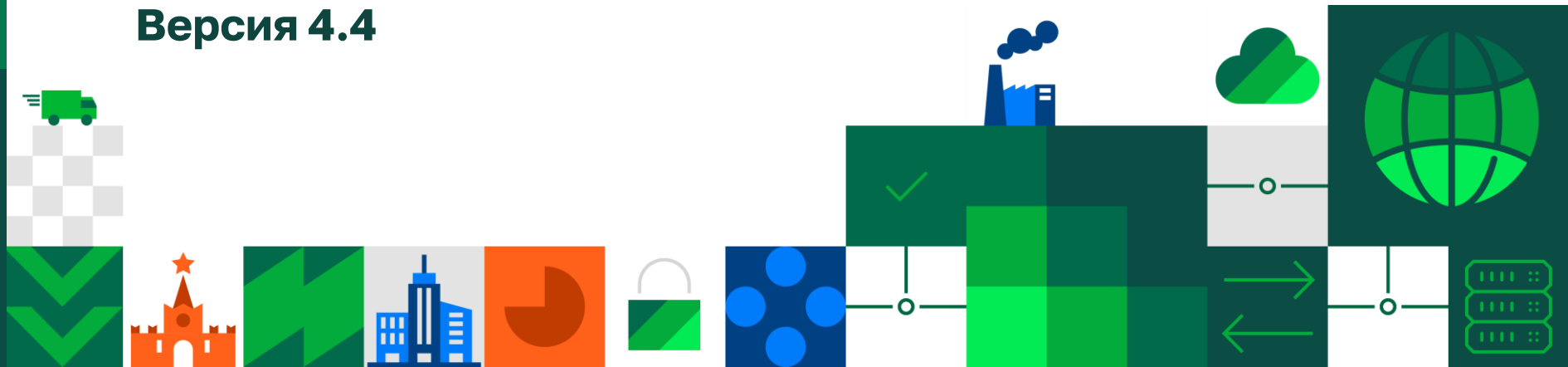
КОД безопасности

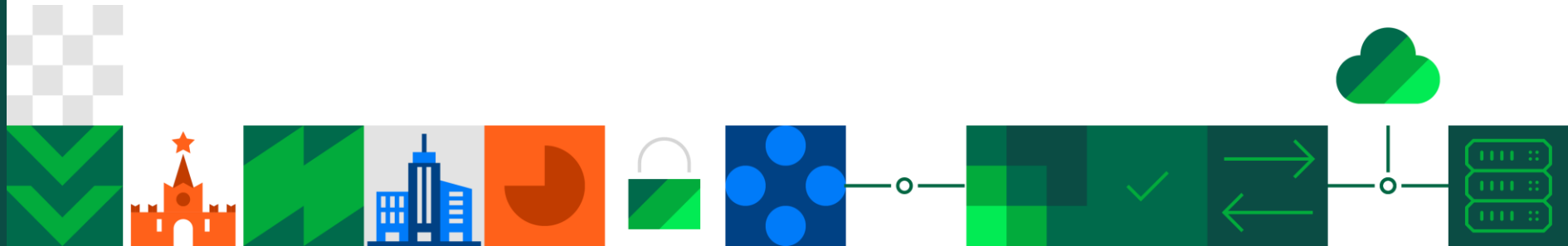
Соболь

Версия 4.4



КОД безопасности

О продукте



КОД безопасности

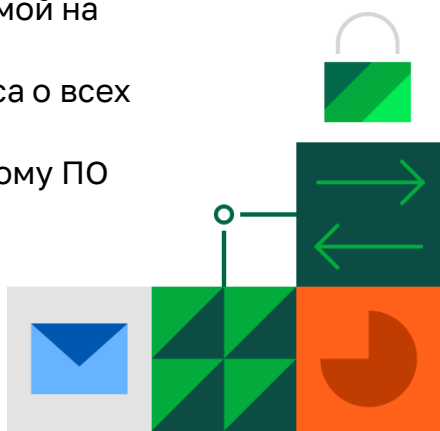
О продукте

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

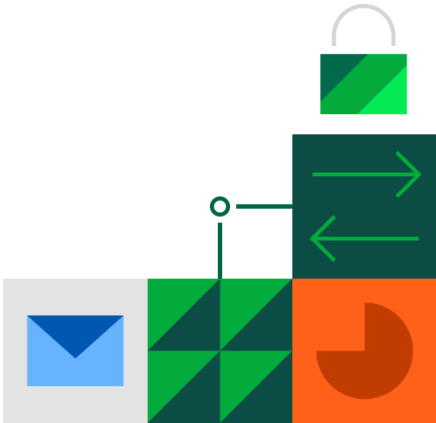


КОД безопасности

Сертификация

ФСТЭК России:

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



КОД безопасности

Риски при защите конечных устройств программными СЗИ

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.

КОД безопасности

Проблемы и решения

Другие средства доверенной загрузки

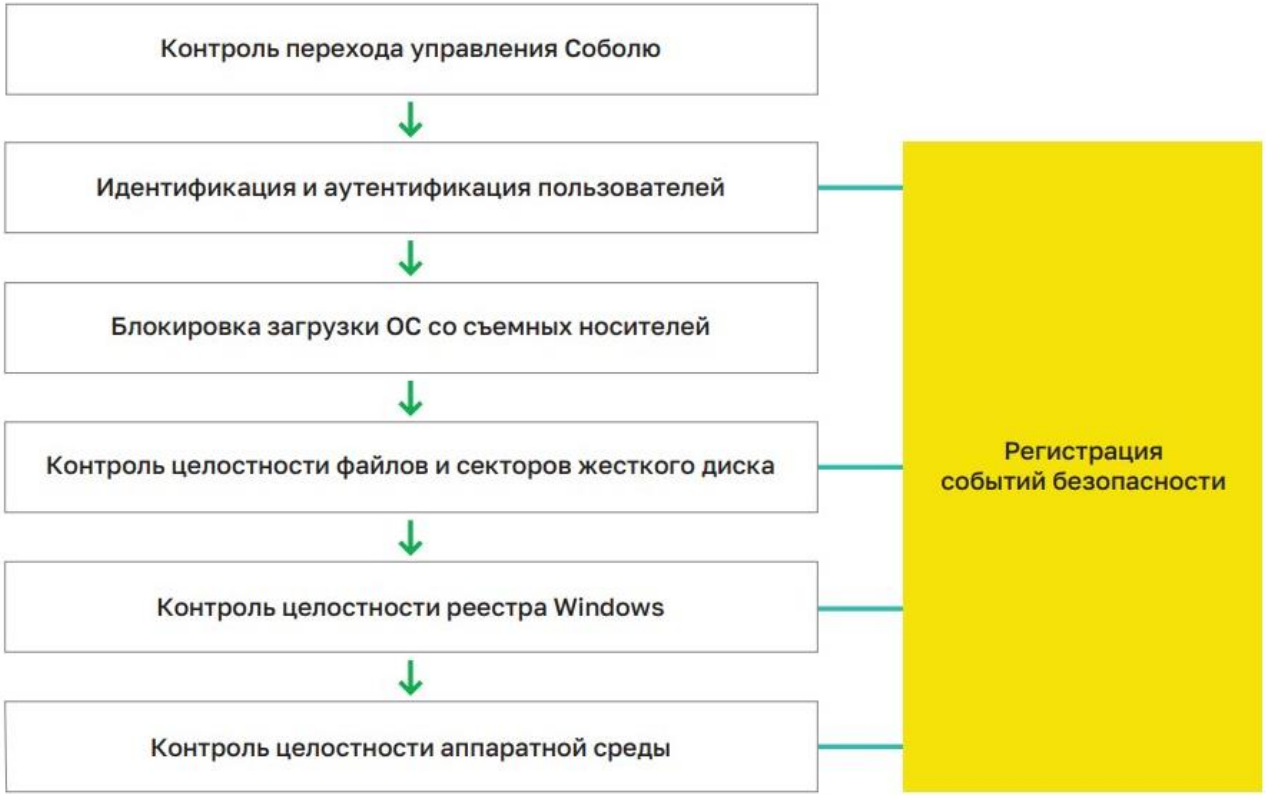
- Ограниченный выбор устройств, подходящих для обработки конфиденциальной информации и гостайны
- После сбоя ОС необходимо проводить вскрытие системного блока для переинициализации АПМДЗ или загрузки с внешнего устройства
- Расчёт контрольных сумм на ресурсах АПМДЗ замедляет загрузку компьютера

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

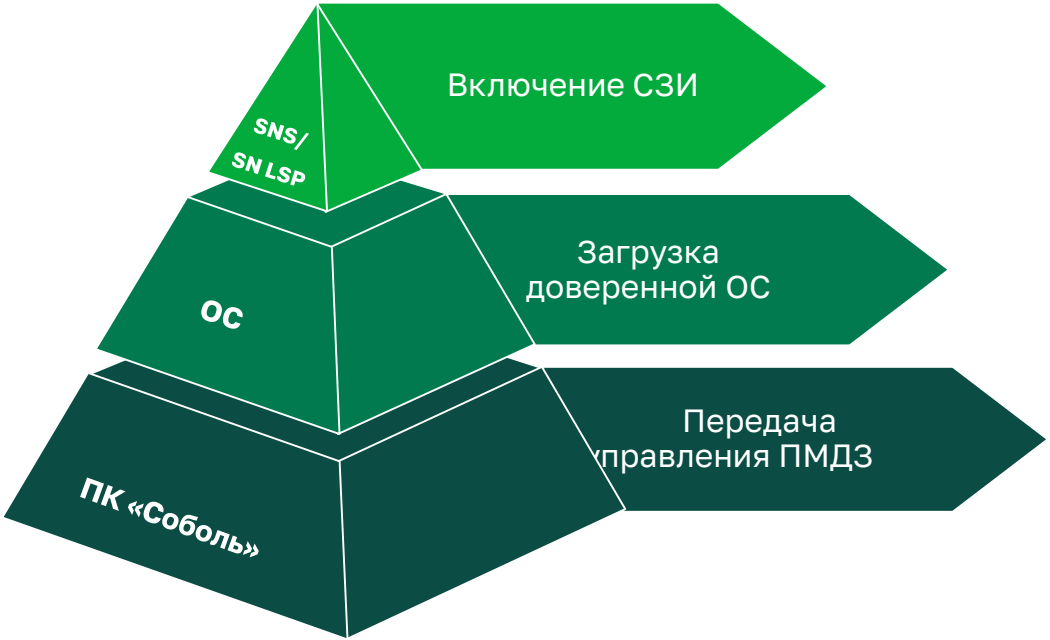
КОД безопасности

Принцип работы



КОД безопасности

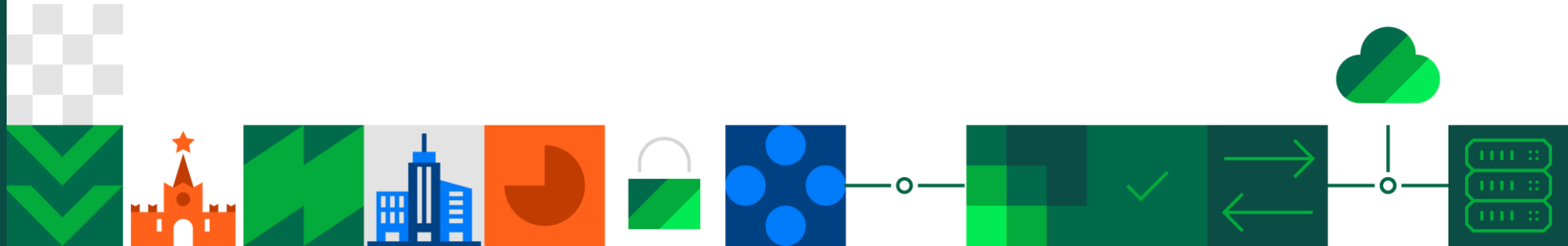
Усиление механизма обнаружения атак



- 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

КОД безопасности

Возможности



КОД безопасности

Контроль целостности

Функционал Соболя

Контроль целостности аппаратной конфигурации компьютера

Контроль целостности файлов до загрузки ОС

Контроль целостности реестра Windows

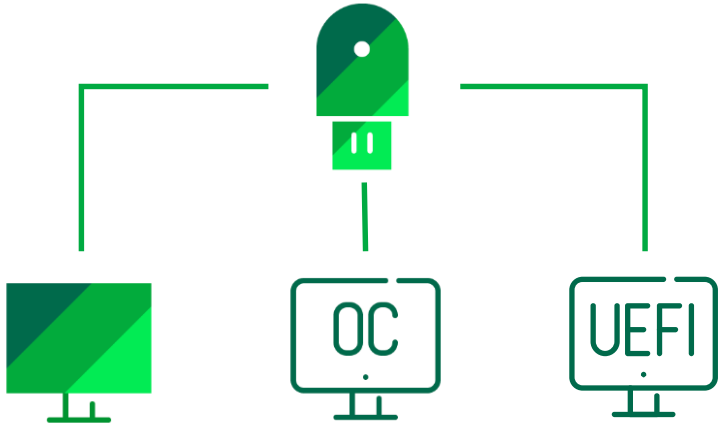
Результат использования

Обнаружение действий продвинутого злоумышленника

Быстрая реакция на инцидент безопасности

Сокращение ресурсов на ликвидацию

Интеграция с SNS и SN LSP



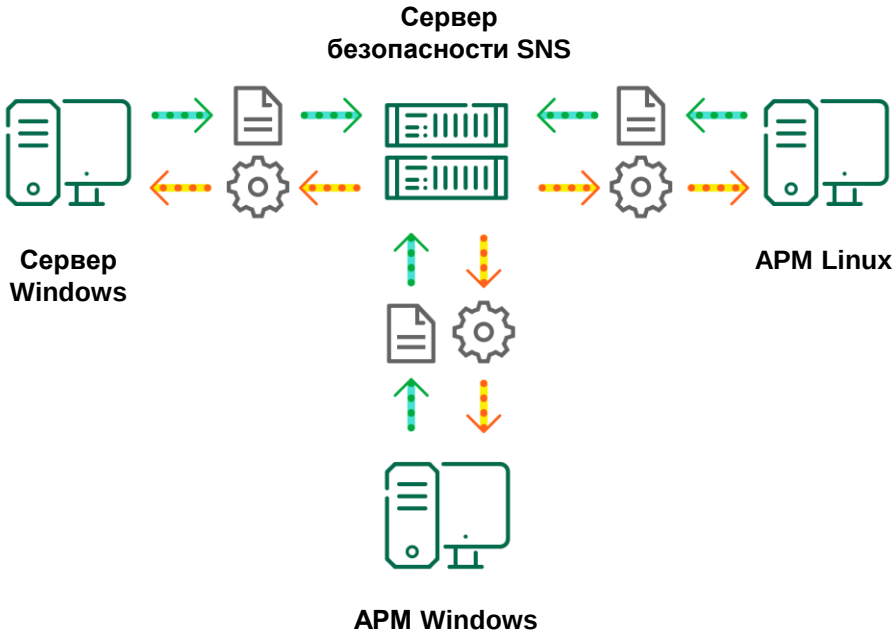
Secret Net Studio
Secret Net LSP

ПК Соболь

Единый идентификатор для:

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

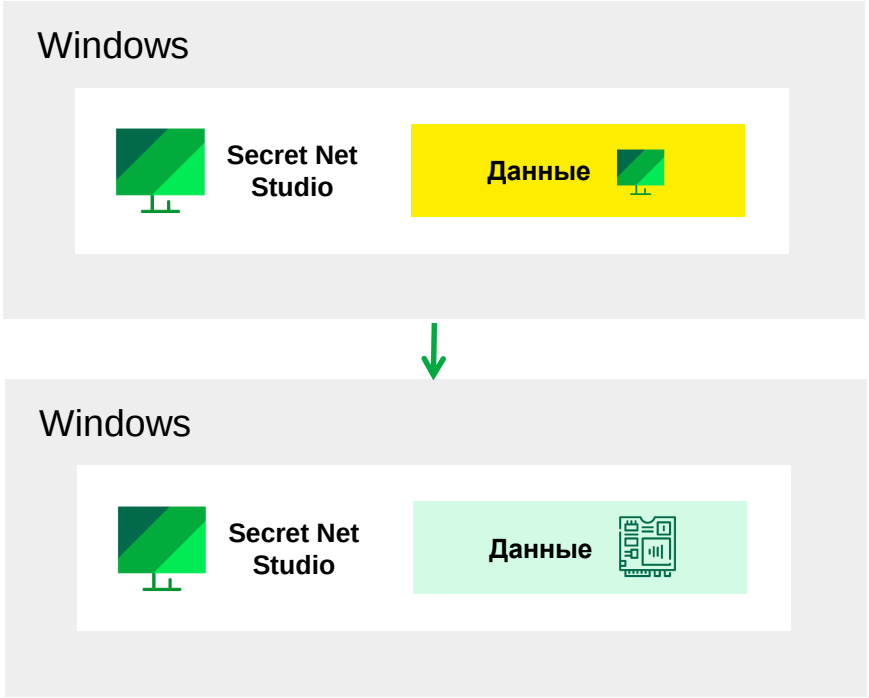
Интеграция с SNS и SN LSP



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

КОД безопасности

Интеграция с SNS



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

КОД безопасности

Идентификация и аутентификация

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	

КОД безопасности

Применение iButton

Внешний считыватель

Внутренний считыватель

КОД безопасности

Компоненты защиты

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

КОД безопасности

Графический интерфейс