КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНФИДЕНТ® ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK

КАК ЗАЩИТИТЬ КИИ С ПОМОЩЬЮ РЕШЕНИЙ DALLAS LOCK?

ЛАМАНОВ СЕРГЕЙ

Руководитель по работе с партнерами
ЦЗИ ГК «Конфидент»

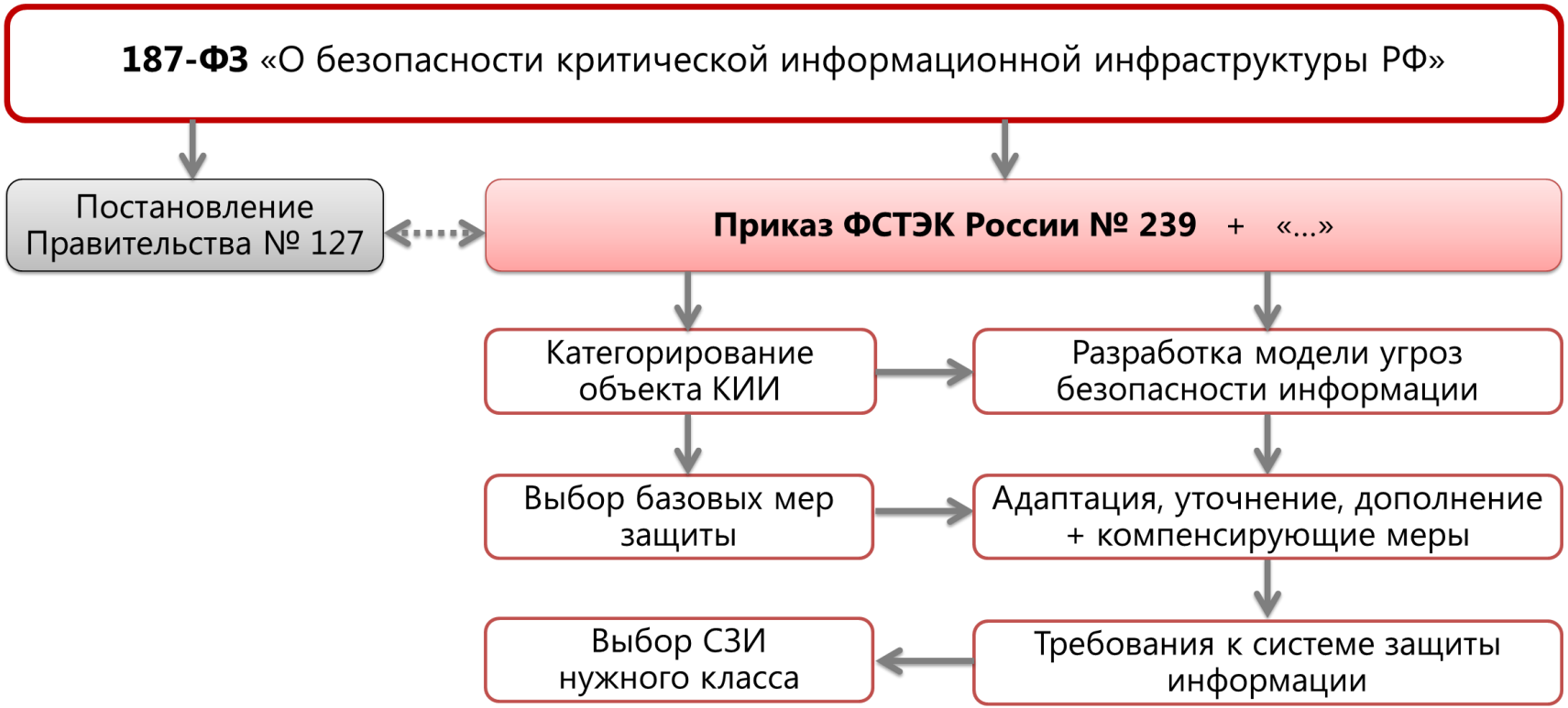
WEB: WWW.DALLASLOCK.RU

EMAIL: LSA@CONFIDENT.RU

Защита ГИС


149-ФЗ «Об информации, информационных технологиях и о защите информации»
Постановление Правительства № 676
Приказ ФСТЭК России № 17 + «Методичка»
Классификация ГИС
Разработка модели угроз безопасности информации
Выбор базовых мер защиты
Адаптация, уточнение, дополнение + компенсирующие меры
Выбор СЗИ нужного класса
Требования к системе защиты информации

Защита КИИ


187-ФЗ «О безопасности критической информационной инфраструктуры РФ»
Постановление Правительства № 127
Приказ ФСТЭК России № 239 + «...»
Категорирование объекта КИИ
Разработка модели угроз безопасности информации
Выбор базовых мер защиты
Адаптация, уточнение, дополнение + компенсирующие меры
Выбор СЗИ нужного класса
Требования к системе защиты информации

Законодательство о КИИ

Федеральный закон от 26.07.2017 г. N 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации» и соответствующие нормативно-правовые акты

Приказ ФСТЭК России от 21.12.2017 г. №235
«Об утверждении Требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования».

Приказ ФСТЭК России от 25.12.2017 г. №239
«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

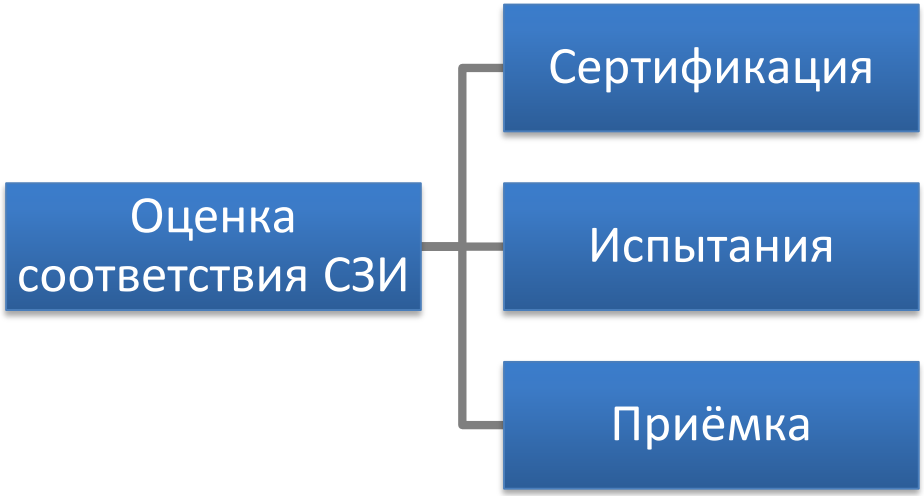
Законодательство о КИИ

Согласно Приказу ФСТЭК России №235 «**Об утверждении Требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования**» к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, относят следующие виды СЗИ:

- ***«средства защиты информации от несанкционированного*** *доступа (включая встроенные в общесистемное, прикладное программное обеспечение);*
- ***межсетевые экраны****;*
- ***средства обнаружения (предотвращения) вторжений*** *(компьютерных атак);*
- *средства антивирусной защиты;*
- *средства (системы) контроля (анализа) защищённости;*
- *средства управления событиями безопасности;*
- *средства защиты каналов передачи данных».*

Законодательство о КИИ

Оценка соответствия СЗИ согласно Приказу ФСТЭК России №235 «**Об утверждении Требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования**»:

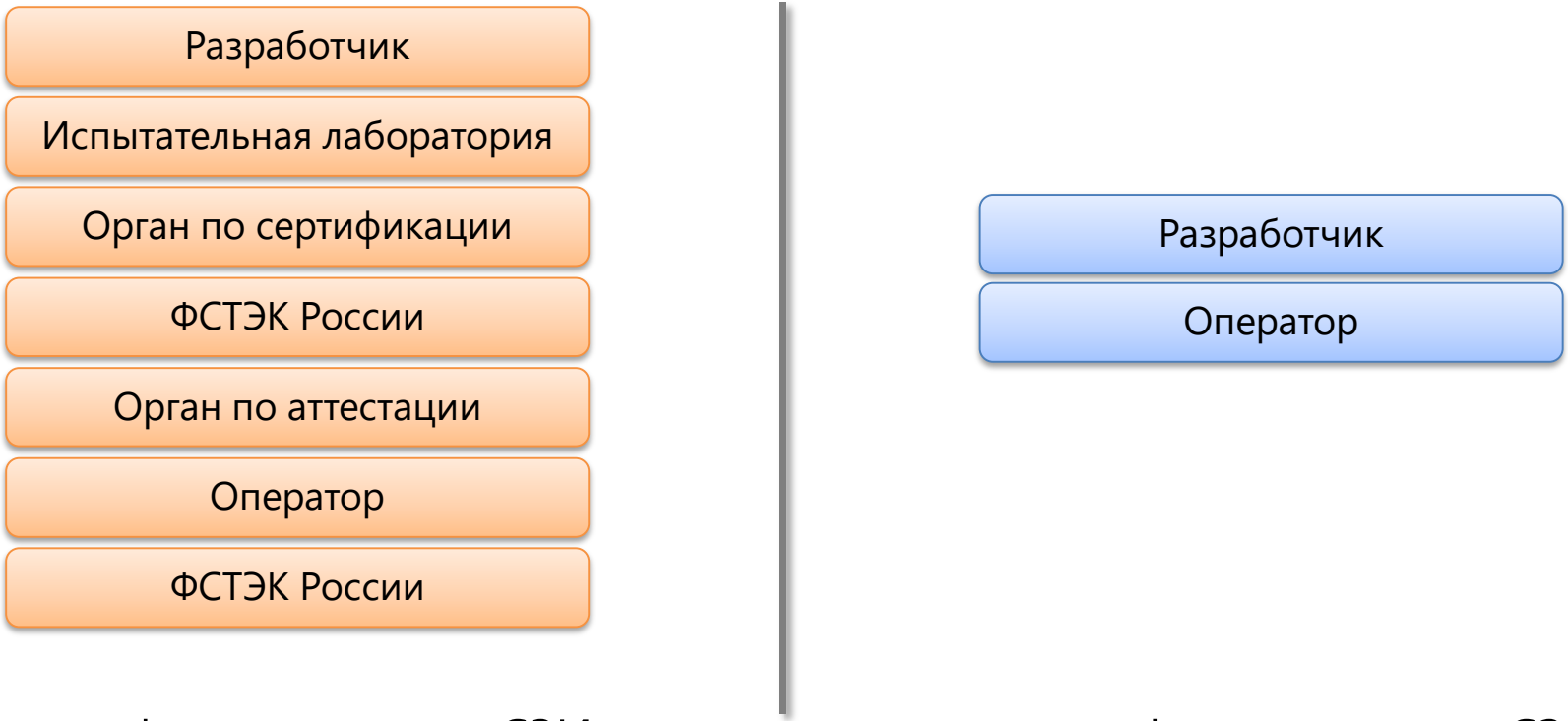


В соответствии с законодательством или по решению субъекта КИИ

Самостоятельно или с привлечением лицензиатов

Самостоятельно или с привлечением лицензиатов

Кем проверяются СЗИ?



сертифицированные СЗИ

не сертифицированные СЗИ

Требования приказа №239

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

«Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой.»

«В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения»

Требования системы сертификации

Приказ ФСТЭК России №55 от 3 апреля 2018 г.
«Положение о системе сертификации средств защиты информации».

Сертификационные испытания включают:

- проверку организации технической поддержки средства защиты информации, предусматривающую оценку соответствия работ (услуг) по технической поддержке средства защиты информации в ходе его эксплуатации, проводимых (предоставляемых) заявителем, требованиям по безопасности информации.

При проверке организации производства программных и программно-технических средств защиты информации проверяется внедрение заявителем процедур безопасной разработки программного обеспечения.

Законодательство о КИИ

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

Требования к СЗИ в зависимости от категории значимости объекта КИИ:

Категория значимости	3	2	1
СЗИ	6+	5+	4+
СВТ	5+	5+	5+
НДВ	-	4+	4+

Законодательство о КИИ

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

Требования к СЗИ в зависимости от категории значимости объекта КИИ:

Категория значимости	3	2	1
СЗИ	6+	5+	4+
СВТ	5+	5+	5+
НДВ		4+	4+
УД	6+	5+	4+

Приказ №60 от 26.03.2019
(регистрация от 18.04.2019)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54443
от 18 апреля 2019

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

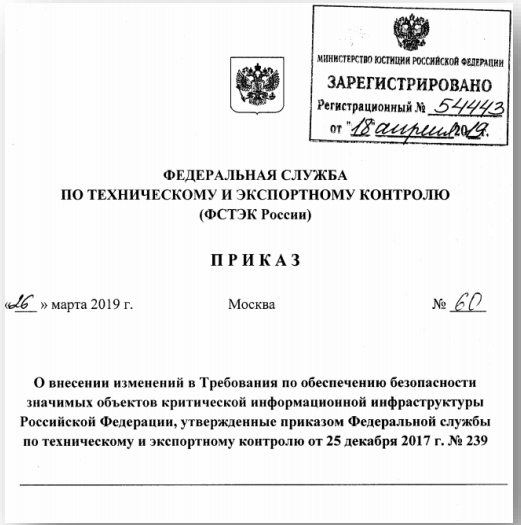
ПРИКАЗ

«16» марта 2019 г. Москва № 60

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

Соответствие законодательству

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



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54443
от "18" апреля 2019

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

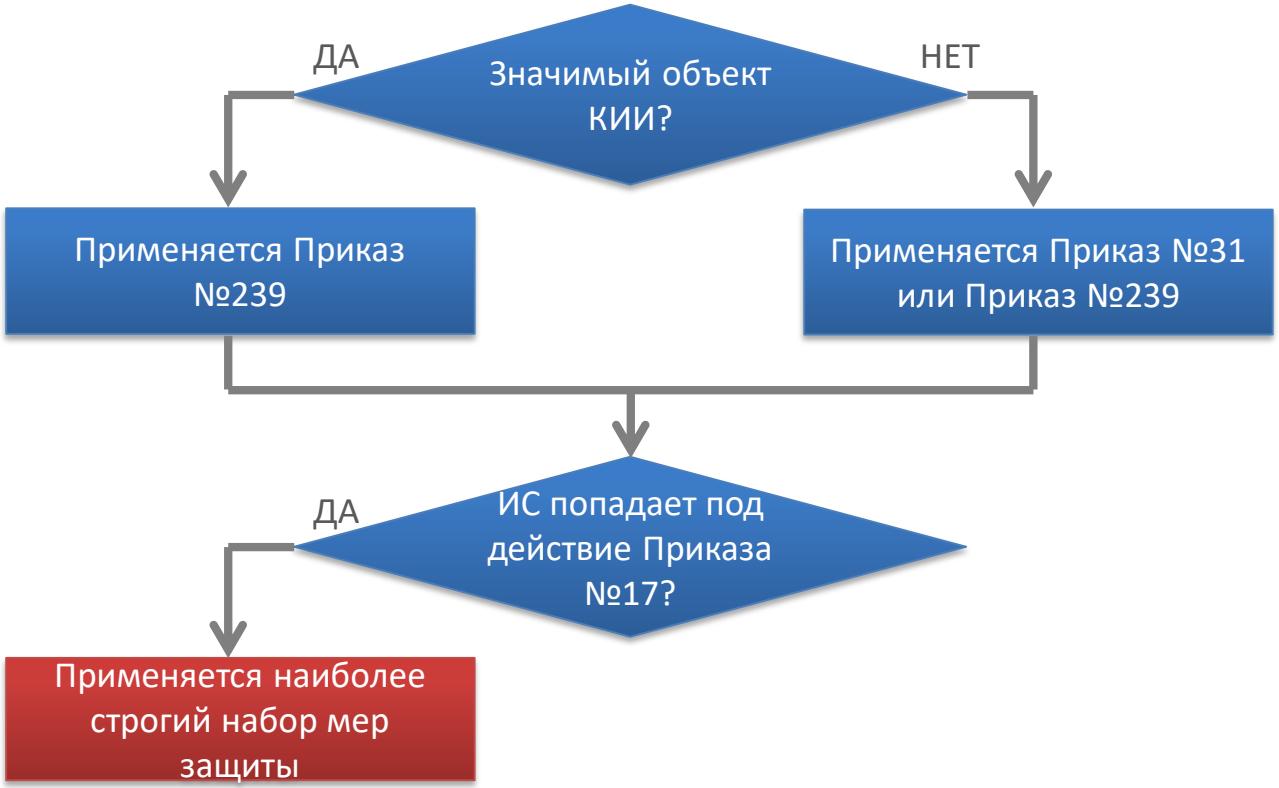
ПРИКАЗ

«16» марта 2019 г. Москва № 60

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

- приведение в соответствие Приказу ФСТЭК России №131 от 30.07.2018 «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия…» - уровни доверия 4, 5, 6 для категорий значимости 1, 2, 3;
- «требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта КИИ» должны быть в ТЗ;
- изменился базовый набор мер.

Законодательство о КИИ



Соответствие законодательству

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

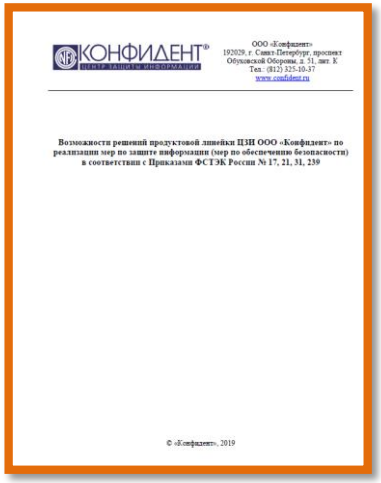
- **Идентификация и аутентификация**
- **Управление доступом**
- **Ограничение программной среды**
- **Защита машинных носителей информации**
- **Аудит безопасности**
- Антивирусная защита
- **Предотвращение вторжений (компьютерных атак)**
- **Обеспечение целостности**
- **Обеспечение доступности информации**
- Защита технических средств и систем
- **Защита информационной (автоматизированной) системы и её компонентов**
- Реагирование на инциденты информационной безопасности
- **Управление конфигурацией**
- **Управление обновлениями программного обеспечения**
- Планирование мероприятий по обеспечению безопасности
- Обеспечение действий в нештатных (непредвиденных) ситуациях
- Информирование и обучение персонала

Соответствие законодательству

Возможности Dallas Lock по выполнению мер защиты информации:

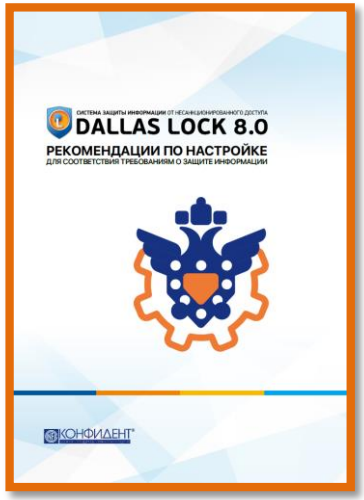
- **Приказ №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».**
- **Приказ №17** «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- **Приказ №21** «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- **Приказ №31** «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Возможности по реализации мер защиты информации



Возможности решений продуктовой линейки ЦЗИ ООО «Конфидент» по реализации мер по защите информации (мер по обеспечению безопасности) в соответствии с Приказами ФСТЭК России № 17, 21, 31, 239

Возможности по реализации мер защиты информации



DALLAS LOCK 8.0
РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Продуктовая линейка Dallas Lock

Dallas Lock 8.0

Dallas Lock Linux

СДЗ Dallas Lock

СЗИ ВИ Dallas Lock

Набор решений для защиты конечных точек в физических и виртуализованных средах с централизованным управлением

Продуктовая линейка Dallas Lock

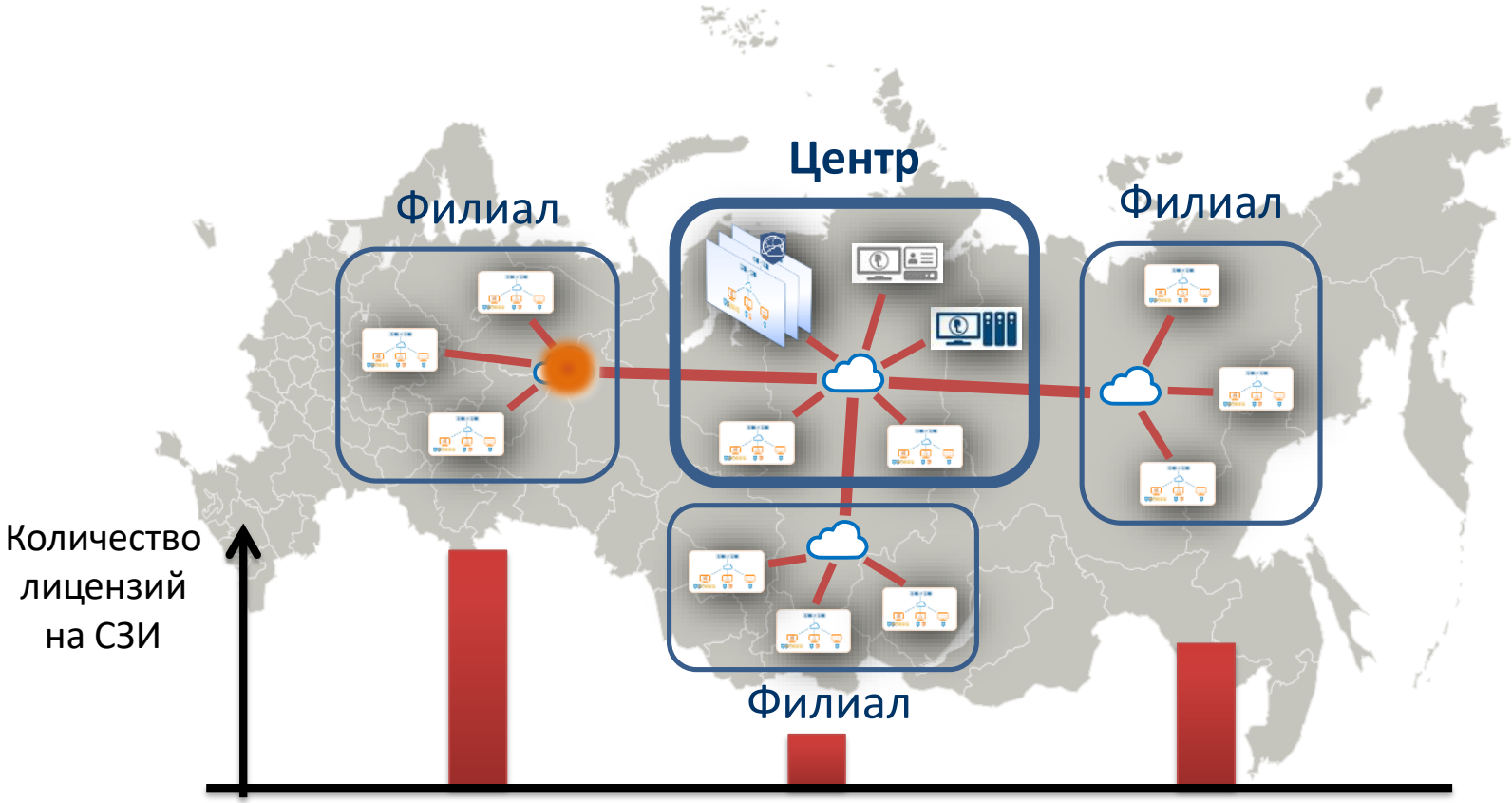
Характеристика	DL 8.0-K	DL 8.0-C	DL Linux	СЗИ ВИ	СДЗ
Тип СЗИ	ПО	ПО	ПО	ПО	ПАК
Централизованное управление	Да + ЕЦУ – 1 кв. 2020 г.				
Сертификат соответствия ФСТЭК России	№ 2720 от 25.09.2012	№ 2945 от 16.08.2013	№ 3594 от 04.07.2016	№ 3837 от 18.12.2017	№ 3666 от 25.11.2016
Сертификат соответствия Минобороны России	–	№ 3902 от 23.03.2018	–	–	№ 3789 от 11.12.2017
Класс защищенности СВТ	5	3	5	5	–
Класс защиты МЭ	4	4	–	–	–
Класс защиты СОВ	4	4	–	–	–
Класс защиты СКН	4	2	–	–	–
Класс защиты СДЗ	–	–	–	–	2
Уровень контроля отсутствия НДВ	4	2	4	4	2
Класс АС	1Г	1Б	1Г	1Г	1Б
Уровень защищенности ПДн Класс ГИС / АСУ ТП / КИИ	1				

Кейс:

Управление лицензиями
на средства защиты информации

Управление лицензиями

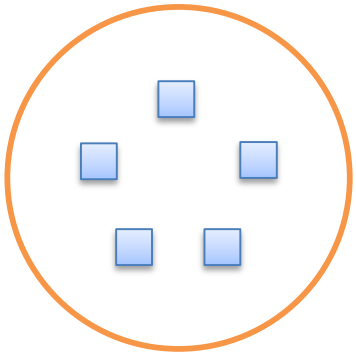
Управление лицензиями



Кейс:

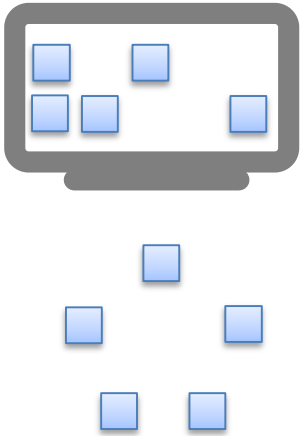
Контроль целостности в больших инфраструктурах

Контроль целостности



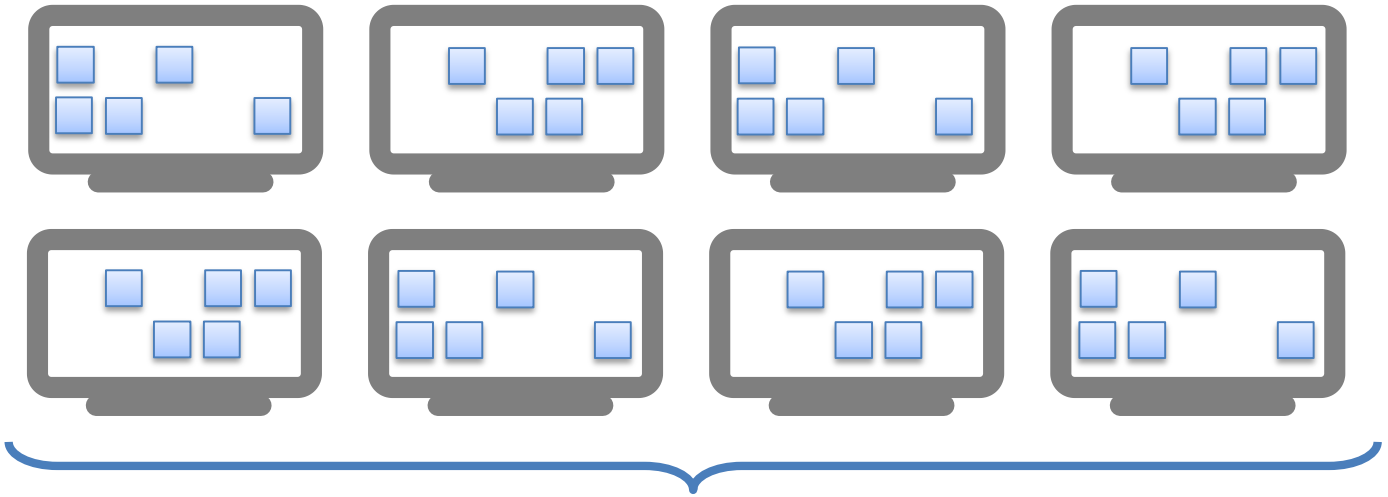
Необходимо контролировать целостность объектов (ресурсов): файлы, «ветки» реестра, программно-аппаратная среда

Контроль целостности



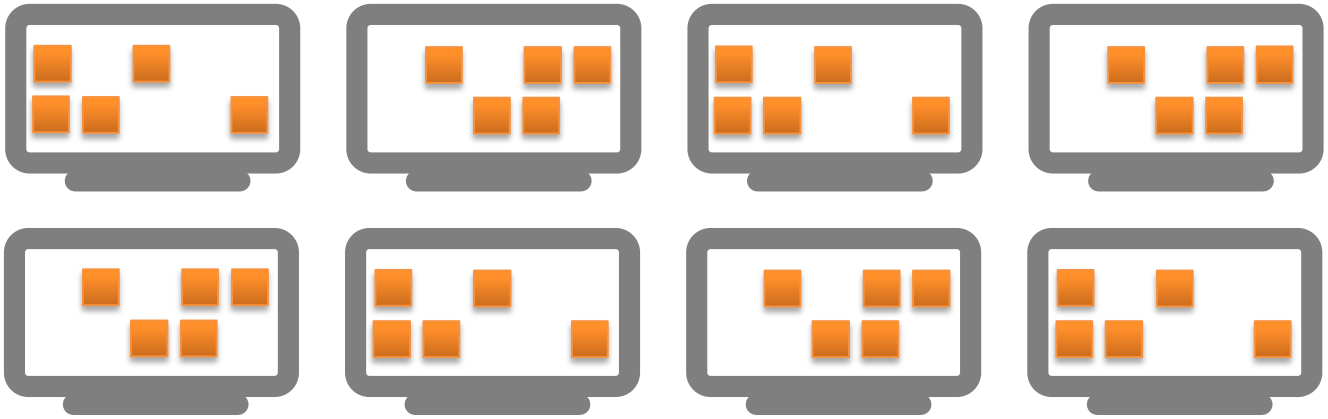
Объекты хранятся «где-то»
на компьютере

Контроль целостности



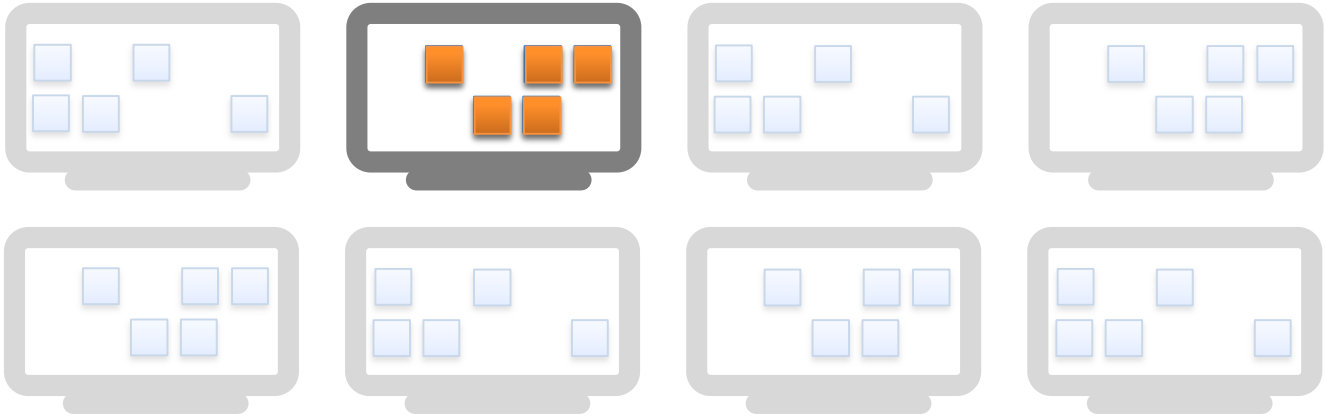
Компьютеров много и они разные (x32, x64), а объекты размещаются в разных местах

Контроль целостности



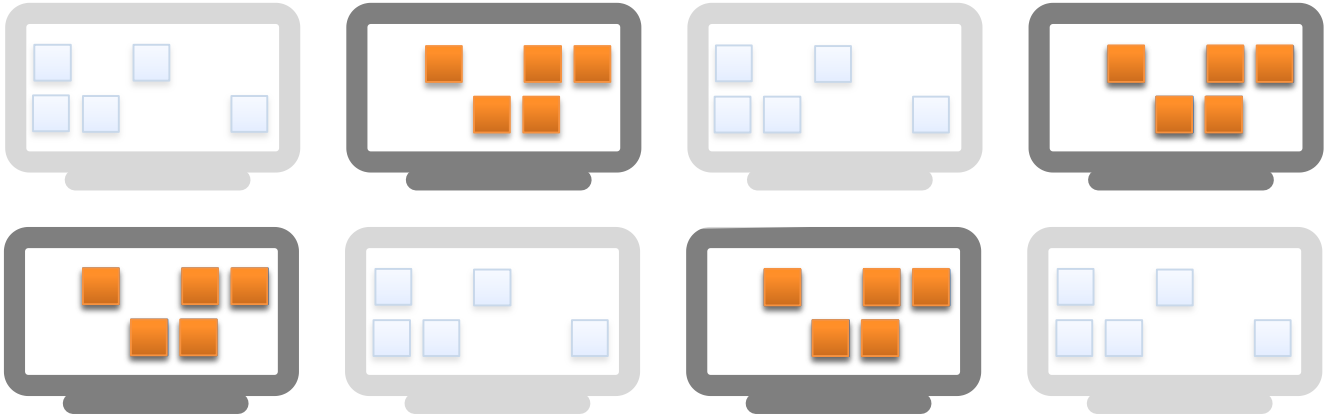
Классическое удалённое управление всё равно занимает слишком много времени, особенно, когда компьютеров сотни и тысячи

Контроль целостности



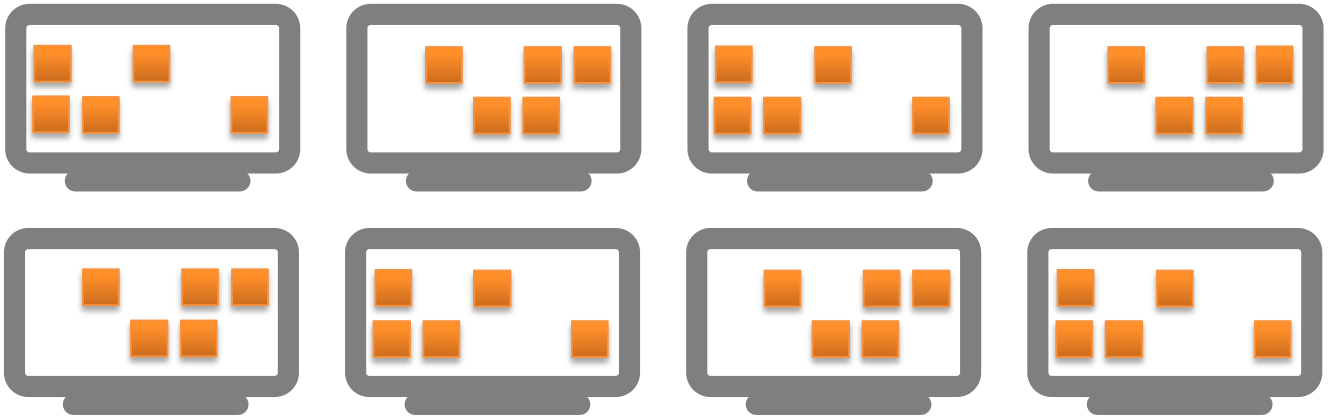
Выбираем любой компьютер и ставим на контроль целостности объекты

Контроль целостности



Dallas Lock сам находит похожие компьютеры и ставит объекты на контроль

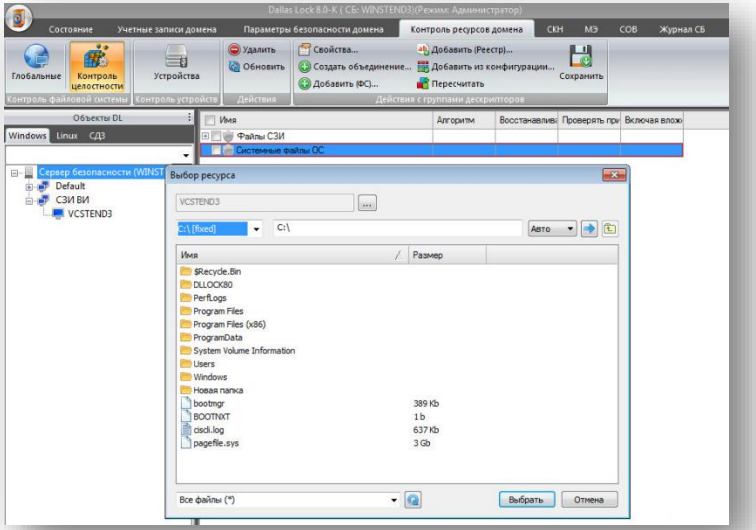
Контроль целостности



Все остальные объекты также легко обнаруживаются в сети

Контроль целостности

Централизованное управление контролем целостности ещё никогда не было столь удобным

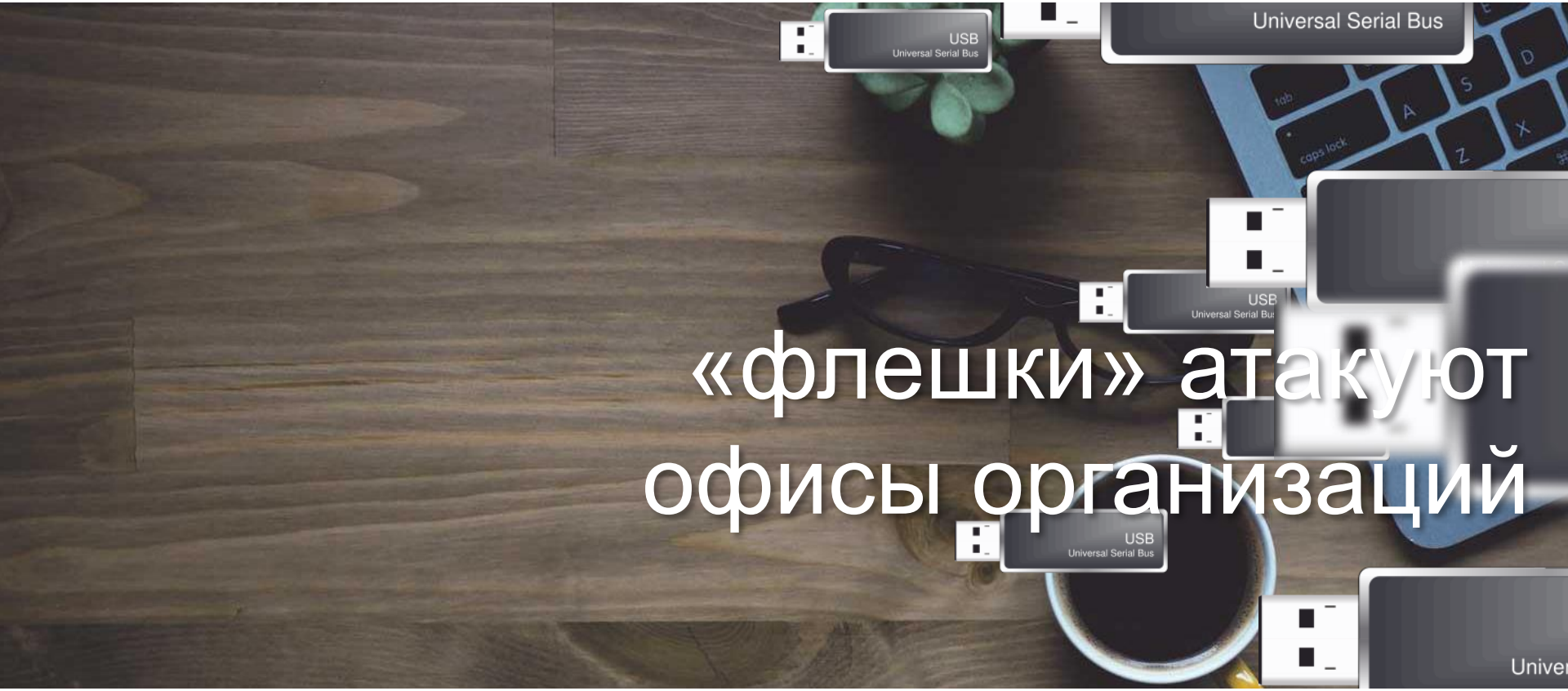


Контроль переноса информации

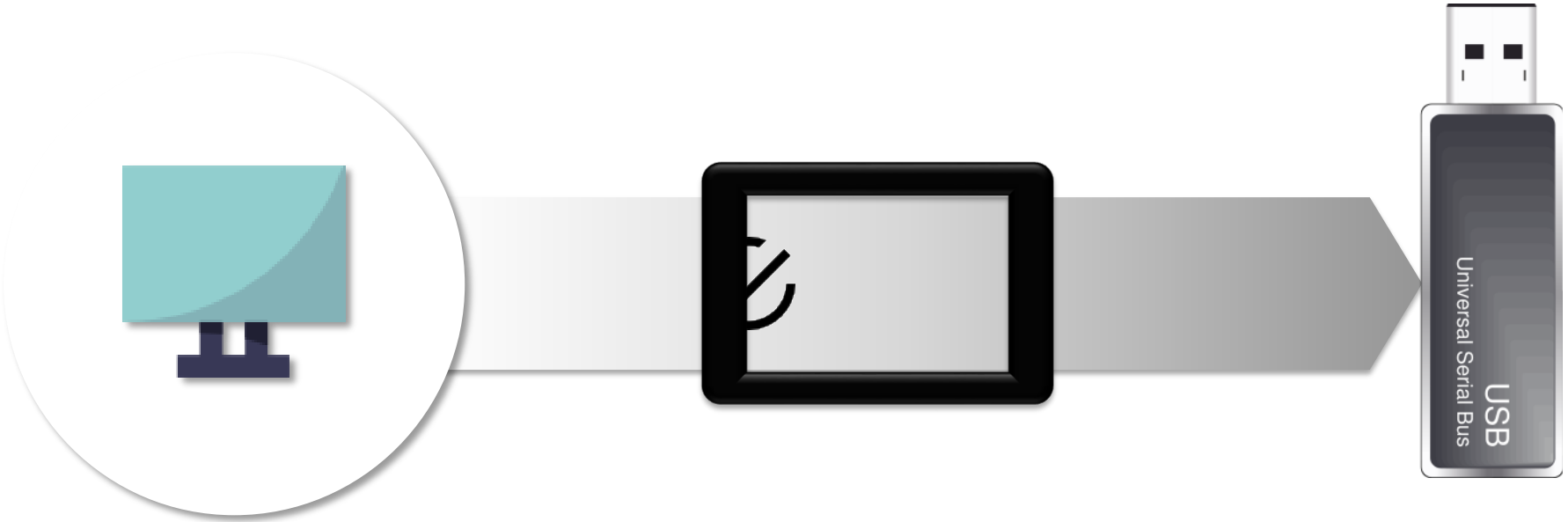
Кейс:

Контроль переноса информации на внешние накопители

Контроль переноса информации

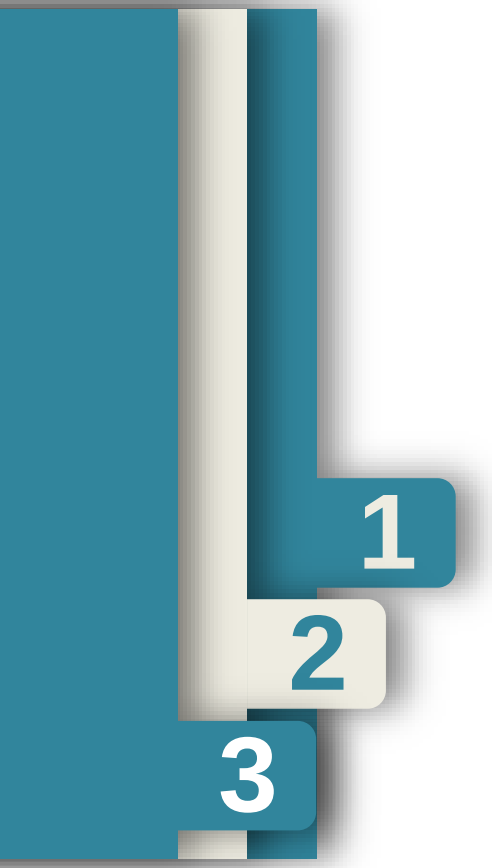


Контроль переноса информации



DLP-система проверяет, являются ли данные конфиденциальной информацией

Контроль переноса информации

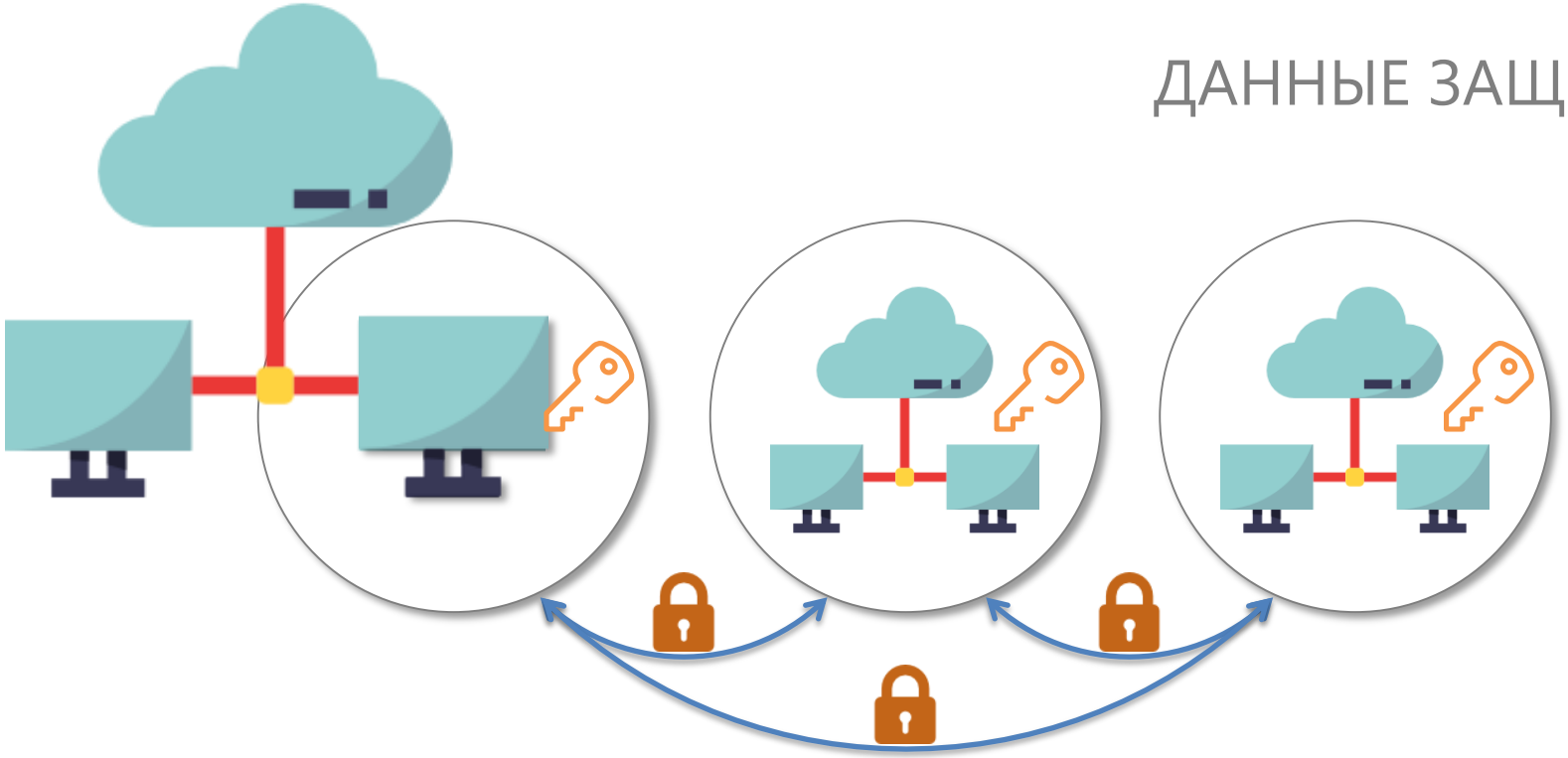


Контроль переноса информации

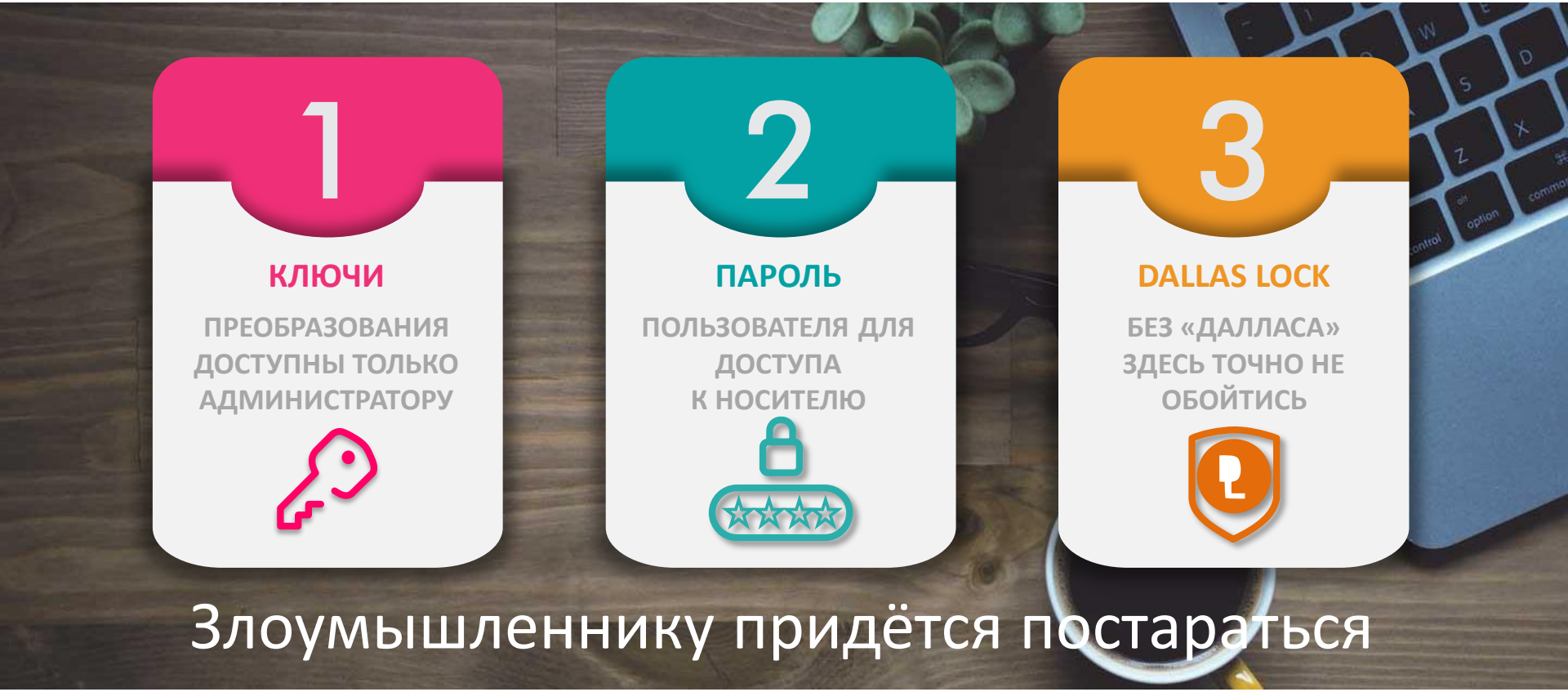
В основе лежит «прозрачное» для пользователя преобразование информации

Контроль переноса информации

ДАННЫЕ ЗАЩИЩЕНЫ



Контроль переноса информации



1

КЛЮЧИ

ПРЕОБРАЗОВАНИЯ ДОСТУПНЫ ТОЛЬКО АДМИНИСТРАТОРУ

2

ПАРОЛЬ

ПОЛЬЗОВАТЕЛЯ ДЛЯ ДОСТУПА К НОСИТЕЛЮ

3

DALLAS LOCK

БЕЗ «ДАЛЛАСА» ЗДЕСЬ ТОЧНО НЕ ОБОЙТИСЬ

Злоумышленнику придётся постараться

Безопасная среда («песочница»)

Кейс:

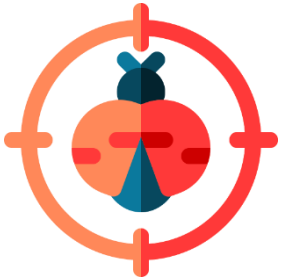
От замкнутой программной среды к безопасной среде

Безопасная среда («песочница»)

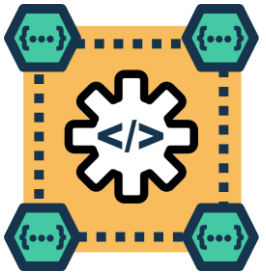
У любого пользователя есть множество идей на тему:
«***почему бы не запустить эту программу***»

Безопасная среда («песочница»)

ЗАПРЕТ АДМИНИСТРАТИВНЫХ ПРИВИЛЕГИЙ



УСТАНОВКА И ОБНОВЛЕНИЕ АНТИВИРУСА



НАСТРОЙКА ЗАМКНУТОЙ ПРОГРАММНОЙ СРЕДЫ

Инструменты администратора ИБ, которые иногда не срабатывают или не совсем удобны

Безопасная среда («песочница»)

- ★ Настраивается администратором ИБ
- ★ Инструмент для пользователя

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

Безопасная среда («песочница»)

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

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

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

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

Привилегированные пользователи

Кейс:

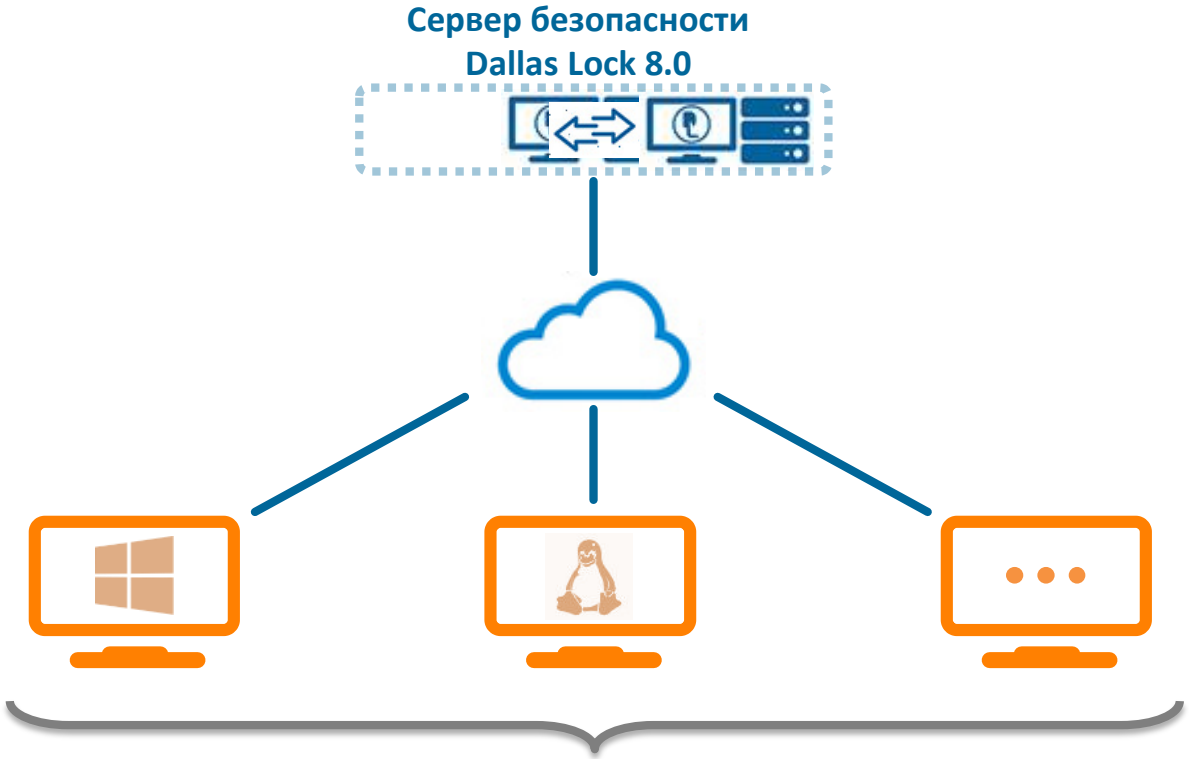
Управление пользователями
с повышенными привилегиями

Привилегированные пользователи

Задачи привилегированных пользователей:

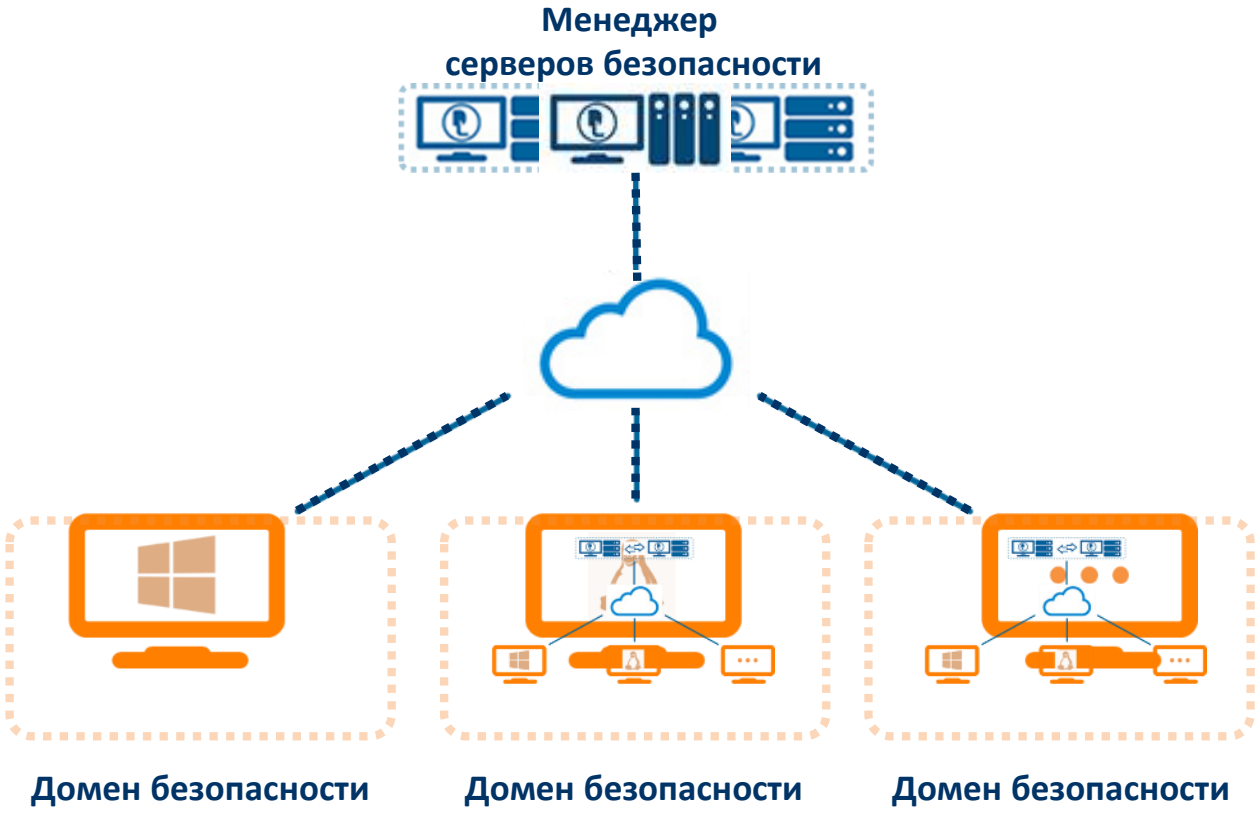
- ★ Установка и обновление средств защиты информации
- ★ Разграничение доступа к информационным ресурсам
- ★ Контроль целостности программно-аппаратной среды
- ★ Управление сменными накопителями
- ★ Управление межсетевым экранированием
- ★ Обнаружение и предотвращение вторжений
- ★ Реагирование на инциденты
- ★ Прочее…

Привилегированные пользователи

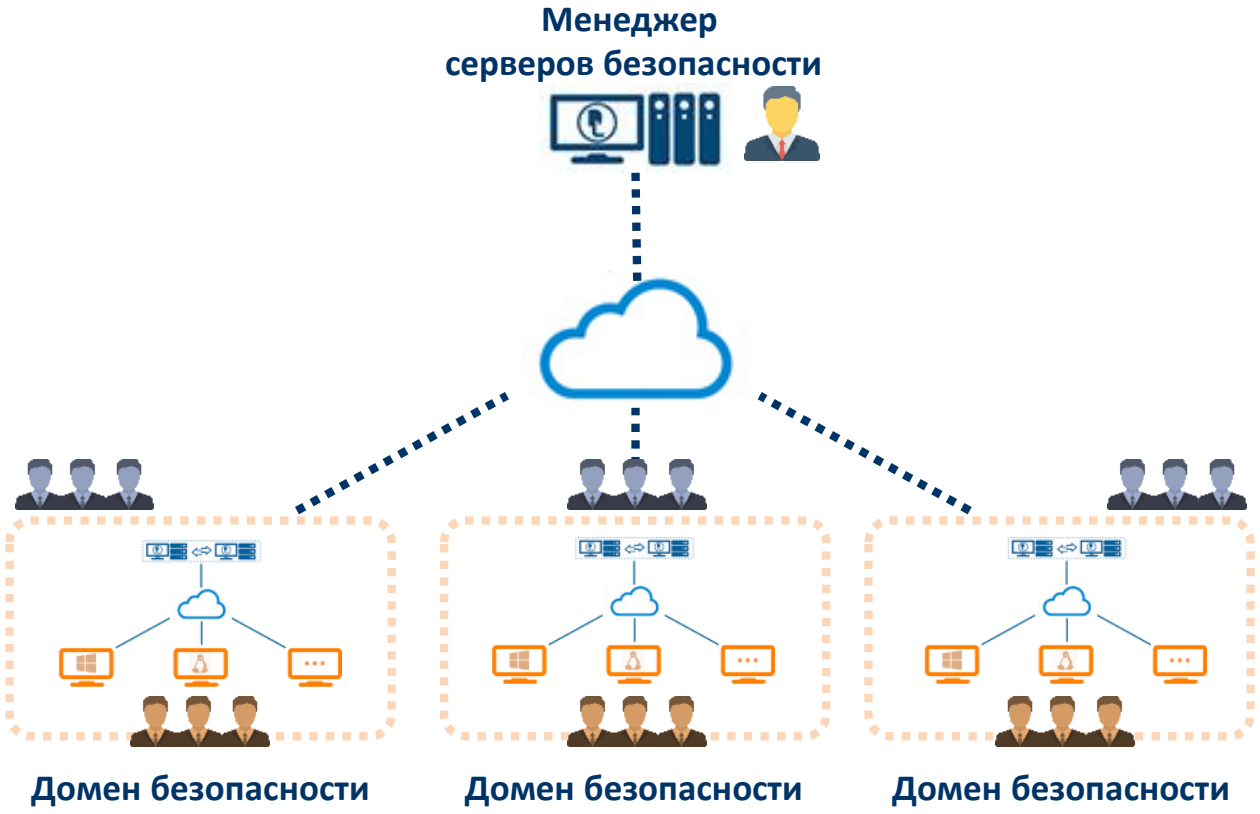


Компьютеры часто объединяются в группы

Привилегированные пользователи



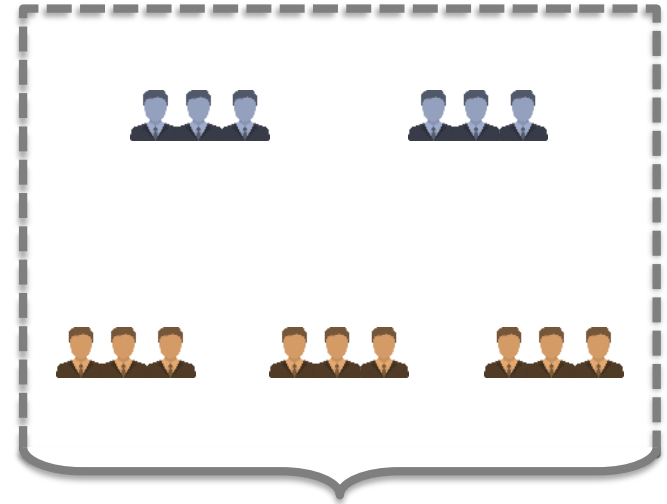
Привилегированные пользователи



Привилегированные пользователи

Привилегированные пользователи

Главный администратор
информационной безопасности



Функциональное распределение обязанностей

Администраторы домена имеют полномочия только в рамках своего **домена безопасности**

Администраторы группы имеют полномочия только в рамках своей **группы компьютеров**

НСД, СКН, МЭ, СОВ, паспортизация ПО и т. п.

КАК защитить КИИ с помощью решений DALLAS LOCK?

Dallas Lock 8.0

Dallas Lock Linux

СДЗ Dallas Lock

СЗИ ВИ Dallas Lock

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK

СПАСИБО ЗА ВНИМАНИЕ!

ЛАМАНОВ СЕРГЕЙ
Руководитель по работе с партнерами
ЦЗИ ГК «Конфидент»
WEB: WWW.DALLASLOCK.RU
EMAIL: LSA@CONFIDENT.RU