Рынок ИБ – тенденции 2016. Взгляд российского разработчика. Информационная безопасность в государственном секторе

Конфиде́нт – человек, с которым ведут интимные разговоры, которому поверяют секреты, тайны. ◆

(«*Замечу вскользь, что в эту несчастную неделю я вынес много тоски, оставаясь почти безотлучно подле бедного сосватанного друга моего в качестве ближайшего его* ***конфидента****». Ф. М. Достоевский, «Бесы», 1872 г. (Цитата из Викитеки.)*)

Свободная энциклопедия **Викисловарь** [vikisłe'vari] многоязычный открытый словарь

КОНФИДЕНТ® CONFIDENT

Более 20 лет на рынке информационной безопасности

Лицензии регуляторов

Более 500 партнёров по РФ

Сертификаты совместимости

Сотни тысяч пользователей Dallas Lock по всей России

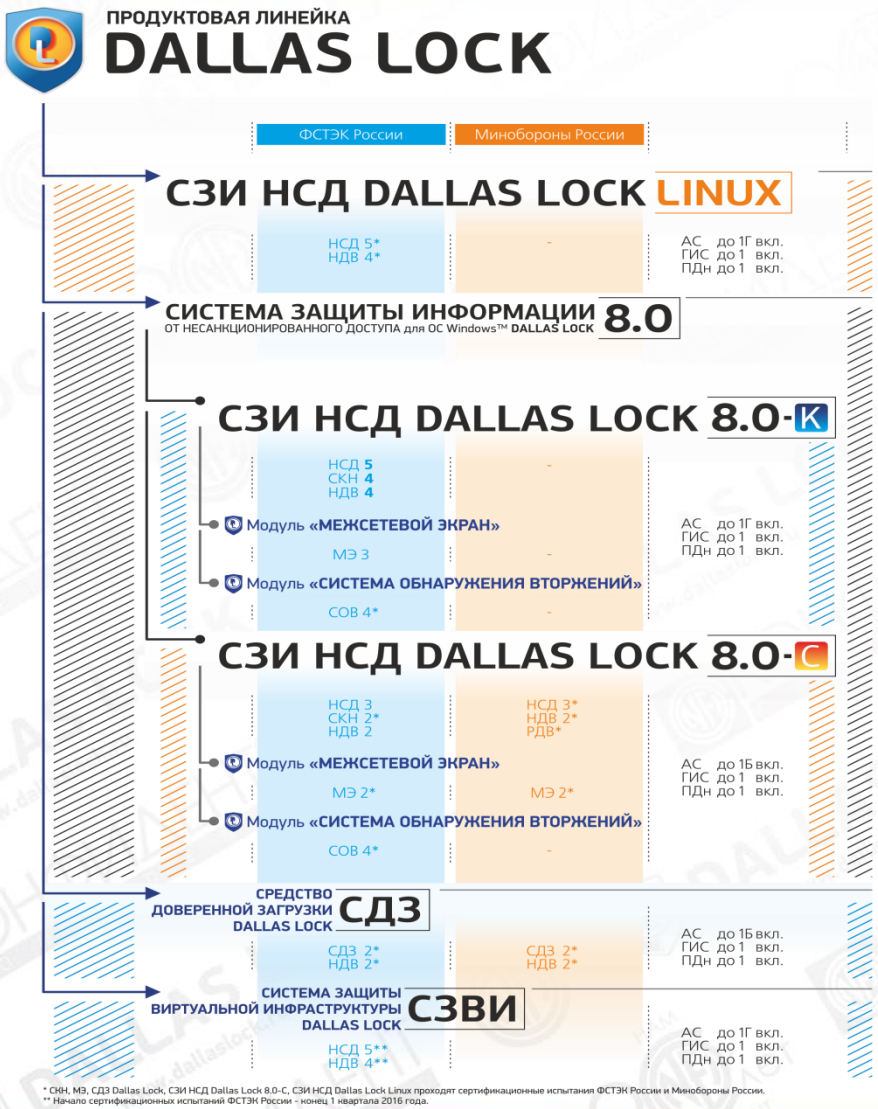
Более 2500 проектов в год с использованием Dallas Lock

Пользователи Dallas Lock

- МЧС России
- ФСО России
- ФНС России
- МВД России
- ФСИН России
- ФСТЭК России
- ФТС России
- ФСКН России
- Роскомнадзор
- Рособрнадзор
- Росстат
- Федеральное медико-биологическое агентство РФ
- Федеральное дорожное агентство РФ
- Банк России
- Национальный банк Республики Абхазия
- Правительство Москвы
- Правительство Санкт-Петербурга
- Администрации субъектов РФ
- Департаменты и центры занятости населения субъектов РФ
- Министерства и департаменты здравоохранения и социального развития субъектов
- Фонды ОМС субъектов РФ
- Министерства и комитеты по управлению имуществом, по земельным отношениям субъектов РФ
- Высшие учебные заведения

- ОАО «ТАНЕКО»
- ООО «Газпром межрегионгаз»
- ОАО «Владимирская областная электросетевая компания»
- ОАО «СибурТюменьГаз»
- ЗАО «Донэнергосбыт»
- ООО «Саратовское предприятие городских электрических сетей»
- ОАО «Первобанк»
- ОАО «Первый Республиканский Банк»
- ООО «Страховое общество «Сургутнефтегаз»
- ООО «Росгосстрах-Медицина»
- НПФ ВТБ
- НПФ «Сургутнефтегаз»
- ОАО «Детский мир»
- ОАО «Объединенная авиастроительная корпорация»
- ОАО «РСК МиГ»
- ОАО «Ангстрем»
- ФГУП «Росморпорт»
- ФГУП «ПО «Октябрь»
- ФГУП «ГосНИИПП» ФСТЭК России
- ФГУП «Гостехстрой» ФСТЭК России
- ОАО «Улан-Удэнский авиационный завод» («Вертолеты России») и другие

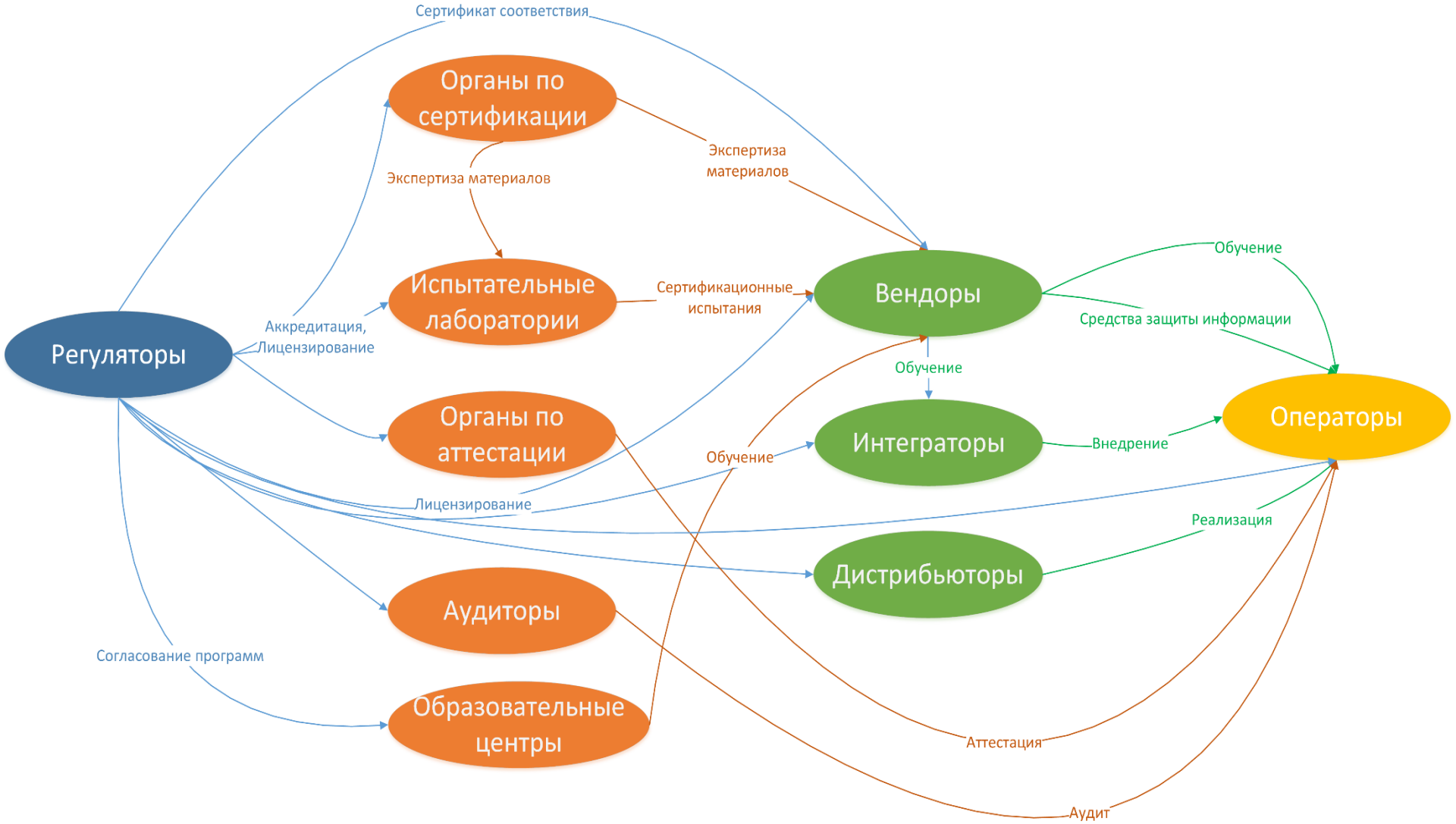
ПРОДУКТОВАЯ ЛИНЕЙКА DALLAS LOCK



- АВТОРИЗАЦИЯ
- КОНТРОЛЬ ПОЛЬЗОВАТЕЛЕЙ
- КОНТРОЛЬ ЦЕЛОСТНОСТИ
- АУДИТ СОБЫТИЙ
- РАЗГРАНИЧЕНИЕ ДОСТУПА
- ЗАЩИТА НОСИТЕЛЕЙ
- КОНТРОЛЬ УТЕЧЕК
- МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ
- ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ
- ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
- ДОВЕРЕННАЯ ЗАГРУЗКА
- ЗАЩИТА ВИРТУАЛИЗАЦИИ

Участники рынка

Рынок ИБ в России



Основные тенденции на рынке ИБ. Регуляторы

Совет безопасности РФ.
Доктрина
информационной безопасности РФ
(проект)

Направления развития

- Развитие отечественных средств и систем защиты информации
- Расширение международной кооперации производителей этих средств и систем
- Развитие нормативно-правовой и методической базы

Основные тенденции на рынке ИБ. Регуляторы

ФСТЭК России

ФСБ России

Роскомнадзор

Минкомсвязи России

Банк России

Министерство обороны РФ

Основные тенденции на рынке ИБ. Регуляторы

ФСТЭК России

Есть

- Приказ № 21 (ПДн)
- Приказ № 17 (ГИС), Меры ГИС
- Приказ № 31 (АСУ ТП)
- Требования к СОВ, САВЗ, СДЗ, СКН
- Банк данных угроз, уязвимостей

В планах 2016 – 2017

- Методические документы АСУ ТП/КВО/КСИИ
- Требования к МЭ, ОС, СУБД, BIOS, DLP, СЗВИ…
- Обновление СЗИ, безопасная разработка
- Методика моделирования угроз
- Новая редакция Приказа № 17

Основные тенденции на рынке ИБ. Регуляторы

ФСБ России

Есть	В планах 2016 – 2017
• Приказ № 378 (использование СКЗИ для защиты ПДн) • Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных	• Приказ о национальном CERT • Серия документов о СОПКА

Основные тенденции на рынке ИБ. Регуляторы

Минкомсвязь России

Есть

- ФЗ № 242 (хранение ПДн)
- Приказ № 96 (импортозамещение)

В планах 2016 – 2017

- Реестр отечественного ПО
- План перехода на СПО

Основные тенденции на рынке ИБ. Вендоры

Импортозамещение ≠ Импортозапрещение

Доля отечественных ИБ-решений

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
ФСТЭК России*		54%		61%								
Минкомсвязь России**	40%						50%					60%
ГК «Конфидент»**		43%					↗					↗

* Во всех отраслях
** В государственном секторе

РОССИЙСКОЕ ПО в ИТ в целом (оценка ГК «Конфидент»)

2014	2015	2016
10%	**12%**	**15%**

ПП РФ № 1236 – запрет на иностранное ПО,

происходящее из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд

с 1 января 2016 года

Определяется перечень программного обеспечения с указанием требований к функционалу.

ПО в реестре распределено по классам, что упрощает поиск.

Обоснование:

- Отсутствует аналогичное отечественное ПО в едином реестре;
- ПО, присутствующее в едином реестре и подходящее по классу и своим функциональным, техническим или эксплуатационным характеристикам ,не соответствует установленным заказчиком требованиям.

Методика не отработана – риски выбора иностранного ПО

Дополнительное время на подготовку документации

03.02.2016 – единый реестр ПО содержит сведения о 3 (трех) программных продуктах

10.02.2016 – единый реестр ПО содержит сведения о 3 (трех) программных продуктах

Актуальный реестр – не ранее III квартала 2016 года

Как готовы к требованиям регуляторов вендоры?

Реакция на выход требований ФСТЭК России:

- требования к **СОВ** (вступили в силу 15 марта 2012 г.).

В реестре ФСТЭК России – **14 (13)** сертифицированных продуктов.
Осведомленность интеграторов – около 100%

- требования к **САВЗ** (вступили в силу 1 августа 2012 г.).

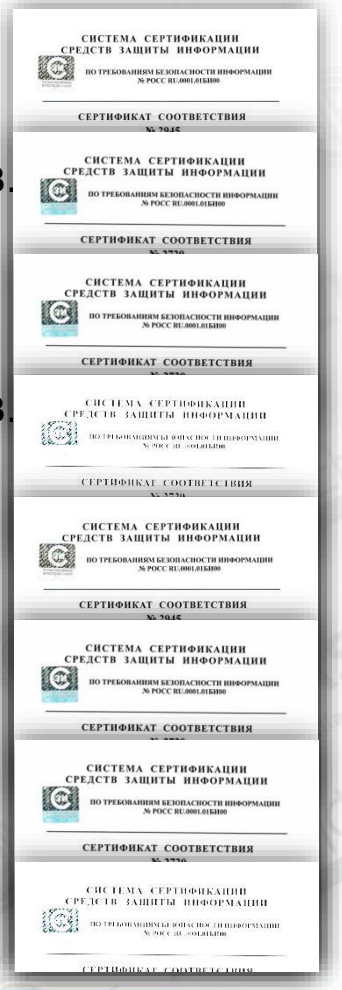
В реестре ФСТЭК России – **14 (12)** сертифицированных продуктов.
Осведомленность интеграторов – около 100%

- требования к **СДЗ** (вступили в силу 1 января 2014 г.).

В реестре ФСТЭК России – **2 (2)** сертифицированных продукта.
Осведомленность интеграторов – около 85%

- требования к **СКН** (вступили в силу 1 декабря 2014 г.).

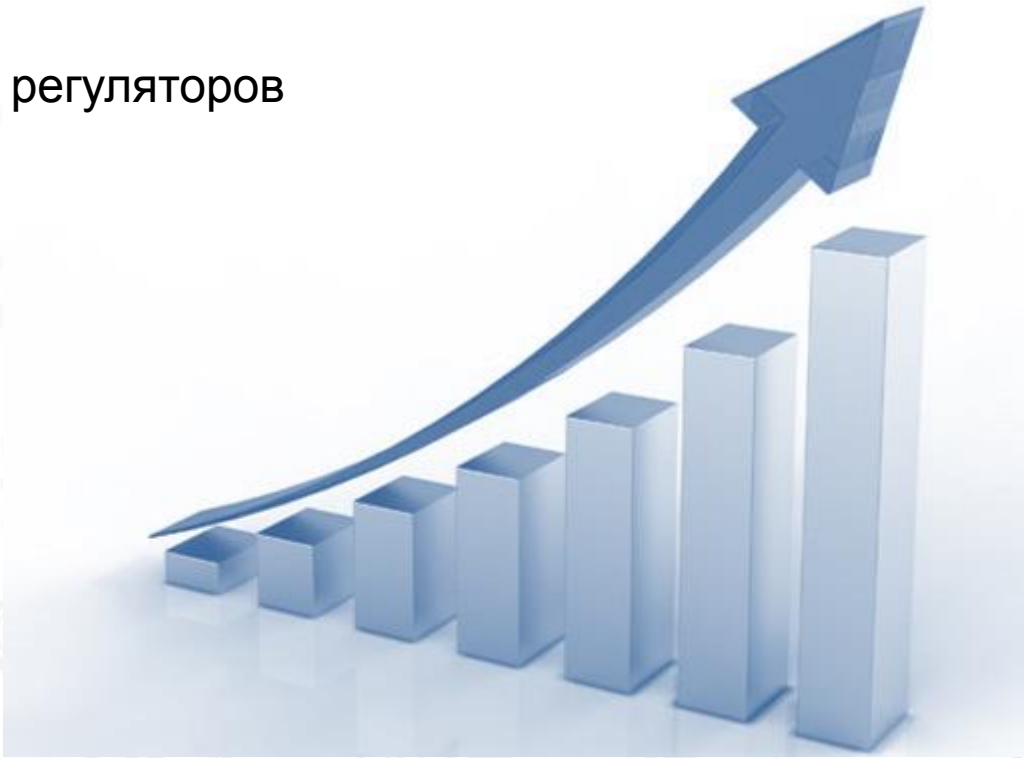
В реестре ФСТЭК России – **0 (2)** сертифицированных продуктов.
Осведомленность интеграторов – около 60%



Основные тенденции на рынке ИБ. Вендоры

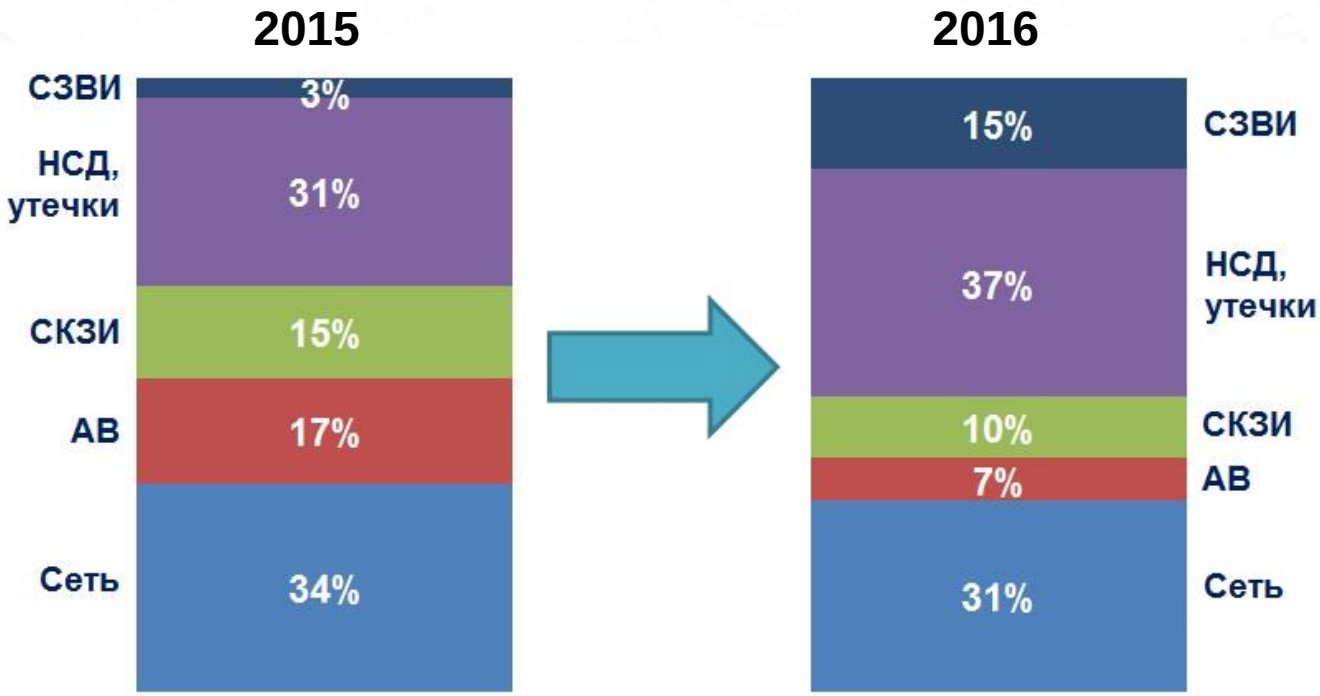
Тенденции развития вендоров:

- развитие компетенций (новые типы СЗИ)
- соответствие новым требованиям регуляторов
- разработка комплексных СЗИ



Основные тенденции на рынке ИБ. Вендоры

Основные СЗИ и их доля в общей ИБ-инфраструктуре



* 1. Без учета наименее востребованных СЗИ (до 3%) – MDM, IAM, САЗ, WCF, SIEM.
2. Сегмент «Сеть» включает МЭ, СОВ, VPN (для корпоративного сегмента поставляются единым продуктом – UTM), а также UTM.
3. Сегмент «НСД, утечки» включает СЗИ НСД, СДЗ, DLP, Endpoint.

Некоторые характеристики проектов

		Требования к АС и СЗИ
ЧТО? Цели, задачи	ПД, ГИС, compliance	Универсальность, многофункциональность
КОГДА? Сроки	Необходимый временной период	Юзабилити (внедрение, администрирование, апгрейд)
СКОЛЬКО? Бюджет	Недостаточный/Расширенный бюджет	Минимальная стоимость приобретения и ССВ, возможность гибкого бюджетирования
ГДЕ? География	Большие площади, труднодоступные районы с плохой инфраструктурой, локальные требования к информатизации	Наличие инструментов удаленного и централизованного внедрения, администрирования, апгрейда
КТО? Исполнители	Федеральные компании, рег. интеграторы, собственные подведомственные структуры, лицензии ФСТЭК России, опыт, репутация, команда	Известность на рынке, присутствие в каждом регионе, наличие партнеров фед. и рег. уровней, система подготовки специалистов, сертификация специалистов
КАК? МТО проекта/заказчика	АС и ПО, много неопределенности на момент проекта, на будущее	Многофункциональность, нечувствительность к «деталям» инфраструктуры, гибкость
КАК? Юр. и полит. аспекты	Сертификаты, лицензии, ИК АС и ПО, импортозамещение	Производитель – лицензиат, решения – с действующими сертификатами, регулярные ИК, желательно – российская компания (владельцы-резиденты РФ, разработка и производство – РФ)
КАК? Окружение проекта	Взаимодействие с региональными ИС, коммерческими ИС, ГИС, универсальность, совместимость АС и ПО	Универсальность, совместимость

ОСОБЕННОСТИ ИБ-ПРОЕКТОВ. ГОСЗАКУПКИ

Основные неточности (ошибки)*

2016: работа над ошибками

* Статистика по результатам анализа специалистами ЦЗИ ГК «Конфидент» требований к конкурсной документации (портал Госзакупок).

Вопросы?

Спасибо за внимание!

ООО «Конфидент»
Центр защиты информации

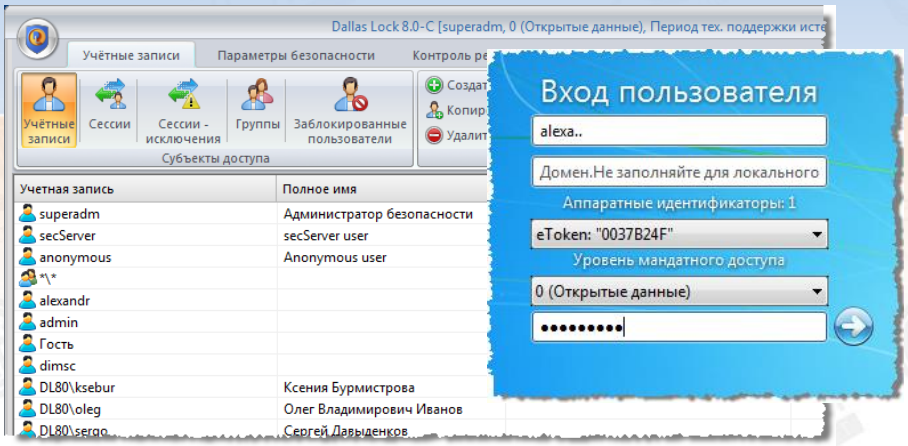
192029, г. Санкт-Петербург,
пр. Обуховской Обороны, д. 51, лит. К
Тел.: +7 (812) 325-10-37 (многоканальный)

ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)**

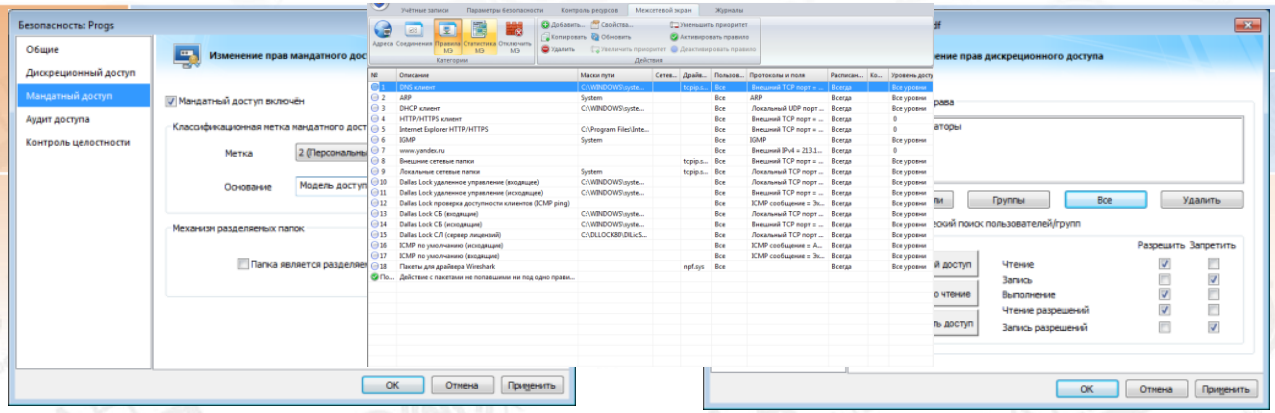
Инструменты по реализации требований	• Идентификация и аутентификацию субъектов доступа по имени пользователя, паролю и аппаратному идентификатору.
	• Идентификация объектов доступа:
	  • терминалов, ЭВМ и узлов сети ЭВМ – по логическим именам;
	  • внешних устройств и внешних носителей информации – по серийному номеру и типу носителя;
	  • программ, томов, каталогов, файлов, записей – по именам

Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



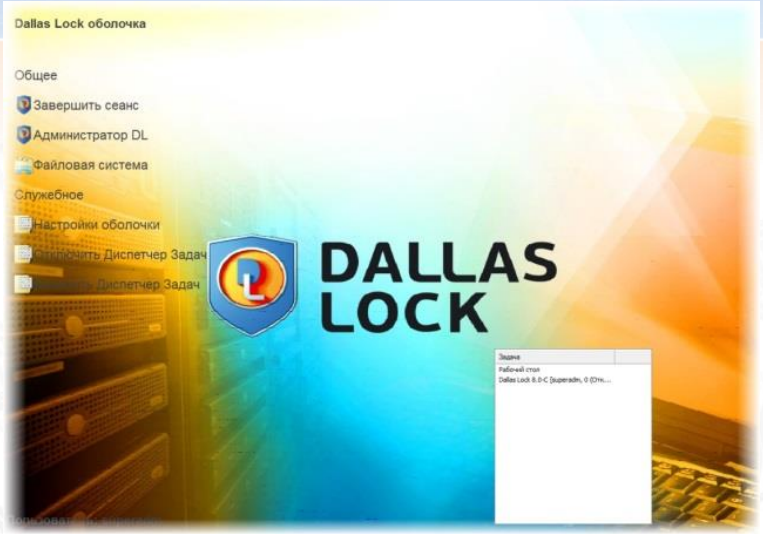
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Управление доступом субъектов доступа к объектам доступа (УПД)** **Межсетевое экранирование (УПД.3)**
Инструменты по реализации требований	• Разграничение доступа дискреционным и мандатным принципами, не зависимыми от ОС механизма • Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между ИС
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux** **МЭ Dallas Lock 8.0**



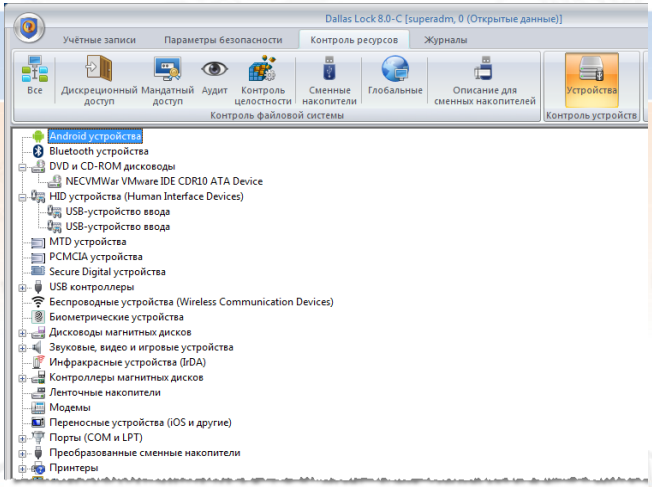
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Ограничение программной среды (ОПС)**	
Инструменты по реализации требований		• Организация замкнутой программной среды, в том числе автоматизированными способами
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)**	



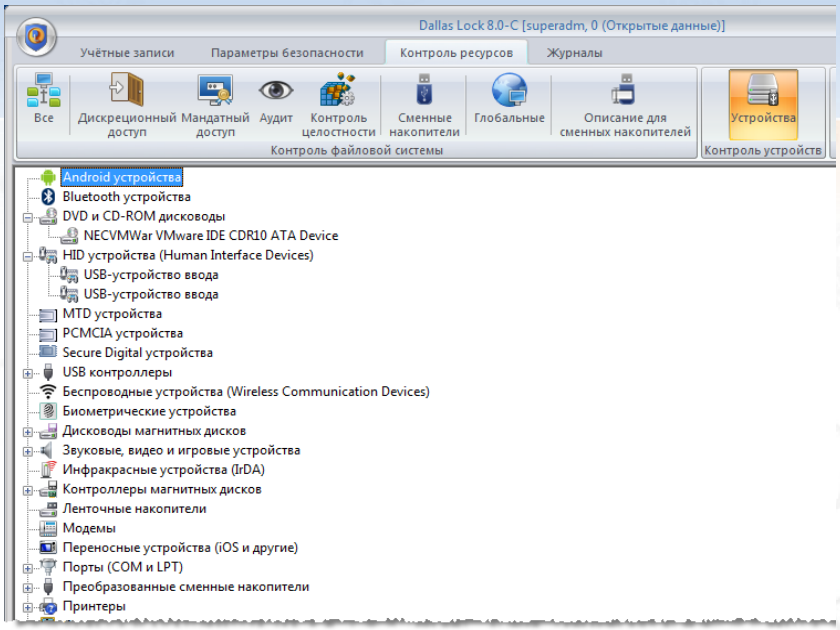
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Защита машинных носителей информации (ЗНИ)**	
Инструменты по реализации требований		• Контроль устройств: разграничение доступа к устройствам, аудит событий. • Преобразование жесткого диска, преобразование сменных накопителей. • СКН. Управление доступом к машинным носителям информации (ЗНИ.2). • СКН. Контроль подключения машинных носителей информации (ЗНИ.7)
Решения Dallas Lock	**СКН Dallas Lock 8.0**	



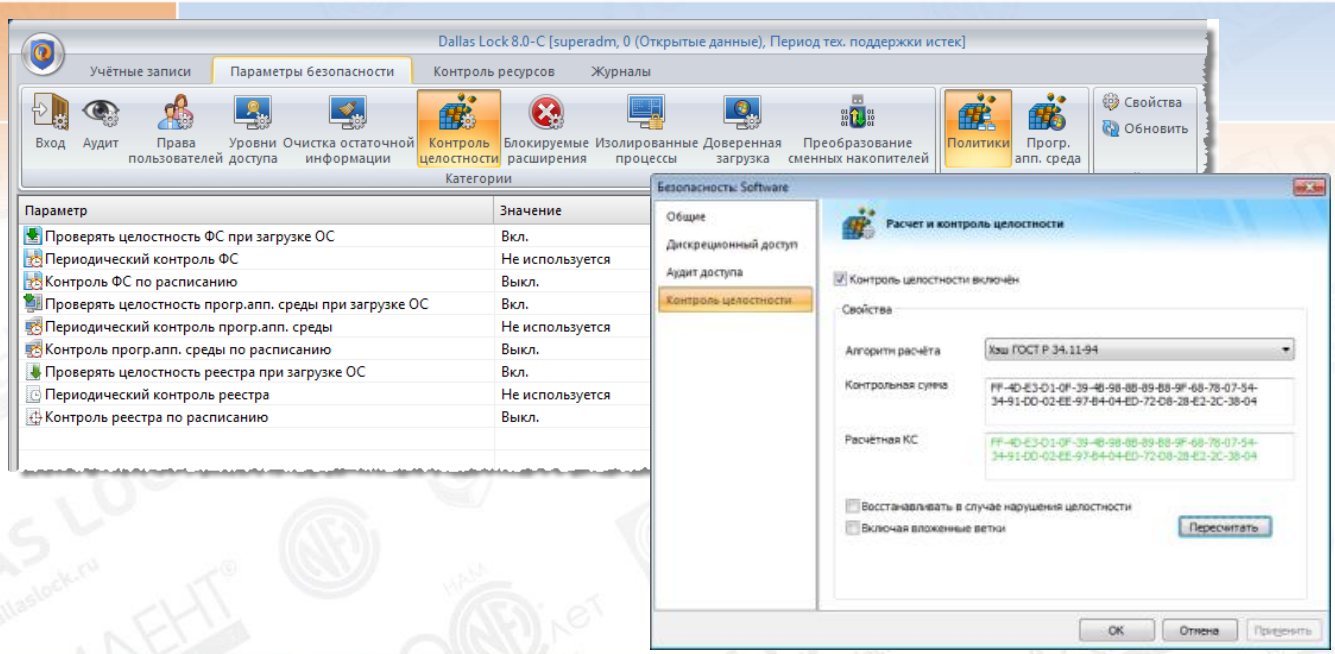
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Регистрация событий безопасности (РСБ)**
Инструменты по реализации требований	• Ведение журналов событий, настройку журналов
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



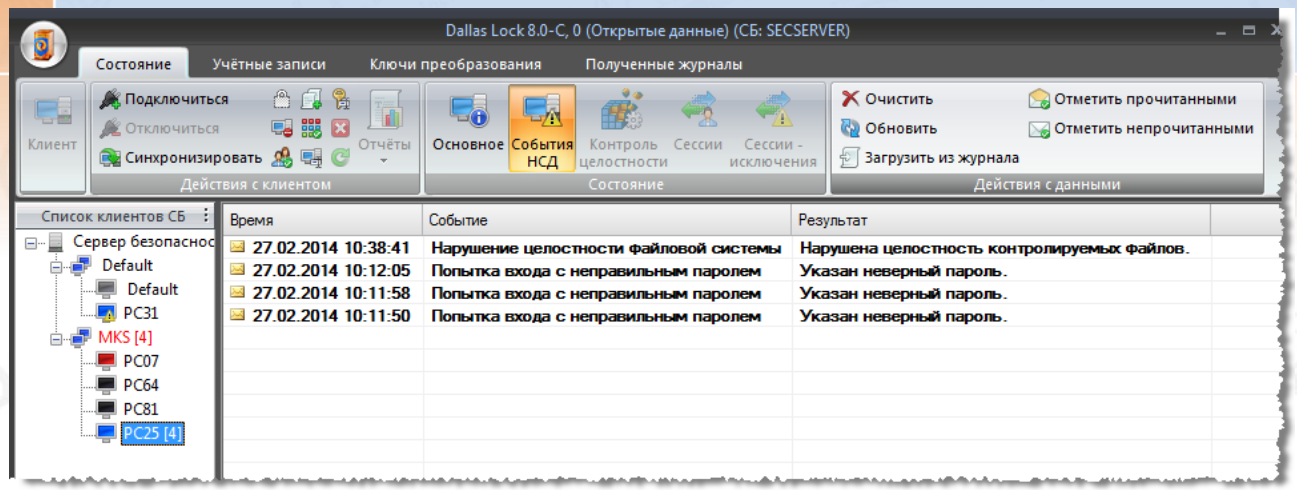
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Антивирусная защита (АВЗ)**	
Инструменты по реализации требований		• Обеспечение целостности: контроль целостности папок, файлов, веток реестра, восстановление файлов и реестра
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**	



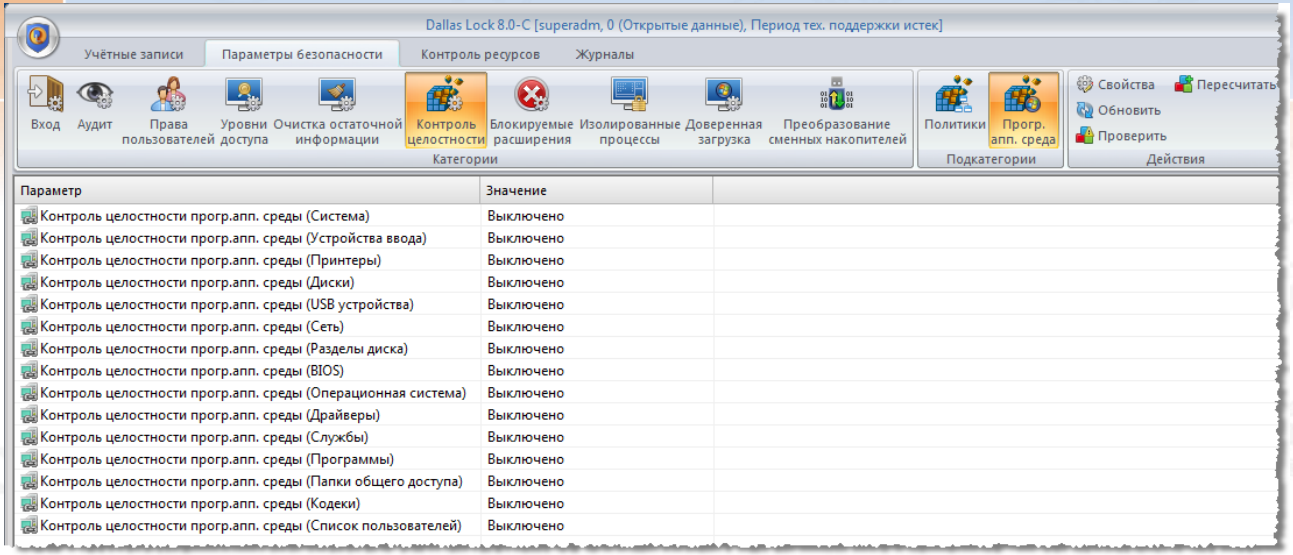
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Обнаружение вторжений (СОВ)**
Инструменты по реализации требований	• Сбор событий, связанных с безопасностью защищаемой системы, хранение информации о событиях. • Отслеживание модификаций объектов ФС и реестра. • Сигнализацию событий НСД, нарушения целостности; блокировку ПК. • Обнаружение и предотвращение сетевых атак
Решения Dallas Lock	**СОВ Dallas Lock 8.0**



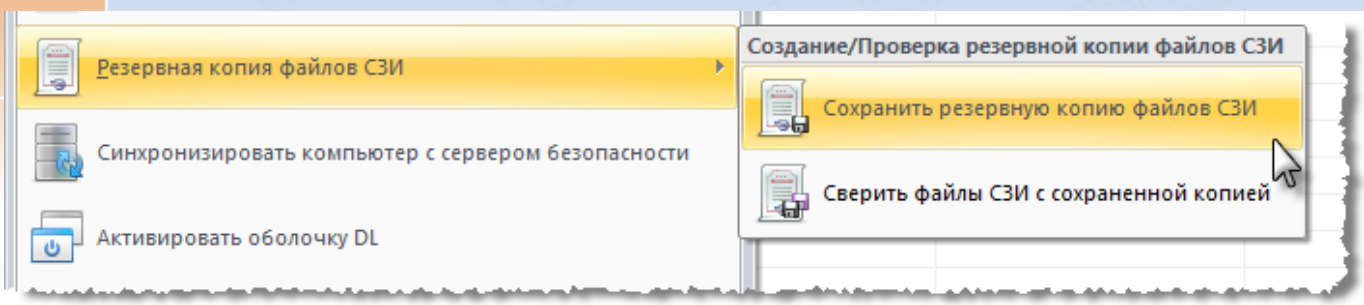
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Контроль (анализ) защищенности информации (АНЗ)**
Инструменты по реализации требований	• Контроль целостности программных средств СЗИ НСД и отдельно назначенных объектов, проверка целостности. • Самотестирование механизмов защиты СЗИ
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



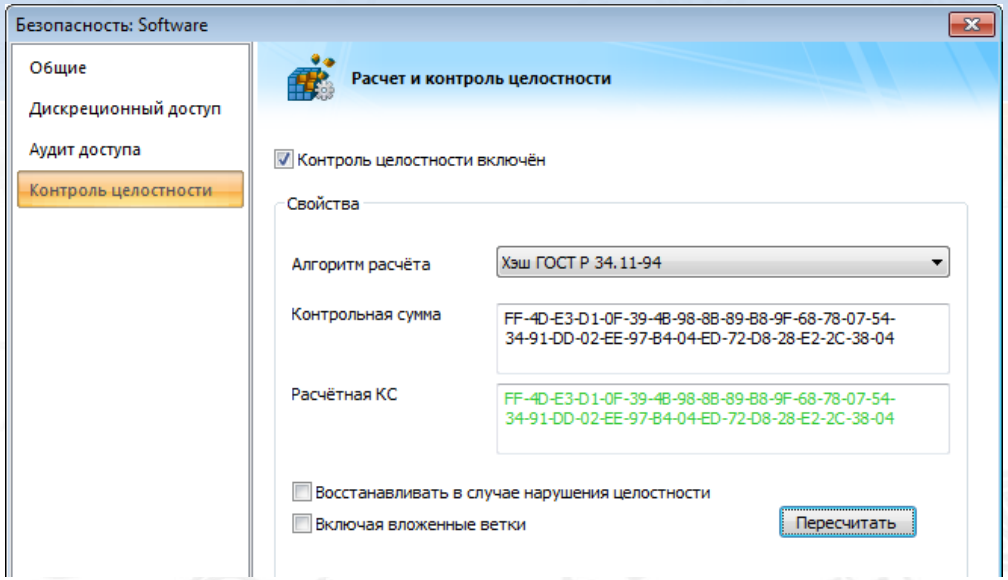
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Обеспечение целостности информационной системы и информации (ОЦЛ)**
Инструменты по реализации требований	• Назначение и проверка целостности объектов (ФС и реестра) различными способами. • Сохранение резервной копии файлов СЗИ НСД
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



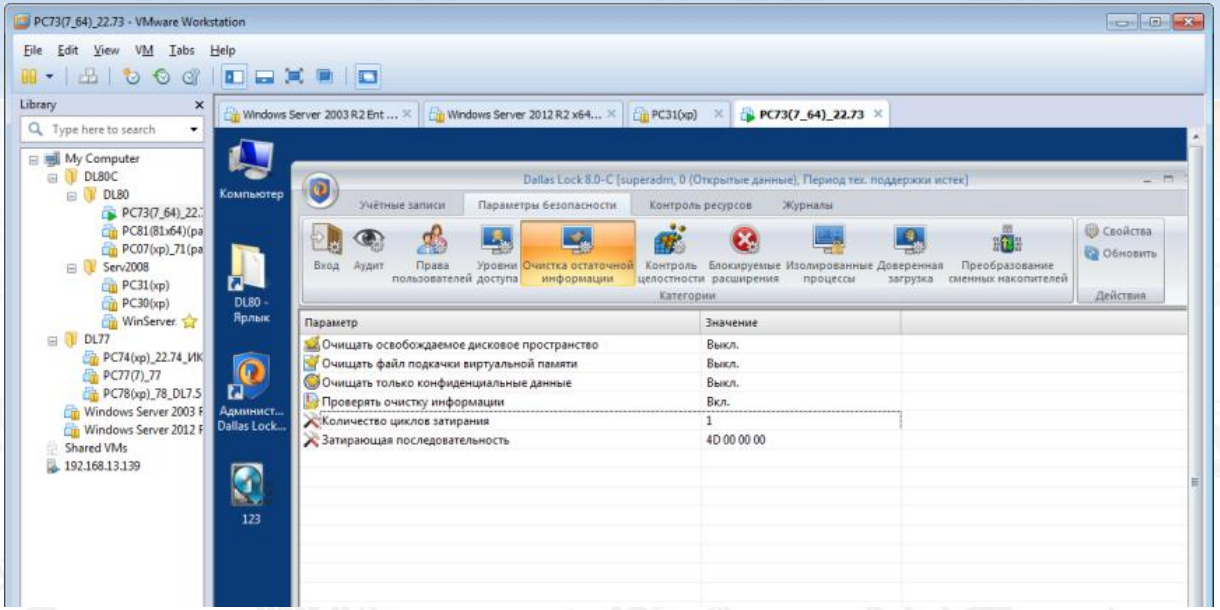
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Обеспечение доступности информации (ОДТ)**
Инструменты по реализации требований	• Восстановление файлов в случае обнаружения нарушения целостности. • Реплицирование серверов безопасности
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



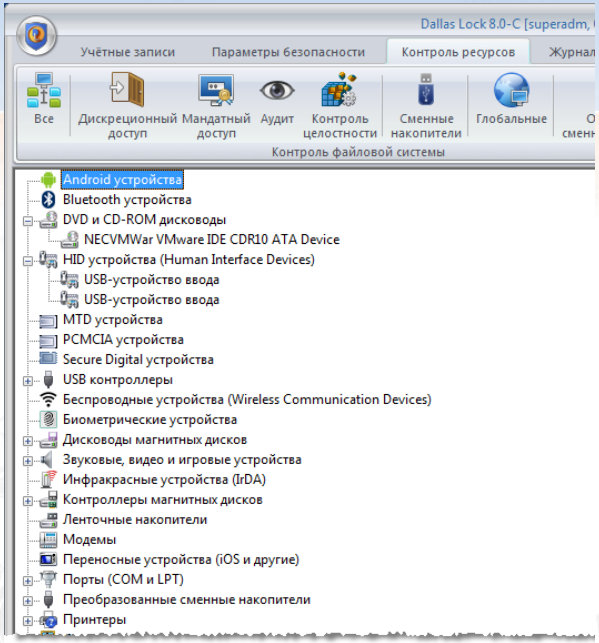
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Защита среды виртуализации (ЗСВ)**
Инструменты по реализации требований	• Полноценное управление доступом внутри виртуальных машин • Управление доступом к объектам виртуальной инфраструктуры (гипервизор, виртуальные машины и т. д.)
Решения Dallas Lock	**СЗВИ Dallas Lock**



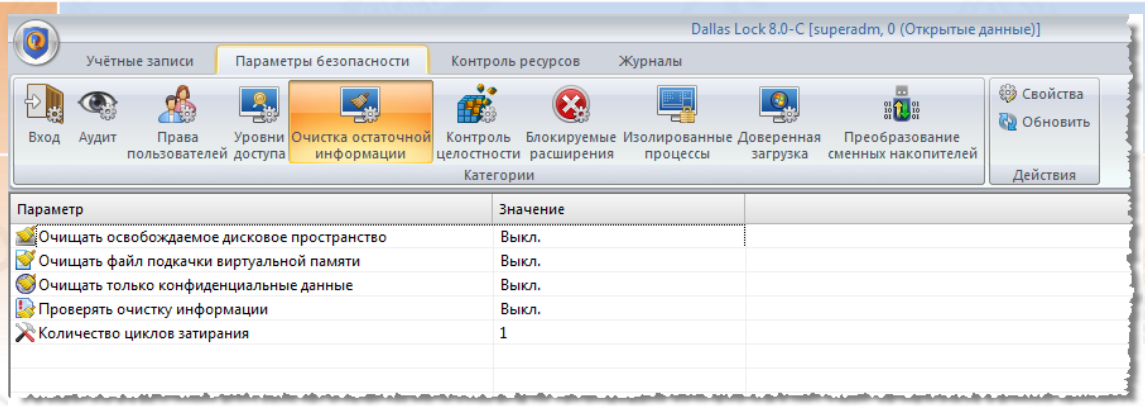
ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Защита технических средств (ЗТС)**
Инструменты по реализации требований	• Защита от утечек информации путем разграничения доступа к устройствам
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux**



ВОЗМОЖНОСТЬ ВЫПОЛНЕНИЯ МЕР ПО ЗИ ПРИКАЗОВ ФСТЭК РОССИИ № 21, 17 И 31

Требования при построении КСЗИ в ГИС (группы мер)	**Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)**
Инструменты по реализации требований	• Защита путем контроля целостности объектов. • Изоляция процессов (выполнение программ) в выделенной области памяти. • Очистка остаточной информации различными способами для различных данных: оперативной памяти, конфиденциальной информации, объектов ФС. • Защита мобильных тех. средств: поддерживается работа на планшетах с Windows 8, 8.1
Решения Dallas Lock	**СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ)** **СЗИ НСД Dallas Lock Linux** **МЭ Dallas Lock**



Вопросы?

Спасибо за внимание!

ООО «Конфидент»
Центр защиты информации

192029, г. Санкт-Петербург,
пр. Обуховской Обороны, д. 51, лит. К
Тел.: +7 (812) 325-10-37 (многоканальный)