КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6 декабря 2018 г.
Астана

ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ ПРОДУКТОВОЙ ЛИНЕЙКИ DALLAS LOCK

#CODEIB

СЕРГЕЙ КУЗНЕЦОВ
Коммерческий директор ЦЗИ ГК «Конфидент»
WEB: WWW.DALLASLOCK.RU
EMAIL: ISC@CONFIDENT.RU

DALLAS LOCK

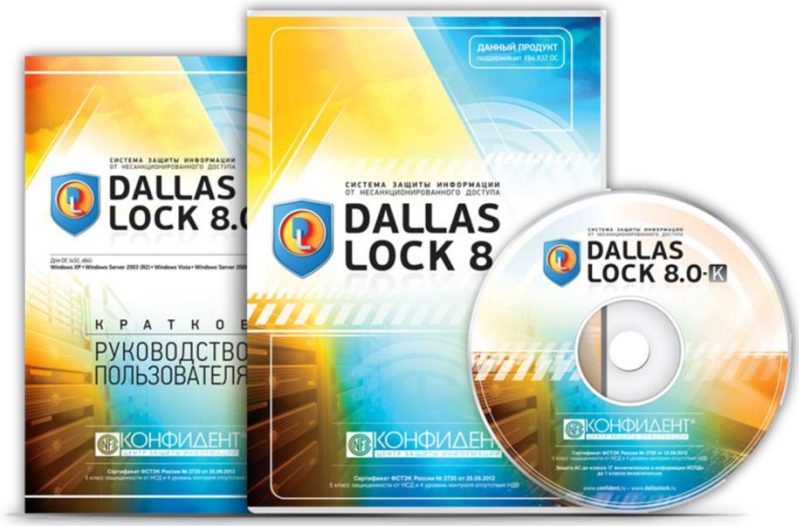
КОНФИДЕНТ® ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Кратко о ГК «Конфидент»

Более 25 лет на рынке средств защиты информации

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кратко о продуктовой линейке DALLAS LOCK



> 4500

проектов ежегодно реализуется в России с использованием продуктов Dallas Lock

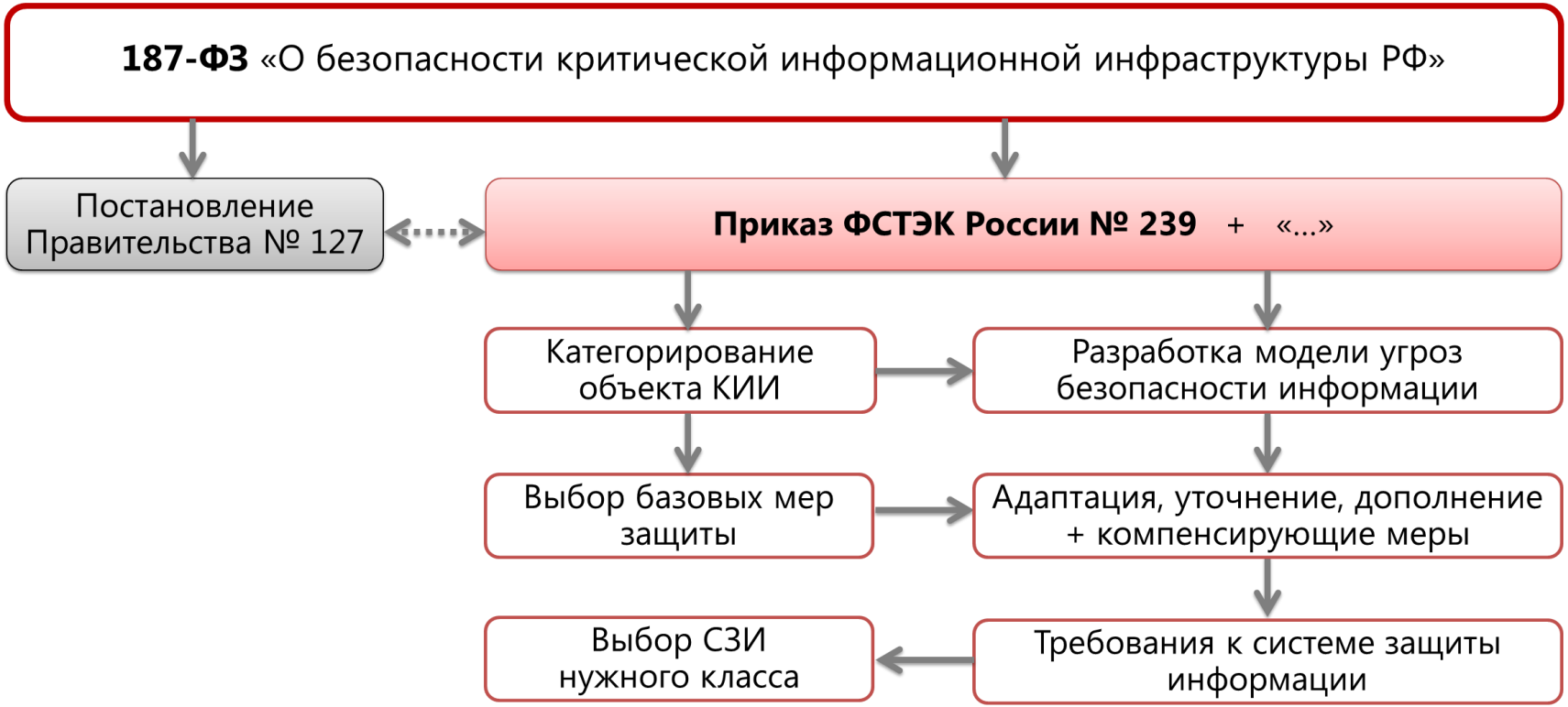
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита ГИС в России

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита КИИ в России



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кем проверяются СЗИ в России?

- Разработчик
- Испытательная лаборатория
- Орган по сертификации
- ФСТЭК России
- Орган по аттестации
- Оператор
- ФСТЭК России

сертифицированные СЗИ

- Разработчик
- Оператор

не сертифицированные СЗИ

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock

СРЕДСТВО ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

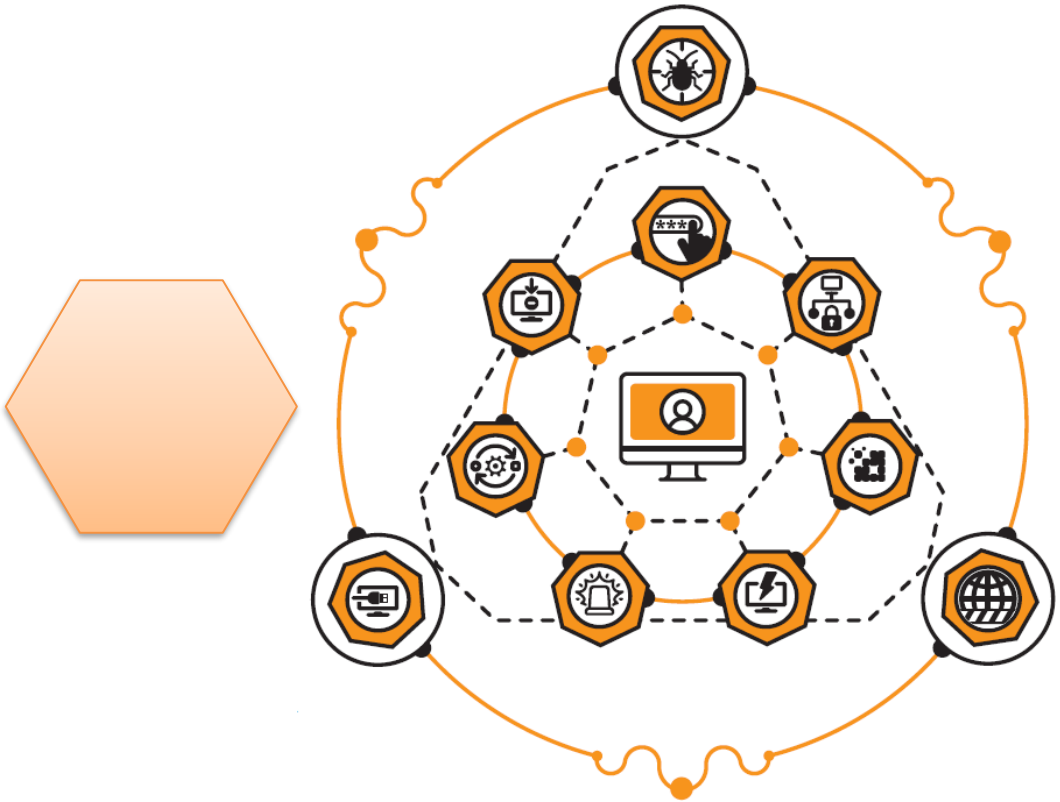
СРЕДСТВО КОНТРОЛЯ СЪЁМНЫХ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

ПЕРСОНАЛЬНЫЙ МЕЖСЕТЕВОЙ ЭКРАН

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Продуктовая линейка Dallas Lock



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

Dallas Lock имеет множество функций, которые не укладываются в традиционное восприятие СЗИ от НСД

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

Дополнение антивируса

- Контроль целостности объектов файловой системы.
- Персональный межсетевой экран и система обнаружения и предотвращения вторжений блокируют вредоносные программы, которые могут попасть по сети.
- Преобразование информации.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

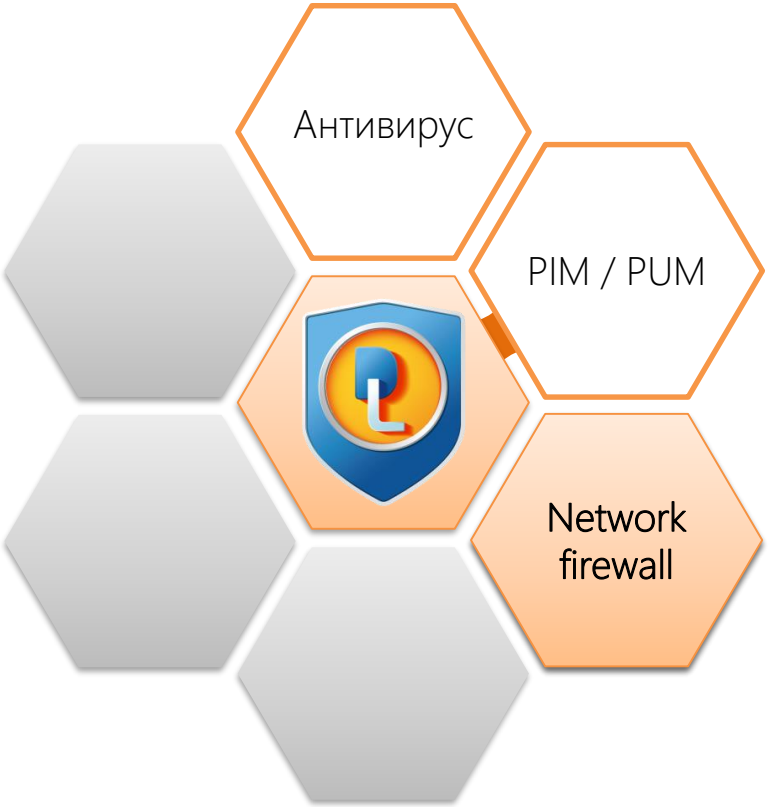
Дополнение систем класса PIM / PUM

В СЗИ Dallas Lock реализовано управление привилегированными пользователями (Privileged Identity Management, Privileged User Management):

- Пользователи с административными правами не имеют возможности деактивировать защиту (только суперадминистратор).
- На каждый Домен безопасности назначается свой администратор ИБ.
- Гибкое разграничение прав, включая ролевую модель Сервера безопасности.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

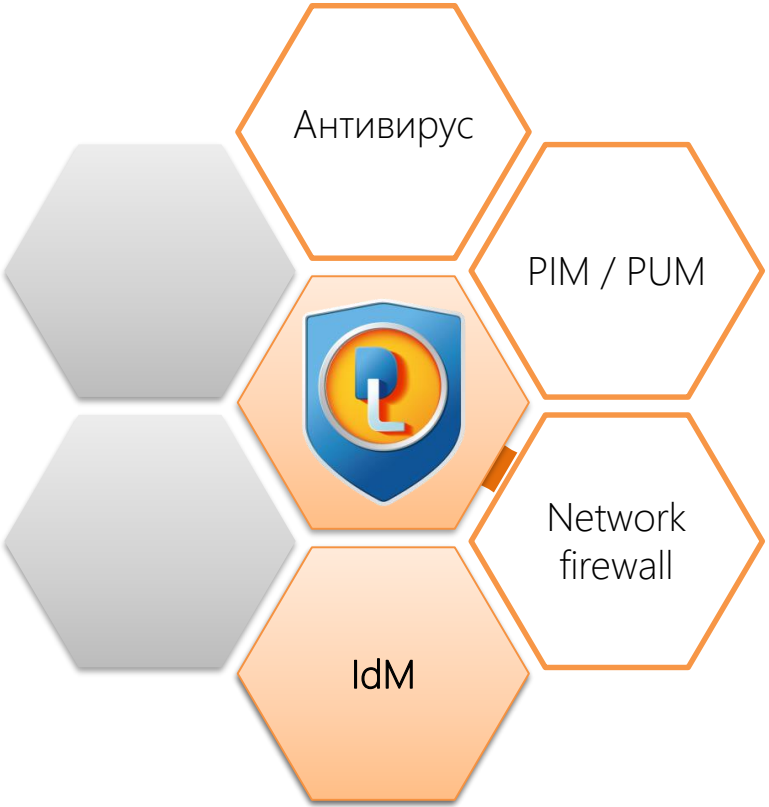


Дополнение МЭ уровня сети

- Персональный межсетевой экран и система обнаружения и предотвращения вторжений защищают от атак, источник которых находится внутри сети предприятия.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений



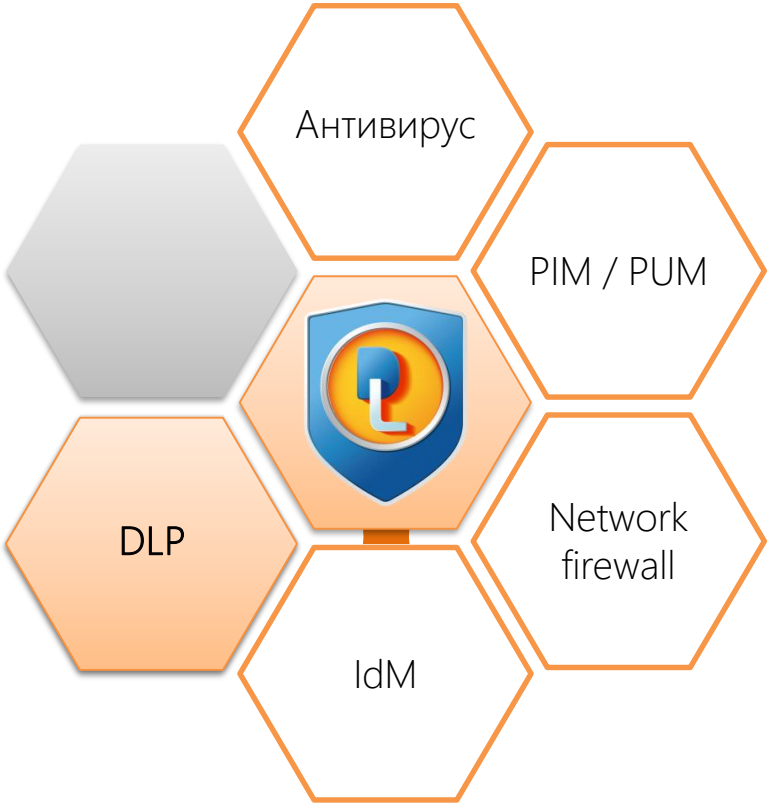
Дополнение систем класса IdM

- Управление пользователями происходит из единой консоли Сервера безопасности, включая управление доменными пользователями, группами и политиками. Именно поэтому нет необходимости использовать стандартную оснастку Active Directory.
- Не санкционированно созданные ИТ-адмиистраторами пользователи не получают прав на доступ к защищённым АРМ.

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

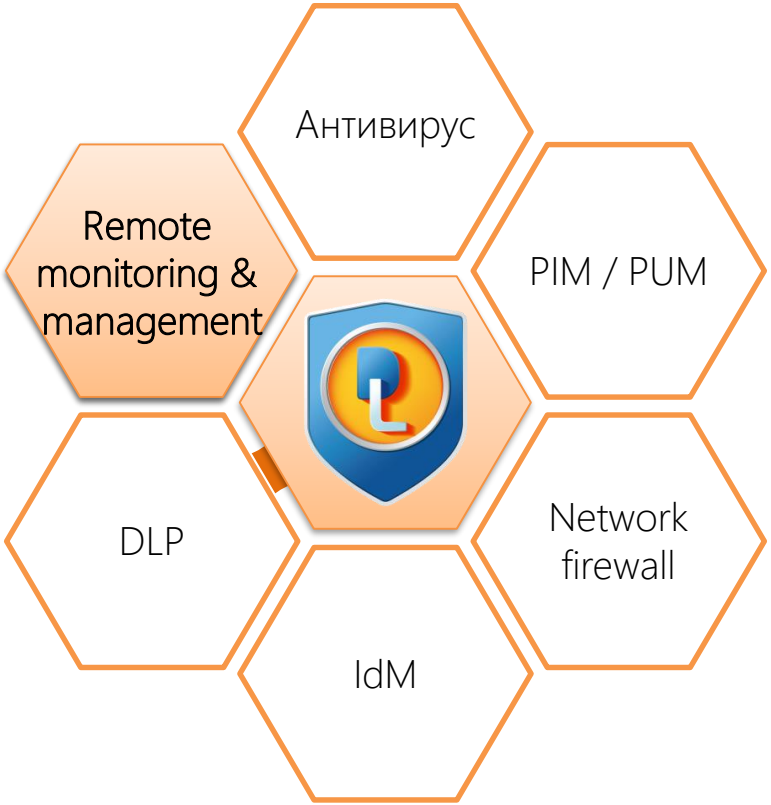


Дополнение систем класса DLP

- Контроль съёмных машинных носителей информации.
- Создание доверенной среды для контроля отчуждения (переноса) информации.
- Теневое копирование.
- Контроль доступа к отдельным программам и сетевой карте.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений

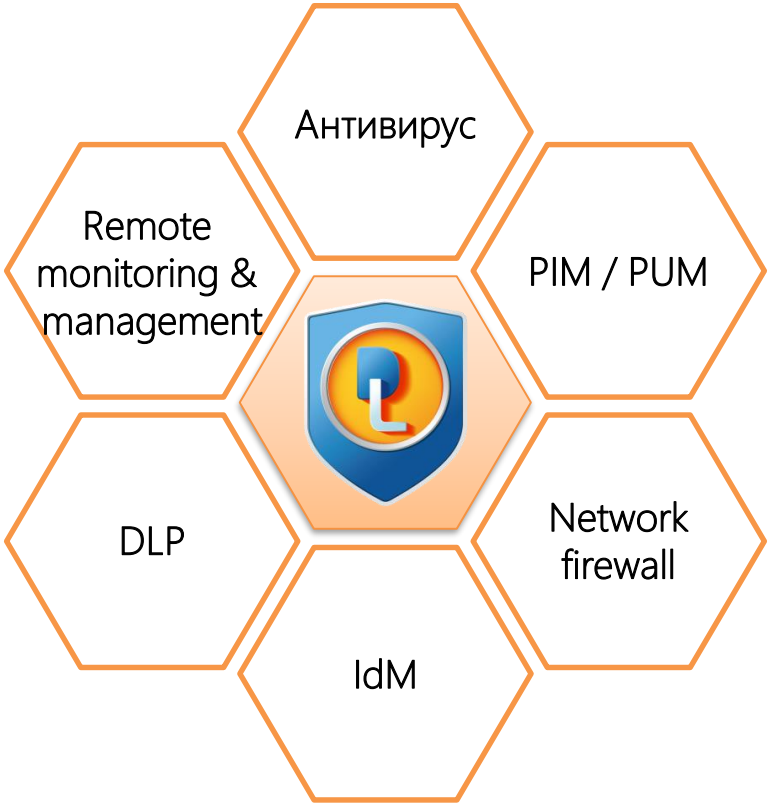


Централизованное управление

- Централизованное развёртывание системы защиты.
- Все модули и защитные механизмы имеют развитые функции централизованного управления (включая аппаратные средства доверенной загрузки).
- Консоль Сервера безопасности имеет панель мониторинга и гибкие инструменты для быстрого расследования инцидентов информационной безопасности.
- Сервер конфигураций отслеживает состав программ на защищаемых АРМ.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнение других решений



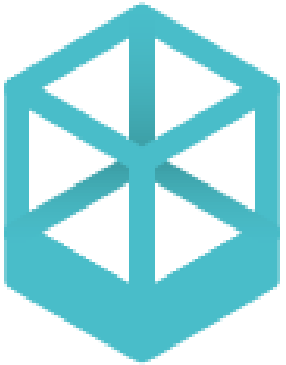
#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Технологии и функции

Управление контролем целостности

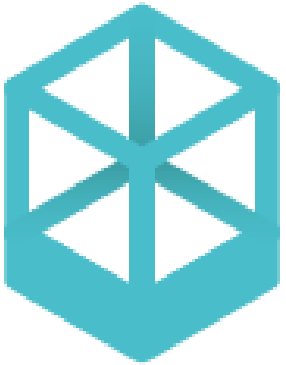
Контроль переноса информации



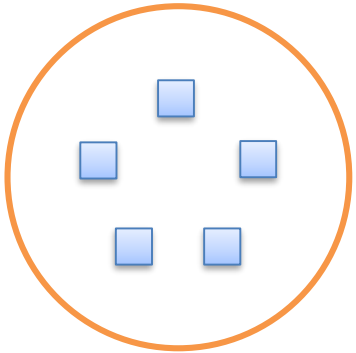
Безопасная среда («песочница»)

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Технологии и функции



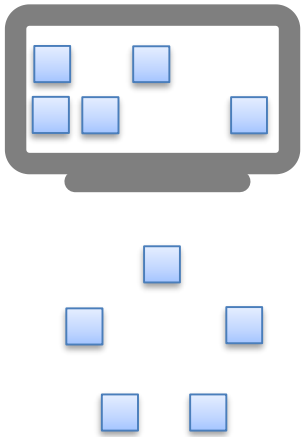
Централизованное управление контролем целостности



Необходимо контролировать целостность объектов (ресурсов): файлы, «ветки» реестра, программно-аппаратная среда

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

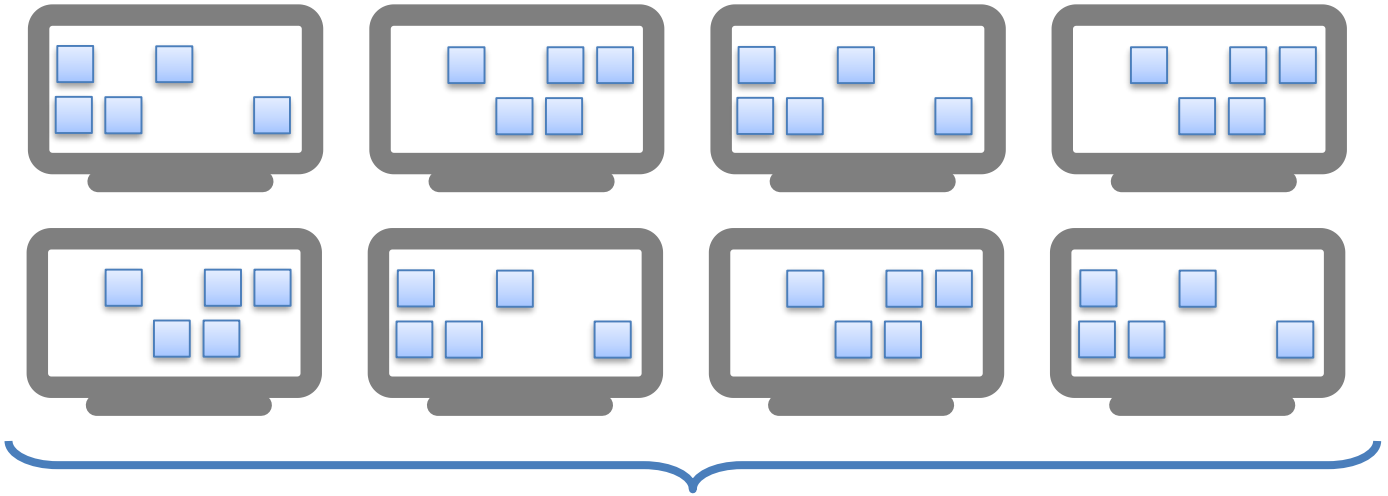
Контроль целостности



Объекты хранятся «где-то»
на компьютере

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль целостности



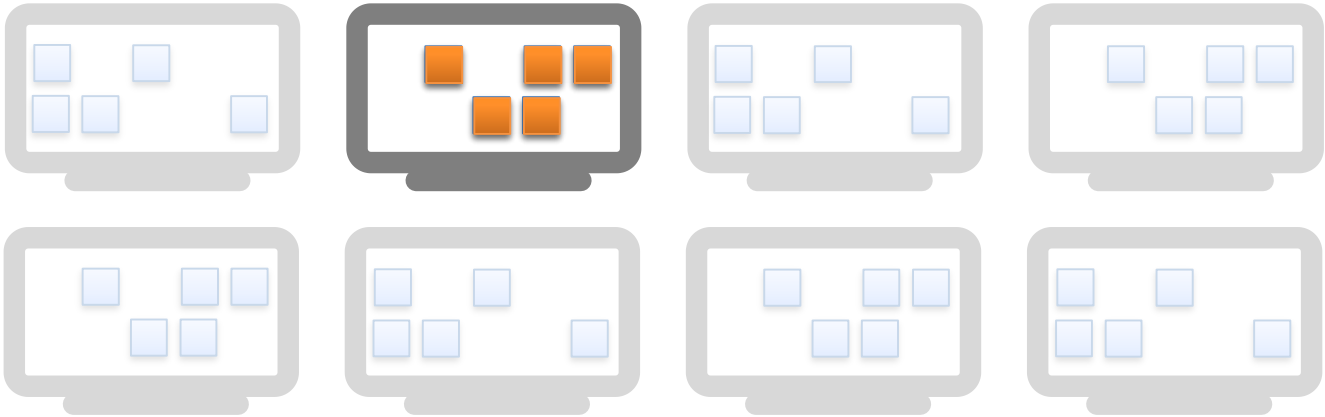
Компьютеров много и они разные (x32, x64), а объекты размещаются в разных местах



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

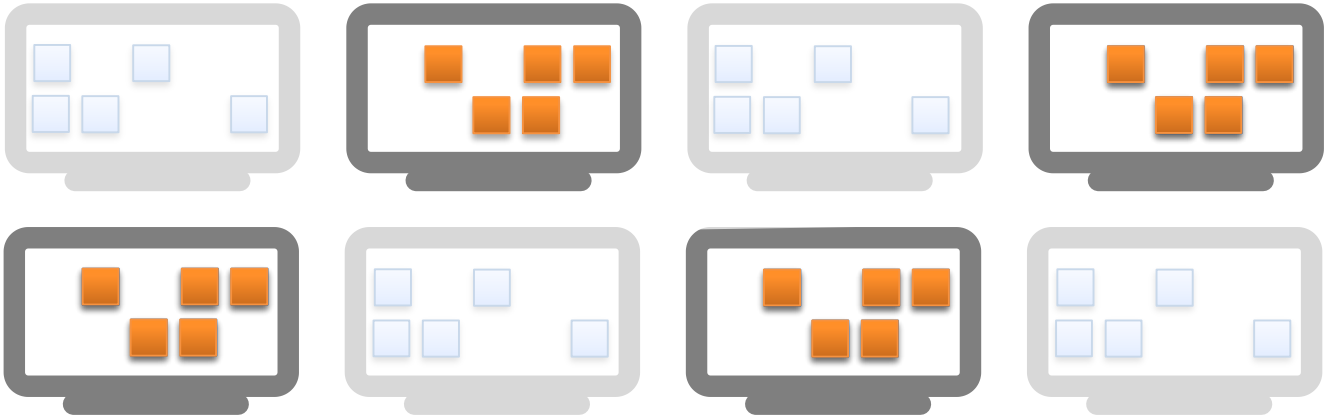
Контроль целостности



Выбираем любой компьютер и ставим на контроль целостности объекты

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль целостности

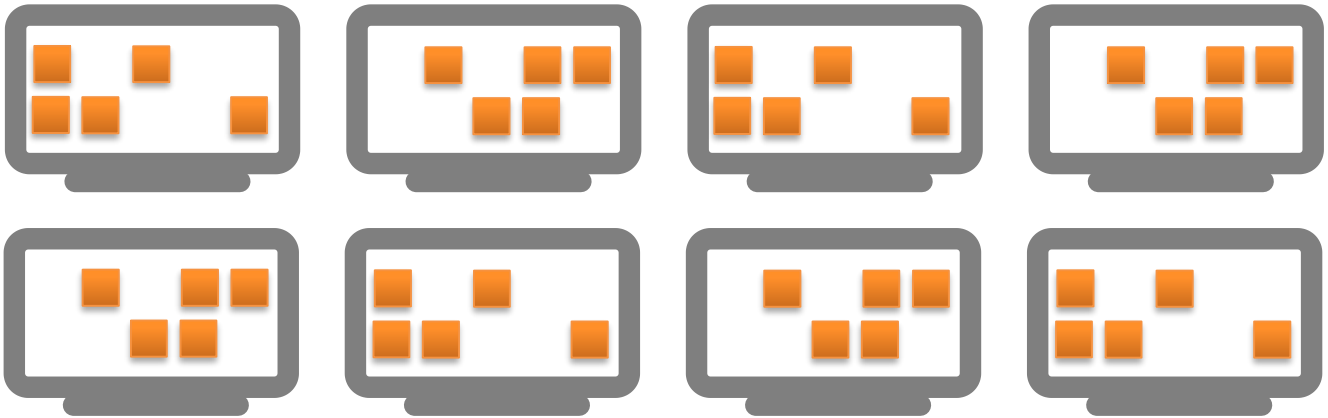


Dallas Lock сам находит похожие компьютеры и ставит объекты на контроль

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль целостности

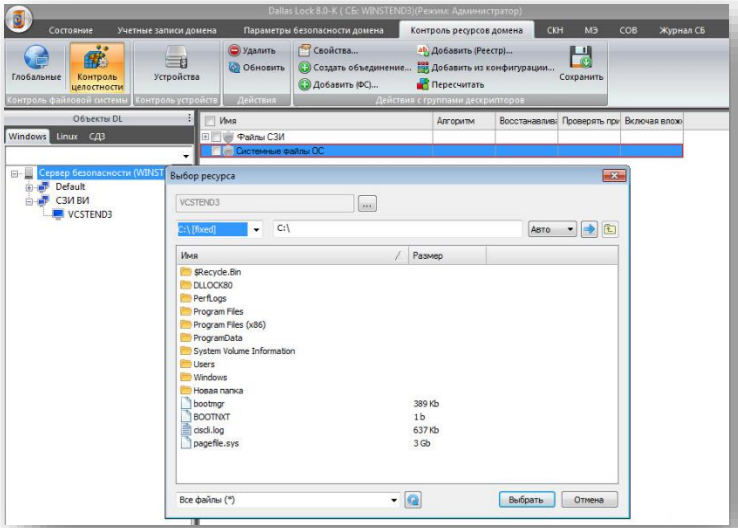


Все остальные объекты также легко обнаруживаются в сети

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль целостности

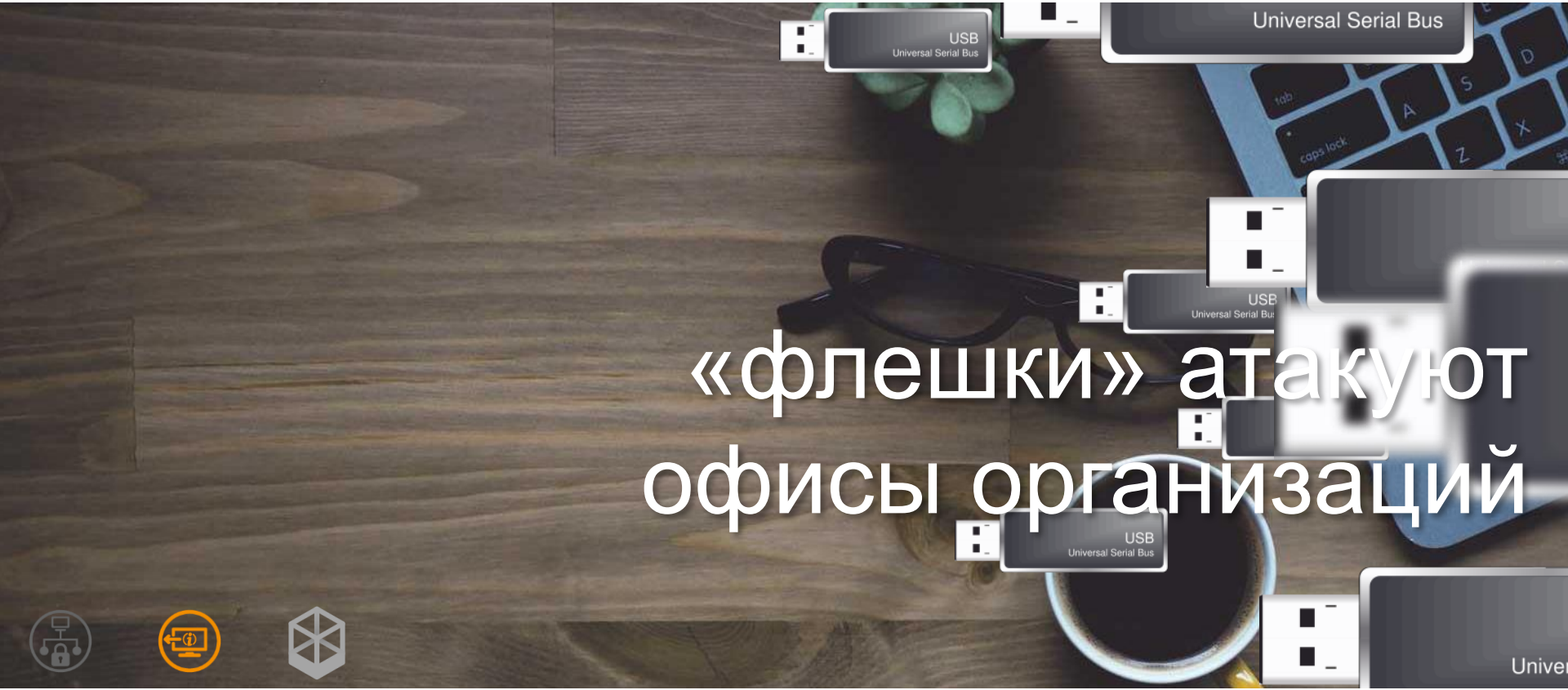
Централизованное управление контролем целостности ещё никогда не было столь удобным



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль переноса информации

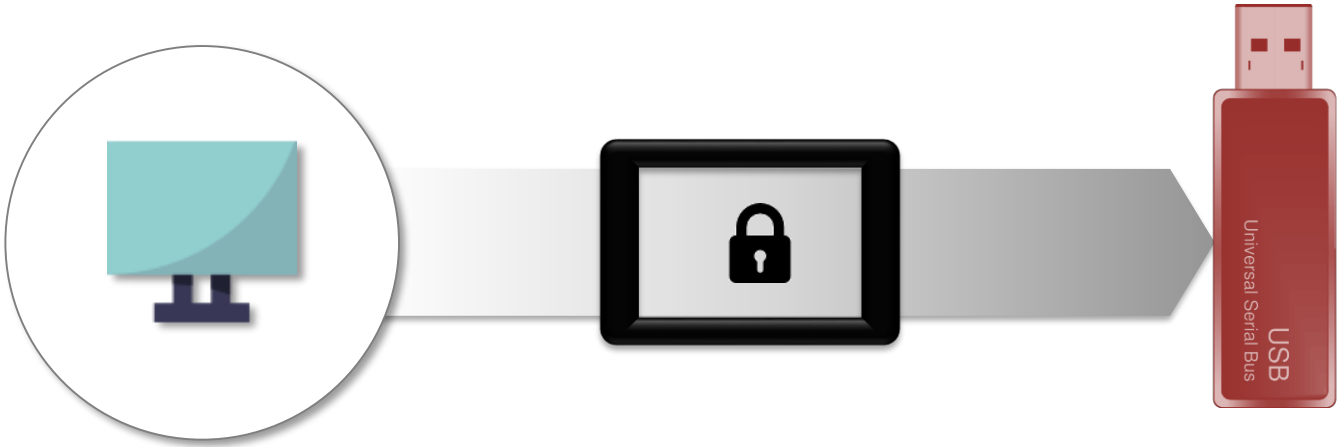


«флешки» атакуют офисы организаций

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль переноса информации



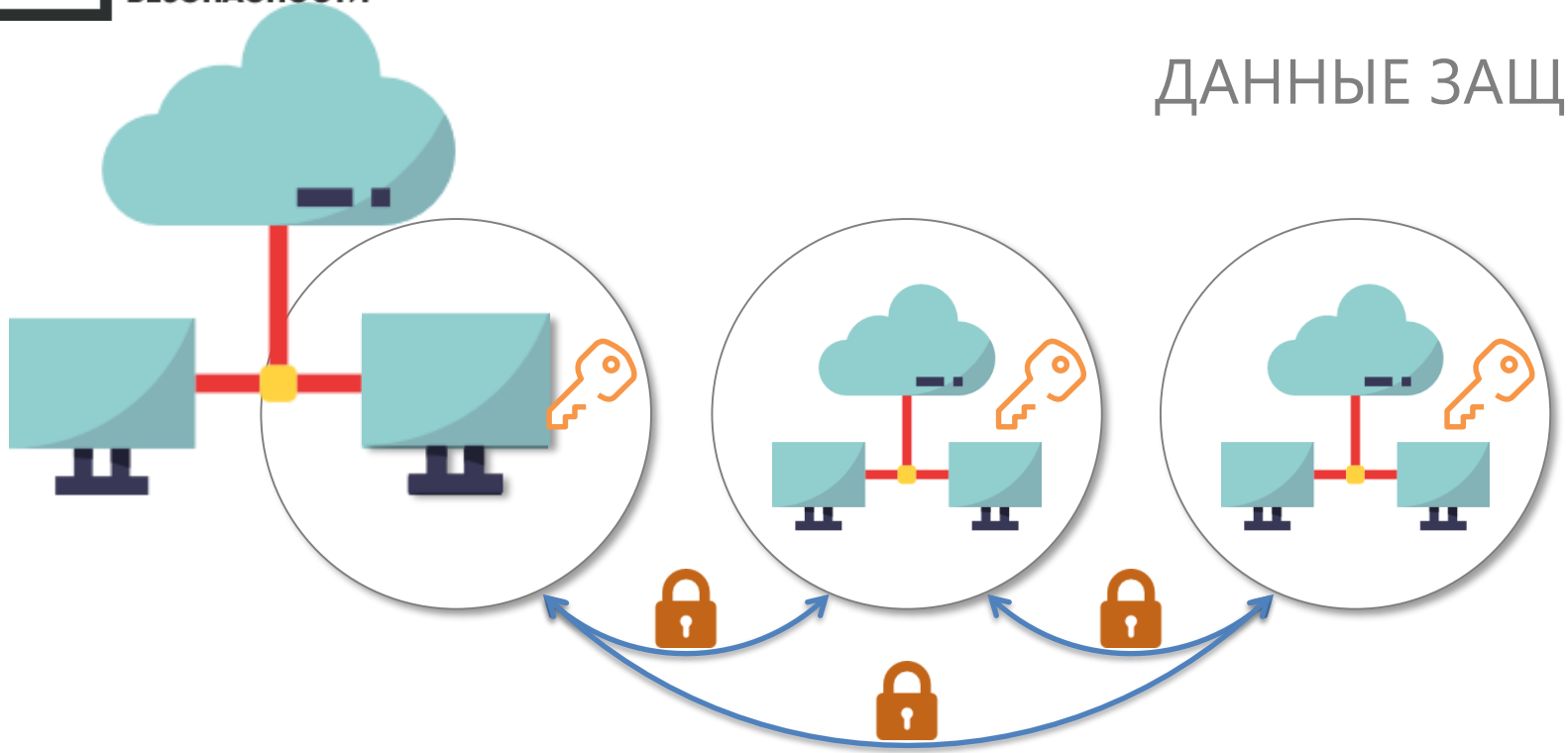
В основе лежит «прозрачное» для пользователя преобразование информации

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Контроль переноса информации

ДАННЫЕ ЗАЩИЩЕНЫ



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасная среда («песочница»)

Приказ ФСТЭК России №239 «**Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации**».

ЗИС.7. Использование эмулятора среды функционирования программного обеспечения («песочница»)

БЕЗОПАСНАЯ СРЕДА
DALLAS LOCK SANDBOX



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасная среда («песочница»)

БЕЗОПАСНАЯ СРЕДА
DALLAS LOCK SANDBOX

Централизованное управление

- потенциально опасные приложения можно запускать в частично виртуализованной безопасной среде
- настройки включают: контроль приложений, эвристический анализ, доступ к файловой системе и реестру
- в журнале фиксируются принудительное завершение приложения с указанием нарушенных правил

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасная среда («песочница»)

Доступно описание на портале dallaslock.ru

Дальнейшее **развитие «Песочницы»**:

- ★ Автоматизация действий пользователя (сценарный подход).
- ★ Повышение удобства использования.
- ★ Возможность ещё более гибкой настройки.

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6 декабря 2018 г.
Астана

#CODEIB

СЕРГЕЙ КУЗНЕЦОВ
Коммерческий директор ЦЗИ ГК «Конфидент»
WEB: WWW.DALLASLOCK.RU
EMAIL: ISC@CONFIDENT.RU

DALLAS LOCK

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ