СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK

Особенности применения современных СЗИ НСД для обеспечения ИБ банков. Dallas Lock. Новые возможности

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Год основания – 1992 г.
Персонал – более 200 человек

Первая в России негосударственная организация, получившая гос. лицензию на деятельность в области ЗИ

КОНФИДЕНТ®
CONFIDENT

Группа компаний «Конфидент» сегодня:

Инженерные системы

- Системы ОВК и ВК (отопление, вентиляция, кондиционирование, водоснабжение, водоотведение)
- Слаботочные системы и автоматизация зданий
- Системы противопожарной защиты
- Системы ЭОМ (электроснабжение, электроосвещение)

Сервисный центр

- Техническое обслуживание систем пожарно-охранной безопасности и инженерных систем
- Приемка в эксплуатацию
- Ремонт и модернизация
- Аварийные работы КРУГЛОСУТОЧНО
- Поставка оборудования и материалов

Информационная безопасность

Центр защиты информации (ЦЗИ)

- Разработка и продвижение линейки Dallas Lock
- Управление партнерской сетью ЦЗИ – более 300 партнеров по всей территории России

Конфидент–Интеграция (КИ)

- Консалтинговые услуги – аудит, анализ рисков, разработка документации,
- Интеграция в сфере ИБ – от проектирования комплексных систем ИБ до внедрения, сопровождения

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Лицензии и сертификаты для осуществления деятельности в области ИБ

Лицензии ФСБ России:

- на право работы со сведениями, составляющими государственную тайну, № 5168 от 30.09.2010 г.
- на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (действует бессрочно) № 801Н от 08.08.2013 г.
- на осуществление разработки и производства средств защиты конфиденциальной информации (действует бессрочно) № 13458К от 05.03.2014 г.

Лицензии ФСТЭК России:

- на проведение работ, связанных с созданием средств защиты информации, № 1101 от 06.10.2011 г.
- на деятельность по разработке и производству средств защиты конфиденциальной информации (переоформлена бессрочно) № 0016 от 31.10.2002 г.
- на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны № 1100 от 06.10.2011 г.
- на осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации (переоформлена бессрочно) № 0024 от 31.10.2002 г.
- на деятельность по разработке и производству средств защиты конфиденциальной информации (действует бессрочно) № 1062 от 19.11.2012 г.
- на деятельность по технической защите конфиденциальной информации (действует бессрочно) № 1877 от 19.11.2012 г.

Лицензия Минобороны России

- на деятельность в области создания средств защиты информации рег. № 1083 от 11.07.2014 г.

Сертификат менеджмента качества ISO 9001:2008

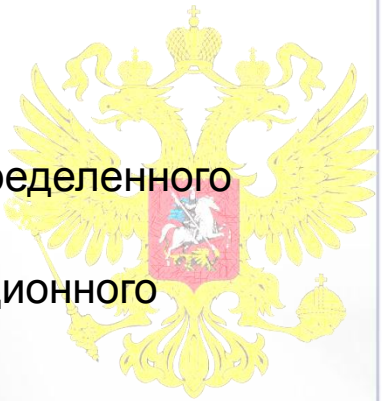
Особенности применения современных СЗИ НСД для обеспечения ИБ банков

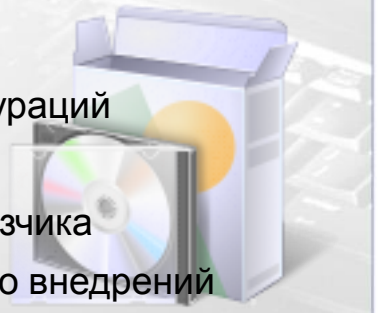
ЮРИДИЧЕСКИЕ АСПЕКТЫ

- Сертификаты регуляторов
- Возможность использования в АС, ГИС и при обработке ПДн определенного класса или уровня, для выполнения требований СТО БР
- История версий и продления сертификатов, проведения инспекционного контроля (ИК) производителем

ТЕХНИКО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

- Технологическое совершенство продукта
  - Развитость функционала (помимо требований РД)
  - Совместимость с другими технологиями и продуктами
  - Поддержка современных ОС и технологий
- Надежность, удобство, апробированность
  - Простота внедрения (развертывания) для различных конфигураций
  - Простота управления системой защиты
  - Стабильность работы и совместимость с приложениями заказчика
  - Масштаб проектов с использованием данной СЗИ, количество внедрений
  - Сроки присутствия решения на рынке и объектах заказчиков





Особенности применения современных СЗИ НСД для обеспечения ИБ банков

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

Ценовая политика. Совокупная стоимость владения (TCO):

- Первичное приобретение
- Внедрение
- Продление сопровождения
- Условия получения исправлений/обновлений по результатам ИК
- Условия обновления между версиями
- Затраты на развертывание и управление СЗИ собственными силами:
  - заработная плата для штата администраторов безопасности
  - потери от простоя на время неработоспособности СЗИ
  - простота и «незаметность» для пользователей и необходимость ресурсов для их обучения
- Обучение администраторов и пользователей СЗИ

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Dallas Lock – программный комплекс средств защиты информации (СЗИ) в ОС семейства **Windows**, в процессе её хранения и обработки, от несанкционированного доступа (НСД)

Функциональные особенности:

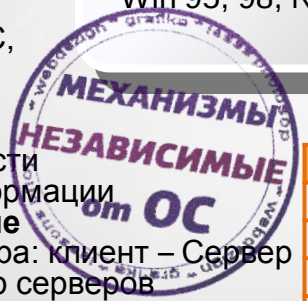
Аутентификация и разграничение доступа:
- Двухфакторная авторизация (пароль + идентификатор)
- Дискреционный и мандатный принципы разграничения доступа к объектам ФС и подключаемым устройствам
- Настройка ЗПС

Регистрация и учет событий:
- Аудит и ведение 6 журналов регистрации событий
- Добавление штампа на документы при печати
- Разграничение доступа к печат

Контроль целостности:
- Контроль целостности ФС, программно-аппаратной среды и реестра
- Блокировка загрузки ПК при нарушении целостности
- Очистка остаточной информации

Централизованное управление
- Трехуровневая архитектура: клиент – Сервер безопасности – Менеджер серверов

Дополнительный и уникальный функционал
- 4 способа преобразования информации
- Удаленное администрирование без СБ
- И прочее



Эволюционное развитие от замка на включение ПК под MS-DOS до современной распределенной системы:

DL 4.1, 5.0
- ✓ Аппаратно-программный комплекс для Win 95, 98, NT

DL 7.X
- ✓ 6.0 – Win 95, 98, ME
- ✓ 7.0 – Win 2003, XP
- ✓ 7.5 – Win 2000, 2003, XP централизованное управление
- ✓ 7.7 – + Win Vista, 2008, 7

DL 8.0-K, 8.0-C
- ✓ Добавлена поддержка x64; + Win 8, 8.1, 2012(R2)
- ✓ 8.0-K – для конфиденциальных данных (1Г)
- ✓ 8.0-C – до уровня «сов. секретно» (1Б)

Современные версии:

	8.0-K	8.0-C
Класс защищенности СВТ	**5**	**3**
Уровень контроля НДВ	**4**	**2**
Класс АС	до **1Г**	до **1Б**
Уровень ПДн	**1**	**1**
Класс ГИС	**1**	**1**
№ сертификата	№ 2720 от 25.09.2012 г.	№ 2945 от 16.08.2013 г.

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Пользователи Dallas Lock

- ФНС РФ
- МВД РФ
- ФСИН РФ
- ФСТЭК РФ
- ФТС РФ
- ФСКН РФ
- Роскомнадзор РФ
- Рособрнадзор РФ
- Росстат РФ
- 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 соц.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 «СибурТюменьГаз»
- ЗАО «Донэнергосбыт»
- ОАО «Владимирская областная электросетевая компания»
- 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 «Ангестрем»
- ФГУП «Росморпорт»
- ФГУП «ПО «Октябрь»
- ФГУП «ГосНИИПП» ФСТЭК РФ
- ФГУП «Гостехстрой» ФСТЭК РФ
- ОАО «Улан-Удэнский авиационный завод» («Вертолеты России») и другие

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Общие угрозы информационной безопасности:

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Группы мер по обеспечению ИБ, закрывающие угрозы:

* Группы мер составлены на основании приказов ФСТЭК России № 17 и № 21

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Выполнение мер по обеспечению ИБ средствами Dallas Lock:

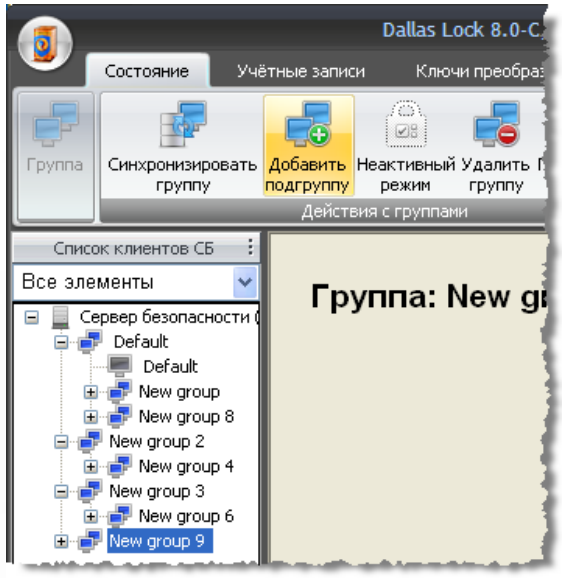
- Идентификация и аутентификация
- Обеспечение целостности информации
- Управление доступом
- Защита технических средств
- Обеспечение доверенной загрузки
- Защита от утечек информации
- Контроль и анализ защищенности информации
- Управление событиями
- Обеспечение доступности информации
- Гарантирован. уничтожение информации
- Антивирусная защита
- Защита виртуальной среды
- Защита мобильной среды
- Защита сетей передачи данных

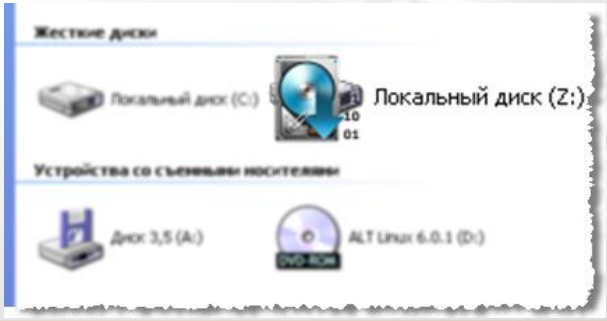
* Группы мер составлены на основании приказов ФСТЭК России № 17 и № 21

Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Обновления Dallas Lock 8.0 по результатам ИК 2014

- **Система уведомлений о сроке технической поддержки**. Действующая тех. поддержка - условие предоставления консультаций по установке и настройке СЗИ НСД, и доступа к сертифицированным обновлениям
- **Новый способы преобразования информации**. Создание средствами СЗИ НСД виртуальных дисков (любого размера на любых носителях) для преобразования информации (незаметно для пользователя) при работе на данных дисках
- **Использование внешних модулей, реализующих функции преобразования,** (сертифицированных и нет) при различных способах преобразования информации
- **Новые возможности централизованного управления средствами СБ:**
  - роль аудитора безопасности
  - управление доступом к сменным накопителям
  - многоуровневая иерархия групп клиентов



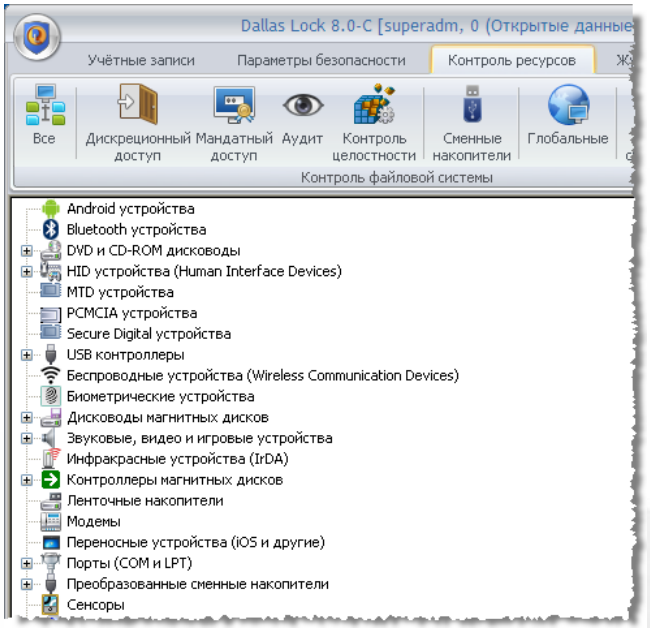


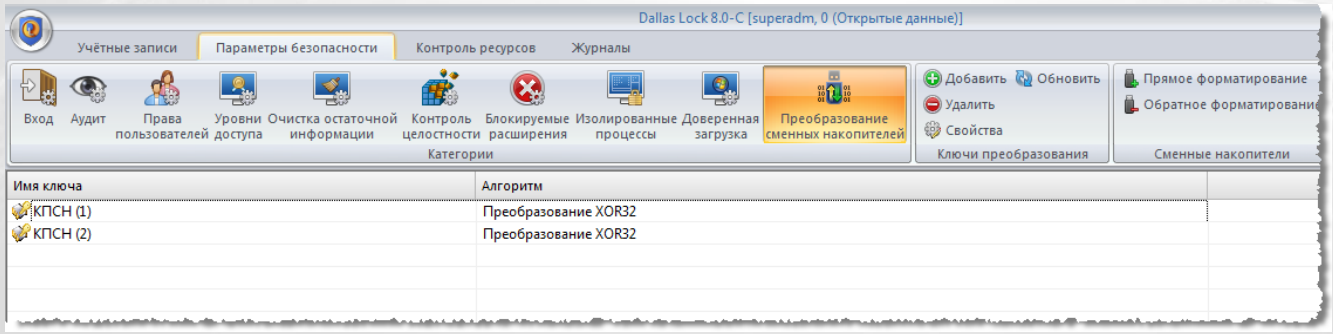
Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Обновления Dallas Lock 8.0 по результатам ИК 2014

Элементы DLP-систем в составе функционала Dallas Lock:

- Контроль устройств
- Теневое копирование файлов, отправляемых на печать
- Теневое копирование файлов, отправляемых на съемные носители
- Преобразование съемных носителей





Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Запланированные обновления Dallas Lock 8.0 на II-III квартал 2015

- **Сервер лицензий Dallas Lock**

Реализован для управления возможными лицензиями Dallas Lock и другими в пределах организации:

- Контроль числа использованных лицензий на СБ
- Контроль суммарного числа используемых в один момент времени терминальных подключений
- Мониторинг используемых лицензий (какой компьютер какую лицензию использует)
- Установка квот подключаемых DL-клиентов к СБ (возможность перераспределения максимально разрешенного количества DL-клиентов)
- Контроль использования в ИС реплицируемых (дублирующих) СБ

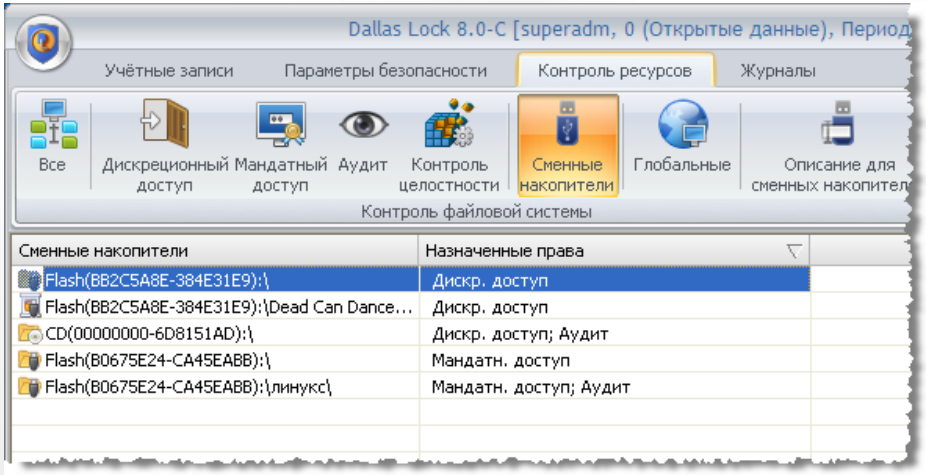
Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Запланированные обновления Dallas Lock 8.0 на II-III квартал 2015

- **Сертификация** на соответствие Требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации (Профиль защиты средств контроля подключения съемных машинных носителей информации **4** класса защиты)

Подсистема контроля съемных машинных носителей информации

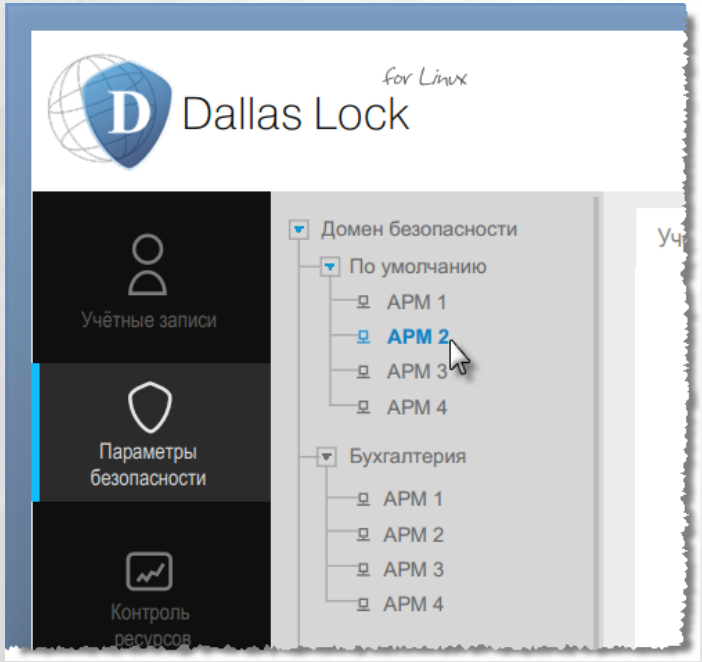
- Контроль подключения съемных носителей:
  - присвоение описания для экземпляров носителей
  - разграничение доступа к классам, к отдельным экземплярам, к объектам ФС на носителях
  - единое управление доступом к съемным носителям средствами СБ
  - аудит событий доступа к съемным носителям
  - сигнализация событий НСД к носителям
- Контроль отчуждения информации с носителей:
  - автоматическое теневое копирование файлов, отправляемых на носители
  - хранение и обработка информации на съемных носителях, помеченных как преобразуемые



Особенности применения современных СЗИ НСД для обеспечения ИБ банков

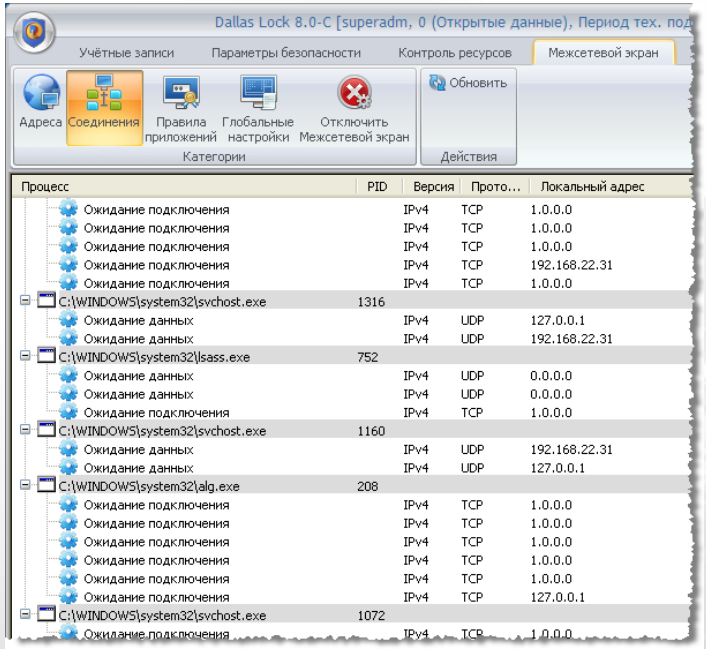
- **Dallas Lock для ОС Linux**

	DLL
Класс защищенности СВТ	**5**
Уровень контроля НДВ	**4**
Класс АС	до **1Г**
Уровень ПДн	**1**
Класс ГИС	**1**



- **Dallas Lock + персональный МЭ**

	МЭ
Класс защищенности СВТ	**3**
Уровень контроля НДВ	**4**
Класс АС	до **1Г**
Уровень ПДн	**1**
Класс ГИС	**1**



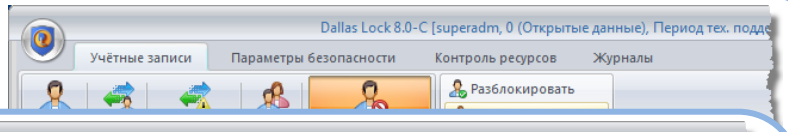
Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Соответствие требованиям СТО БР ИББС-1.0-2014

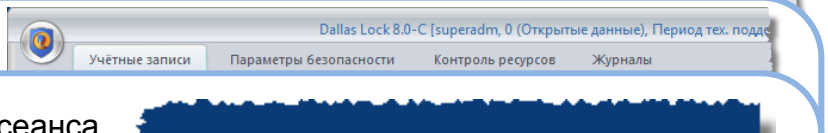
Возможность выполнения общих требований по обеспечению ИБ банковских технологических процессов, в рамках которых обрабатываются ПДн, средствами Dallas Lock 8.0

№	Наименование требования	Раздел Стандарта	Функционал в Dallas Lock 8.0
1	Идентификация, аутентификация, авторизация субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов)	7.4.3	
2	Разграничение доступа к информ… метода… с определением для ка… инф…		
3	Уп… чи… те…		* частично подразумевается МЭ
4	…		
5	…		
6	…		
7	…		
8	… повторной аутентификации и авторизации для продолжения работы		
9	Ограничение действий пользователей по изменению настроек их автоматизированных мест (ограничения на изменение BIOS)	7.4.3	✖

Управление свойствами каждой…

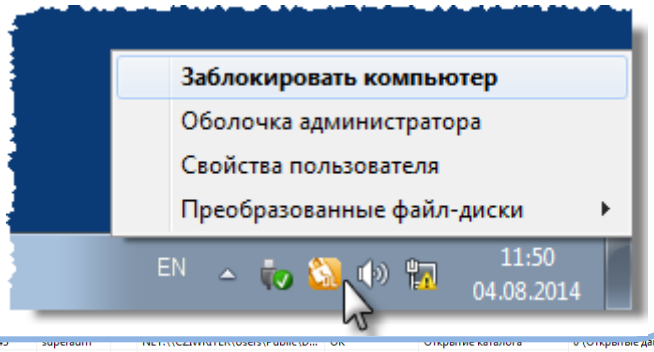


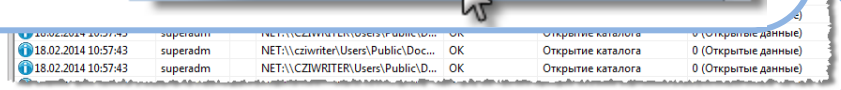
Блокир… запис… опред… собы… (неве… парол… опред… во ра…



Контрол… целостн…

Блокировка сеанса при бездействии (средствами Windows), блокировка сеанса пользователем через иконку Dallas Lock в системном трее





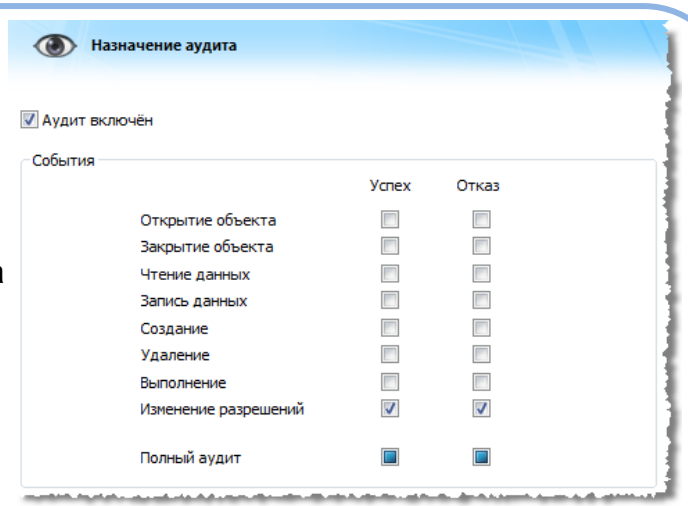
Особенности применения современных СЗИ НСД для обеспечения ИБ банков

Соответствие требованиям СТО БР ИББС-1.0-2014

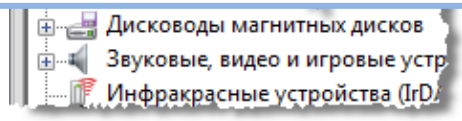
Возможность выполнения общих требований по обеспечению ИБ банковских технологических процессов, в рамках которых обрабатываются ПДн, средствами Dallas Lock 8.0

№	Наименование требования	Раздел Стандарта	Функционал в Dallas Lock 8.0
10	Управление составом разрешенных действий до выполнения идентификации и аутентификации	7.4.3	
11	Огран… АБС … изме…	…3	
12	Конт… инфо… соеди…	…	* частично подразумевается настройка сетевого оборудования
13	Выявление … числе баз …	…	* Частично
14	Контрол… в случае…	…	* установка на планшет, контроль съемных накопителей
15	Процед… «самоса…	…1.4	
16	Определ…	7.4.4	
17	Обеспечение генерации временных меток для регистрируемых действий и операций и синхронизации системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных	7.4.4	* Функция ОС

Возможность выбора определенных событий при настройке аудита



«Беспроводные устройства» (Wireless Communication Devices)



Особенности применения современных СЗИ НСД для обеспечения ИБ банков

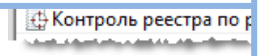
Соответствие требованиям СТО БР ИББС-1.0-2014

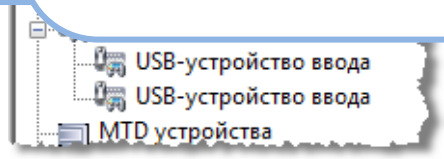
Возможность выполнения общих требований по обеспечению ИБ банковских технологических процессов, в рамках которых обрабатываются ПДн, средствами Dallas Lock 8.0

№	Наименование требования	Раздел Стандарта	Функционал в Dallas Lock 8.0
18	Определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн	7.11.6	+ орг.меры
19	Определ… О…	11.6	* частично
20			
21			* используется МЭ
22		6	* используется МЭ, СОВ
23	за… целостности		* используется СОВ
24	Опр… исполь… информации, с… информации	номеру и типу носителя	1.6
25	Определение, в… архивам ПДн	к	7.11.6 + орг.меры

В разделе «Контроль ресурсов», на вкладке «Устройства» возможно разграничение доступа к:

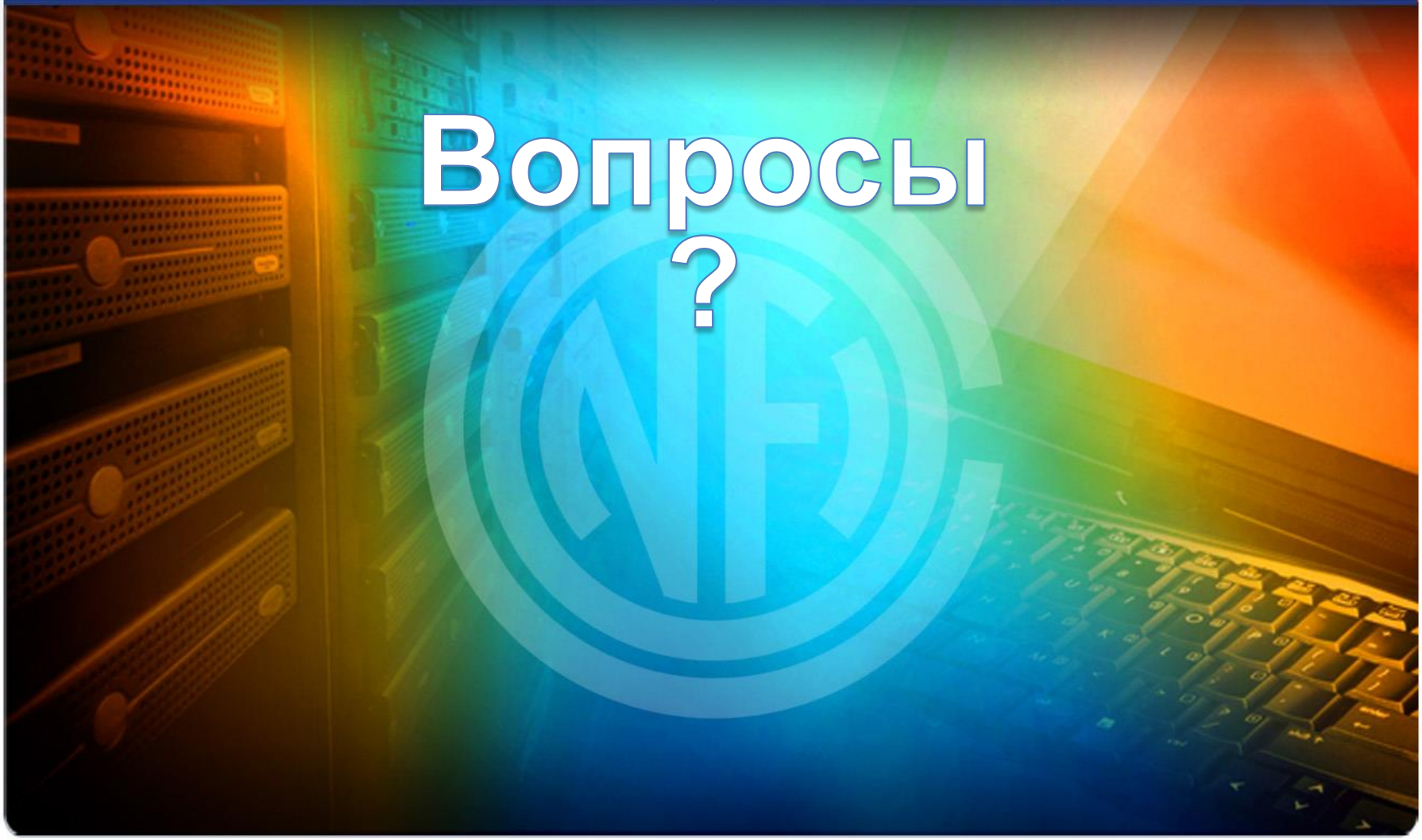
- «Secure Digital устройства»
- «Переносные устройства»
- «Сменные накопители» (CD ROM, FDD, USB-Flash)
- «HID-устройства» (Human Interface Device);
- «Порты» (COM и LPT)





Разграничение доступа к архивированным данным в электронном виде:

- Защита носителя информации (преобразование)
- Контроль доступа к объектам (файлам и папкам)


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)