МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени М.Т. Калашникова»

Кафедра «Защита информации в компьютеризованных системах»

Отчёт по курсовой работе

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем »

на тему: «Изучение системы защиты информации от несанкционированного доступа Dallas Lock 8.0. Подсистема управления доступом»

Выполнил:

студент группы С09-361-1

Якимов Ю.А.

Проверил:

к.т.н, доцент

Стукалина Е. Ф.

Ижевск 2017

**Содержание**

[**Введение** 3](#_Toc500417448)

[**1.** **Назначение и возможности системы защиты** 4](#_Toc500417449)

[**1.1.** **Общее описание** 4](#_Toc500417450)

[**1.2.** **Функции** 5](#_Toc500417451)

[**1.3.** **Структура и составные модули.** 6](#_Toc500417452)

[**1.3.1.** **Программное ядро (Драйвер защиты).** 6](#_Toc500417453)

[**1.3.2.** **Подсистема администрирования.** 6](#_Toc500417454)

[**1.3.3.** **Подсистема управления доступом.** 7](#_Toc500417455)

[**1.3.4.** **Подсистема регистрации и учета.** 7](#_Toc500417456)

[**1.3.5.** **Подсистема идентификации и аутентификации.** 8](#_Toc500417457)

[**1.3.6.** **Подсистема гарантированной зачистки информации.** 8](#_Toc500417458)

[**1.3.7.** **Подсистема преобразования информации.** 8](#_Toc500417459)

[**1.3.8.** **Подсистема контроля устройств.** 8](#_Toc500417460)

[**1.3.9.** **Подсистема межсетевого экранирования.** 8](#_Toc500417461)

[**1.3.10.** **Подсистема контроля целостности.** 8](#_Toc500417462)

[**1.3.11.** **Подсистема восстановления после сбоев.** 8](#_Toc500417463)

[**1.3.12.** **Подсистема развертывания (установочные модули).** 8](#_Toc500417464)

[**1.4.** **Достоинства** 8](#_Toc500417465)

[**2.** **Установка системы защиты** 9](#_Toc500417466)

[**2.1.** **Требования к аппаратному и программному обеспечению** 9](#_Toc500417467)

[**2.2.** **Процедура установки системы защиты** 11](#_Toc500417468)

[**3.** **Настройка системы. Подсистема управления доступом** 16](#_Toc500417469)

[**3.1.** **Управление учетными записями** 16](#_Toc500417470)

[**3.1.1.** **Полномочия на управление учетными записями** 18](#_Toc500417471)

[**3.1.2.** **Создание и удаление локальных пользователей** 19](#_Toc500417472)

[**3.1.3.** **Создание и удаление групп пользователей** 26](#_Toc500417473)

[**3.1.4.** **Число разрешенных сеансов** 28](#_Toc500417474)

[**3.1.5.** **Смена пароля пользователя** 29](#_Toc500417475)

[**3.1.6.** **Сессии-исключения** 31](#_Toc500417476)

[**3.2.** **Заблокированные пользователи** 33](#_Toc500417477)

[**3.3.** **Параметры входа** 34](#_Toc500417478)

[**3.3.1.** **Разрешение и запрет интерактивного и удаленного входов в ОС** 34](#_Toc500417479)

[**3.3.2.** **Настройка параметров входа** 35](#_Toc500417480)

[**4.** **Эксплуатация системы защиты** 41](#_Toc500417481)

[**Заключение** 43](#_Toc500417482)

[**Список использованной литературы** 44](#_Toc500417483)

# **Введение**

С каждым годом увеличивается количество информации, растет ее спрос, а значит и растет ее ценность, в связи с этим возрастают требования по ее защите. Так же быстрыми темпами совершенствуются компьютерные технологии. Из-за ежегодного обновления компьютерных технологий возникают новые угрозы для информации. Следовательно, возрастет необходимость ее защиты. Для того чтобы защита была полной необходимо прорабатывать ее комплексно.  
Утечка любой информации может отразиться на деятельности организации, предприятия. Особую роль играет конфиденциальная информация, потеря которой может повлечь большие изменения в самой организации и материальные потери. Поэтому мероприятия по защите информации в данное время очень актуальны и важны.

Для обеспечения полноценной защиты конфиденциальной информации необходимо проводить комплексный анализ каналов утечки, каналов и методов несанкционированного воздействия на информацию. Одним из многих средств защиты информации является Dallas Lock 8.0.

1. **Назначение и возможности системы защиты**
   1. **Общее описание**

Система защиты информации от несанкционированного доступа Dallas Lock 8.0 предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему и выходящими за её пределы, обеспечения защиты информации в АС посредством её фильтрации. Система защиты Dallas Lock 8.0 представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов. Использование системы защиты Dallas Lock 8.0 в проектах по защите информации позволяет привести автоматизированные системы в соответствие требованиям законодательства Российской Федерации. Система защиты предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (файловых, контроллерах домена и терминального доступа). Может функционировать как на автономных персональных компьютерах, так и на компьютерах в составе локально-вычислительной сети, в том числе под управлением контроллера домена. Система защиты Dallas Lock 8.0 обеспечивает защиту информации от несанкционированного доступа на ПК в ЛВС через локальный, сетевой и терминальный входы. Также обеспечивает разграничение полномочий пользователей по доступу к файловой системе, устройствам и другим ресурсам компьютера. Разграничения касаются всех пользователей – локальных, сетевых, доменных, терминальных.

* 1. **Функции**

Программные средства защиты информации, функционирующие в составе СЗИ Dallas Lock, позволяют:

 управлять доступом к электронным ресурсам;

 разграничение доступа к внешним накопителям, как по типам, так и по конкретным экземплярам;

 использовать электронные индефикаторы;

 контролировать сложность и использование паролей;

 авторизовать пользователя до загрузки операционной системы;

 ограничивать круг доступных для пользователя элементов файловой системы

 осуществлять контроль целостности компонентов системы и параметров компьютера;

 использовать систему очистки остаточной информации;

 журналировать события раздельными списками, с контролем времени, пользователя и прочего;

 добавлять штампы на документы, сохранять теневые копии, разграничивать доступ пользователей к печати;

 шифровать данные, создавать файлы-контейнеры;

 осуществлять удалённое администрирование рабочих станций с установленным клиентом;

 использовать механизм блокировки компьютера;

 создавать «Замкнутую программную среду»;

 блокировать доступа к файлам по расширению;

 осуществлять резервное копирование информации.

* 1. **Структура и составные модули.**

Система защиты Dallas Lock 8.0 состоит из следующих основных компонентов:

* + 1. **Программное ядро (Драйвер защиты).**

Является ядром системы защиты и выполняет основные функции СЗИ НСД:

* обеспечивает мандатный (для редакции «С») и дискреционный режимы контроля доступа к объектам файловой системы и устройствам;
* обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
* обеспечивает работу механизма делегирования полномочий;
* обеспечивает проверку целостности СЗИ НСД, объектов ФС, программно-аппаратной среды и реестра;
* драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД.

Драйвер защиты автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие. С драйвером защиты взаимодействуют защитные подсистемы, перечисленные ниже.

* + 1. **Подсистема администрирования.**

Включает в себя:

* подсистему локального администрирования. Обеспечивает возможности по управлению СЗИ НСД, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс Windows Explorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования.
* подсистему удаленного администрирования. Позволяет выполнять настройку системы защиты с удалённого компьютера.
* подсистему централизованного управления. Включает в себя основные компоненты:
* модуль «Сервер безопасности», который позволяет объединять защищенные компьютеры в Домен безопасности для централизованного и оперативного управления клиентами;
* модуль «Менеджер серверов безопасности», который позволяет объединить несколько серверов безопасности в единую логическую единицу – «Лес безопасности».
  + 1. **Подсистема управления доступом.**

Включает в себя:

* подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов;
* подсистему доступа к файловой системе, реестру и устройствам, в составе которой:

1. подсистема дискреционного доступа;
2. подсистема мандатного доступа (для редакции «С»);

* модуль доверенной загрузки уровня загрузочной записи (для редакции «C»). Является опционным модулем, включается по команде администратора и может быть не активированным. Активный модуль отрабатывает до начала загрузки ОС.
  + 1. **Подсистема регистрации и учета.**

Включает в себя:

* подсистему аудита. Обеспечивает ведение аудита и хранение информации 8-ми категорий событий в журналах;
* подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.
  + 1. **Подсистема идентификации и аутентификации.**

Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему;

* + 1. **Подсистема гарантированной зачистки информации.**

Обеспечивает зачистку остаточной информации.

* + 1. **Подсистема преобразования информации.**
    2. **Подсистема контроля устройств.**

Обеспечивает возможность разграничения доступа к подключаемым на ТС устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

* + 1. **Подсистема межсетевого экранирования.**

Обеспечивает контроль, а также фильтрацию потоков информации, поступающих в автоматизированную систему и выходящих за её пределы.

* + 1. **Подсистема контроля целостности.**

Обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД, восстановление файлов и веток реестра в случае нарушения их целостности.

* + 1. **Подсистема восстановления после сбоев.**
    2. **Подсистема развертывания (установочные модули).**
  1. **Достоинства**
* система полностью сертифицирована;
* производителем заявлен дружественный интерфейс;
* простота установки и настройки;
* высокая надёжность и стабильность системы благодаря встроенной системе резервного копирования собственных файлов;
* подробная документация;
* постоянная поддержка разработчиком.

1. **Установка системы защиты**
   1. **Требования к аппаратному и программному обеспечению**

Система защиты Dallas Lock 8.0 может быть установлена на персональные компьютеры, портативные и мобильные ПК (ноутбуки и планшетные ПК), сервера (файловые, контроллеры домена, терминального доступа) и виртуальные машины (например, VMware), работающие как в автономном режиме, так и в составе локально-вычислительной сети. Система защиты Dallas Lock 8.0 может работать на любом компьютере, работающем под управлением следующих ОС:

* Windows XP (SP 3) (Professional, Home, Starter);
* Windows Server 2003 (R2) (SP 2) (Web, Standard, Enterprise, Datacenter);
* Windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
* Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
* Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
* Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
* Windows 8 (Core, Pro, Enterprise);
* Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
* Windows 8.1 (Core, Pro, Enterprise);
* Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
* Windows 10.

Система защиты Dallas Lock 8.0 поддерживает 32- и 64-битные версии ОС Windows1. Система защиты Dallas Lock 8.0 позволяет защищать информационные ресурсы рабочего пространства Windows To Go операционной системы Windows 8 на USB-накопителе. Минимальная и оптимальная конфигурация ПК определяется требованиями к версии операционной системы Windows, на которую установлена система защиты Dallas Lock 8.0.

Для размещения файлов системы и ее работы требуется не менее 30 Мбайт пространства на системном разделе жесткого диска. Для использования Dallas Lock 8.0 на компьютере в составе ЛВС необходимо настроить сетевой протокол TCP/IP. Для использования аппаратных идентификаторов требуется наличие в аппаратной части ПК соответствующих портов: USB-порта или COM-порта.

* 1. **Процедура установки системы защиты**

1. Для установки СЗИ НСД Dallas Lock 8.0 необходимо запустить приложение DallasLock8.0С.msi (DallasLock8.0K.msi), которое находится в корневой директории дистрибутива (или выбрать данное действие в меню окна autorun. Рис.1, рис.2).

Если Dallas Lock 8.0 устанавливается на ПК, не оснащенный приводом компакт дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с инсталляционного диска на данный ПК необходимый msi-файл любым удобным способом: через ЛВС, USB Flash-накопитель и др. После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге инсталляции предоставляется возможность отмены инсталляции с возвратом сделанных изменений. Для этого служит кнопка «Отмена». Выполнение следующего шага инсталляции выполняется с помощью кнопки «Далее**».**

****

Рис.1 – Окно autorun.



Рис.2 – Окно autorun с выбором установки.

1. При установке системы защиты на компьютере с установленной ОС Vista и выше после запуска приложения, на экране будет выведено окно для подтверждения операции (Рис.3).



Рис.3 – Разрешение на установку программы в ОС.

После подтверждения запустится программа установки СЗИ НСД Dallas Lock 8 (Рис. 4).

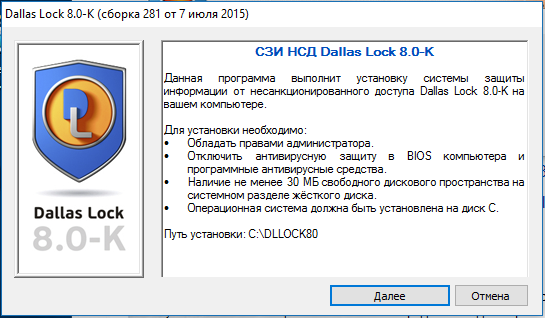


Рис.4 – Окно начала установки системы защиты.

1. Для установки необходимо нажать кнопку «Далее», после чего программа установки приступит к инсталляции. На данном этапе программа установки попросит осуществить ввод параметров установки (Рис.5).

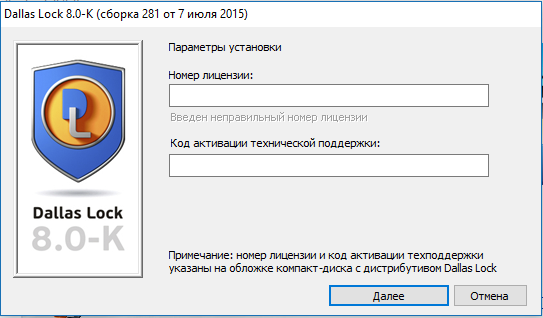


Рис.5 – Ввод параметров установки.

1. Для защиты от нелегального использования продукта необходимо ввести номер лицензии Dallas Lock 8.0 и код технической поддержки, которые указаны на обложке компакт-диска с дистрибутивом в соответствующих полях. Следует обратить внимание, что номер лицензии может либо активировать модуль «Межсетевой экран», либо оставлять его неактивным (в зависимости от приобретенного изделия). После этого необходимо нажать кнопку «Далее».

**Примечание.** Поле «Код технической поддержки» не является обязательным при установке СЗИ НСД, но является обязательным при обновлении. При установке без использования кода технической поддержки его необходимо ввести в процессе эксплуатации СЗИ НСД (нажать кнопку основного меню и выбрать пункт «О программе», в появившемся окне нажать «Сменить номер лицензии»). Так же в появившемся окне можно изменить номер лицензии. Следует обратить внимание, что при активном модуле «Межсетевой экран» в случае ввода номера лицензии для изделия без модуля «Межсетевой экран», на экран будет выведено предупреждение и соответствующий модуль будет деактивирован. Действующий код технической поддержки является условием предоставления помощи в установке и настройке СЗИ НСД специалистами компании-разработчика, а также условием доступа к сертифицированным обновлениям. При завершении срока технической поддержки при запуске модулей администрирования будет появляться предупреждающее сообщение.

1. В том случае, когда необходимо ввести компьютер в Домен безопасности в процессе установки системы, то в соответствующие поля необходимо ввести имя Сервера безопасности и его ключ доступа. Если этого не сделать на этапе установки, то компьютер не будет введен в Домен безопасности, но это можно будет сделать и после установки СЗИ НСД.

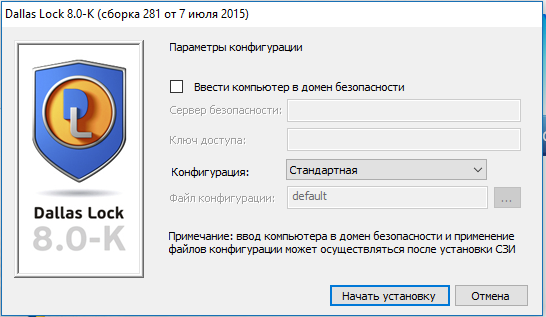


Рис.6 – Введение в домен безопасности на этапе установки.

1. Указать, если требуется, файл конфигурации, для этого нажать кнопку поиска рядом с полем ввода и в появившемся окне проводник выбрать заранее сохраненный файл.
2. После нажатия кнопки «Далее» процесс установки системы защиты будет завершен. После нажатия кнопки «Перезагрузка» через 30 секунд произойдет автоматическая перезагрузка ПК (Рис.7).

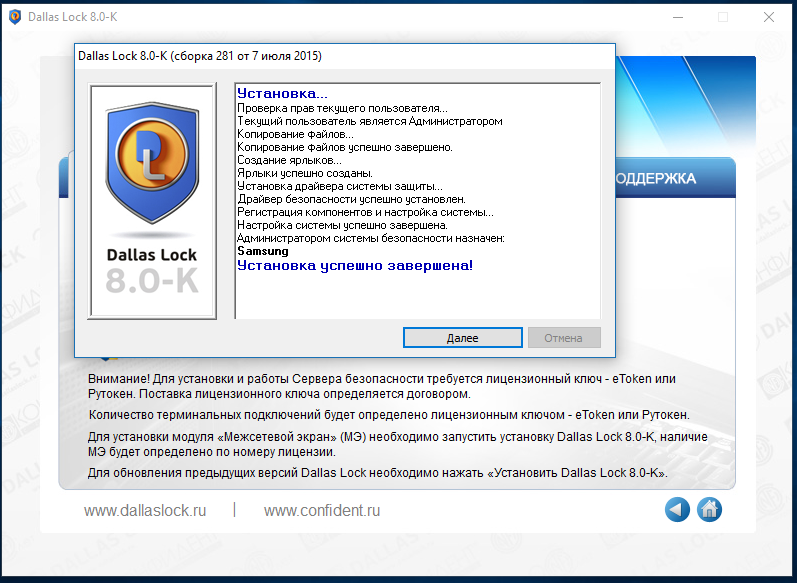


Рис.7 – Завершение установки программы.

После перезагрузки первый вход на защищенный компьютер сможет осуществить пользователь, под учетной записью которого выполнялась инсталляция системы защиты Dallas Lock 8.0. Это может быть локальный пользователь ОС, доменный пользователь, если компьютер является клиентом контроллера домена или учетная запись Windows Live ID (Windows 8 и выше). Во время первого входа на защищенный компьютер после загрузки ОС появится всплывающее сообщение о том, что данный компьютер защищен Dallas Lock 8.0. После установки системы защиты и перезагрузки компьютера в меню «Пуск» появится ярлык оболочки администратора СЗИ НСД Dallas Lock 8.0.

1. **Настройка системы. Подсистема управления доступом**
   1. **Управление учетными записями**

В СЗИ НСД Dallas Lock 8.0 возможна регистрация пользователей следующих видов:

**1.** Пользователей, созданных средствами ОС Windows на данном локальном компьютере.

**2.** Пользователей, созданных средствами СЗИ НСД.

**3.** Пользователей, созданных средствами службы Active Directory (если компьютер находится в ЛВС под управлением Контроллера домена).

Пользователи, зарегистрированные в операционной системе Windows, автоматически не становятся зарегистрированными пользователями в системе защиты Dallas Lock 8.0 и не могут работать на защищенном компьютере. В то же время при создании нового пользователя в системе защиты он автоматически становится пользователем ОС. Процесс регистрации будет описан ниже.

Для просмотра и редактирования учетных записей пользователей в оболочке администратора системы защиты необходимо выбрать вкладку «Учетные записи» (Рис.8):

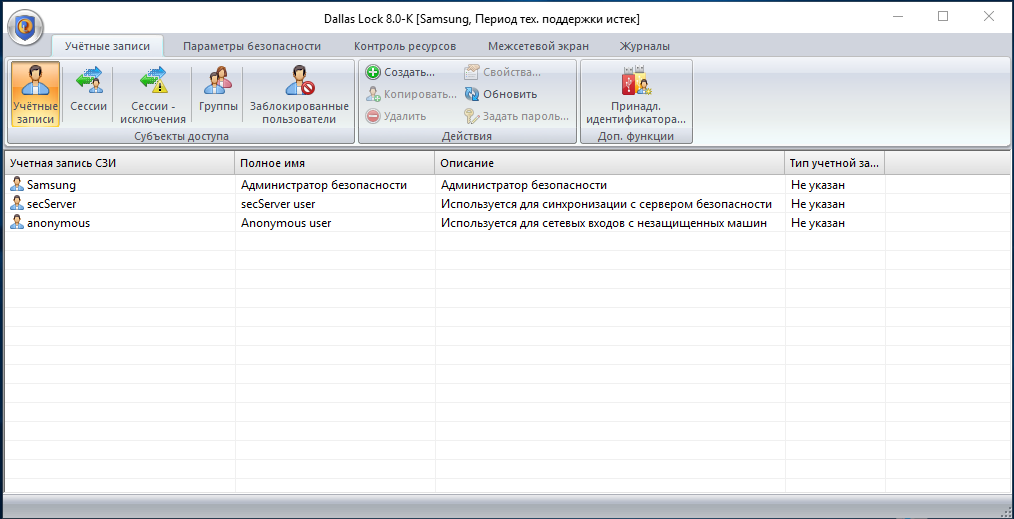
****

Рис.8 –Вкладка Учетные записи.

Число зарегистрированных пользователей на каждом защищенном компьютере ограничивается только размером свободного дискового пространства. Один пользователь может быть зарегистрирован на нескольких ПК. По умолчанию в системе защиты Dallas Lock 8.0 всегда присутствуют следующие учетные записи:

• **Суперадминистратор** − учетная запись пользователя, установившего СЗИ НСД (запись невозможно удалить из системы);

• **anonymous** − учетная запись для проверки входов с незащищенных системой машин (запись невозможно удалить из системы, но можно отключить, при этом следует помнить, что учетная запись anonymous на контроллере домена всегда должна быть включена);

• **secServer** − через эту учетную запись Сервер безопасности подключается к данному ПК и проводит оперативное управление (запись невозможно удалить из системы, но можно отключить);

• **\*\\*** − специальная учетная запись, разрешающая всем доменным пользователям вход на защищенный системой компьютер. Создаётся только на ПК, которые в момент установки СЗИ НСД входят в домен Active Directory. Запись можно удалить или отключить.

Зарегистрированные, но отключенные учетные записи выделяются иконкой . Пользователь, установивший систему защиты, обладает всеми полномочиями администрирования (управления) системы защиты и всеми правами по доступу к ресурсам, причем эти права и полномочия в дальнейшем невозможно ограничить. Суперадминистратор регистрирует в системе защиты других пользователей. При этом он может делегировать зарегистрированному пользователю все или часть своих полномочий на администрирование.

* + 1. **Полномочия на управление учетными записями**

Регистрировать и удалять пользователей, а также просматривать и редактировать учетные записи может только пользователь, наделенный соответствующими полномочиями по администрированию.

Полномочиями для создания, удаления и изменения учетных записей пользователей в системе защиты обладают: суперадминистратор и пользователи (группы пользователей), указанные в списке разрешенных параметра «Учетные записи: Управление» на вкладке «Права пользователей» (Рис.9). По умолчанию это администраторы.

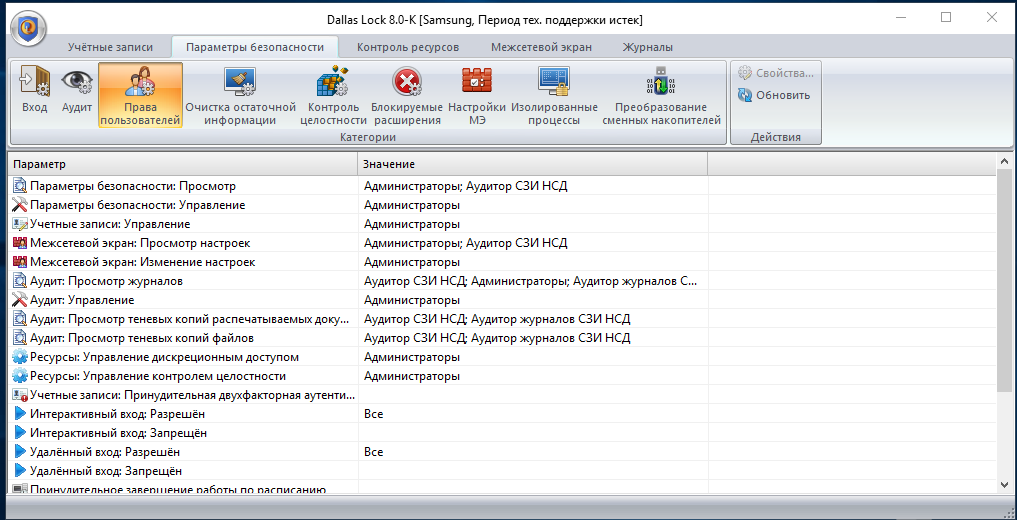


Рис.9 –Параметр, определяющий полномочия на управление учетными записями.

* + 1. **Создание и удаление локальных пользователей**
       1. **Создание пользователей**

Перед созданием новой учетной записи необходимо убедиться в том, что нужная учетная запись еще не создана в операционной системе. В таком случае, достаточно будет ее просто зарегистрировать, выбрав из списка, вызываемого кнопкой поиска. Для создания нового пользователя в системе защиты необходимо:

**1.** Выделить категорию «Учетные записи» в оболочке администратора.

**2.** Нажать кнопку «Создать» в категориях «Действия» или выбрать соответствующую из контекстного меню, нажав правую кнопку мыши.

**3.** На экране появится окно создания новой учетной записи (Рис.10).

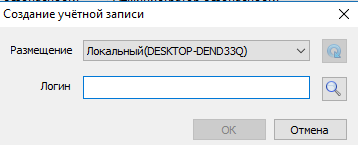


Рис.10 –Окно создания учетной записи.

**4.** В поле «Размещение» необходимо выбрать значение «Локальный».

**5.** В поле «Логин» необходимо ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:

• максимальная длина имени − 20 символов;

• имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ \*);

• разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

Кнопка поиска, расположенная рядом с полем логина, разворачивает список учетных записей пользователей, зарегистрированных в ОС данного ПК, и позволяет выбрать пользователя из уже существующих (Рис.11).

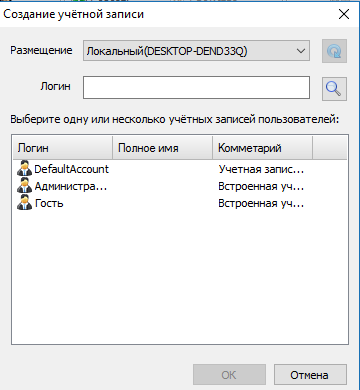


Рис.11 –Учетные записи, зарегистрированные в ОС компьютера.

Также можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

**6.** После нажатия «OK» появится окно редактирования параметров учетной записи (Рис. 12).

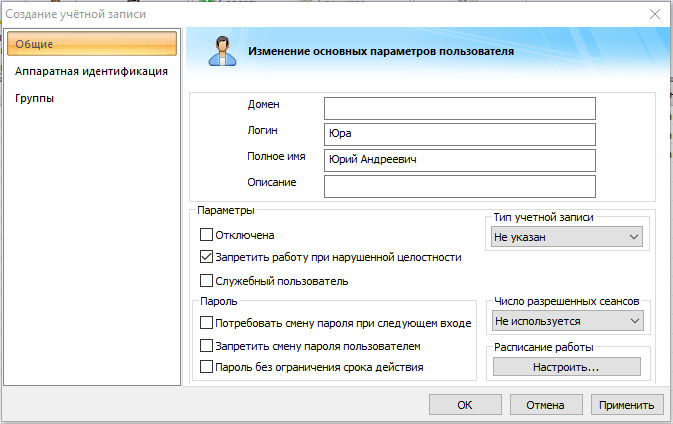


Рис.12 –Окно редактирования параметров новой учетной записи.

На вкладке «Общие» предлагается заполнить следующие учетные данные и параметры:

• заполнить **«Полное имя»** пользователя;

• в поле «**Описание**» ввести любой комментарий. Длина комментария не более 256 символов. Вводить комментарий и полное имя не обязательно.

Поле **«Логин»** и поле **«Домен»** остаются без возможности изменения (название домена для локального пользователя остается пустым).

• политики «**Отключена**» и «**Запретить работу при нарушении целостности**» задаются при необходимости: • Администратор имеет возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на защищенный компьютер до тех пор, пока администратор не деактивирует эту опцию.

• Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «Запретить работу при нарушении целостности» активизирована, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется. Если же эта опция не включена, то при обнаружении нарушения целостности будет отображено только предупреждение;

• флажок в поле «**Служебный пользователь**» предоставляет данной учетной записи особый статус;

• необходимо выбрать **«Тип учетной записи».** Для типа «Временный» обязательным условием является настройка расписания работы пользователя. По умолчанию тип учетной записи будет иметь значение «Не указан».

• необходимо выбрать «**Уровень мандатного доступа»** (только в Dallas Lock 8.0 редакции «С»)**,** под которым пользователь сможет работать (подробнее в разделе «Мандатный доступ»);

• необходимо выбрать значение в поле **«Число разрешенных сеансов»**;

• необходимо задать «**Расписание работы»** пользователя, выбрать период и время. Вне указанного периода пользователь не сможет зайти на защищенный ПК. Кроме того, по окончании времени работы ПК пользователя будет заблокирован при условии включения параметра безопасности «Принудительное завершение работы по расписанию» («Параметры безопасности» => «права пользователей»);

• отмеченный параметр «**Потребовать смену пароля при следующем входе**» единовременно запросит смену пароля при входе;

• поле «**Запретить смену пароля пользователем**»;

• флажок в поле «**Пароль без ограничения срока действия**» отменяет действие политики входа «Максимальный срок действия паролей», распространяемой на всех пользователей.

Далее, в процессе создания или регистрации нового локального пользователя администратор имеет возможность включить его в определенную группу. В окне закладки «Группы» отображены названия групп, в которые включен пользователь (Рис.13). По умолчанию, каждый новый пользователь входит в группу «Пользователи».

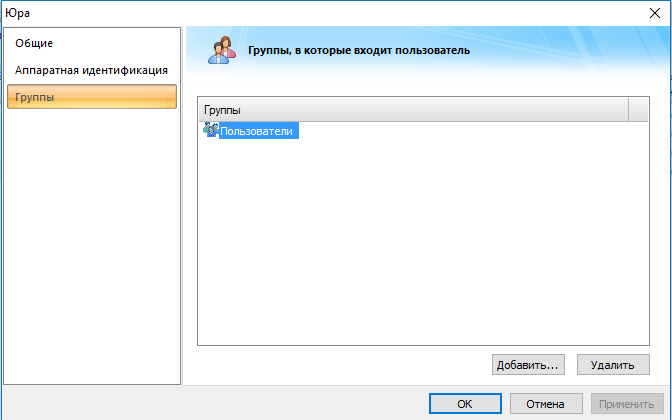


Рис.13 –Окно редактирование списка групп пользователя.

**7.** Чтобы включить пользователя в определенную группу необходимо нажать «Добавить». Появится список всех групп пользователей, имеющихся в системе (кроме тех, в которые пользователь уже включен) (Рис.14).

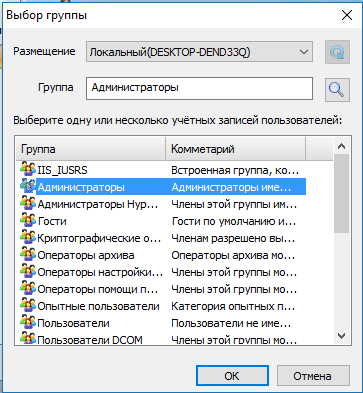


Рис.14 –Окно выбора групп для учетной записи.

**8.** В поле «Размещение» необходимо оставить значение «Локальный». В списке групп нужно выбрать необходимую. Одновременно можно выделить несколько групп в списке.

**9.** Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки «ОК» (Рис.15).

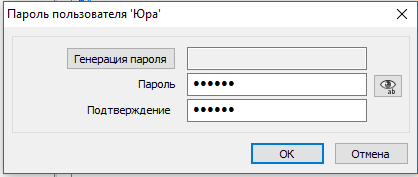


Рис.15 –Форма ввода пароля.

При вводе пароля необходимо руководствоваться следующими правилами:

• максимальная длина пароля 32 символа;

• пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;

• сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором.

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку с надписью «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение». Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

* + - 1. **Удаление пользователей**

Для удаления пользователя из системы защиты вне зависимости от того, какими средствами он создан или зарегистрирован в самой системе защиты, необходимо выделить его имя в списке главного окна программы, нажать кнопку «Удалить» или выбрать соответствующее действие из контекстного меню. Подтвердить операцию. Учетная запись будет удалена и из системы защиты и из операционной системы. Следует отметить, что при удалении самой системы защиты Dallas Lock 8.0 с компьютера, учетные записи пользователей, созданные средствами системы защиты через оболочку администратора, остаются в операционной системе, как и учетные записи, созданные в ОС и зарегистрированные в системе защиты.

* + - 1. **Создание учетной записи путем копирования**

При создании учетной записи пользователя, которая имеет одинаковые свойства с другой учетной записью, можно воспользоваться функцией копирования. Для этого необходимо выбрать учетную запись в списке и нажать «Копировать» на панели действий (Рис.16).

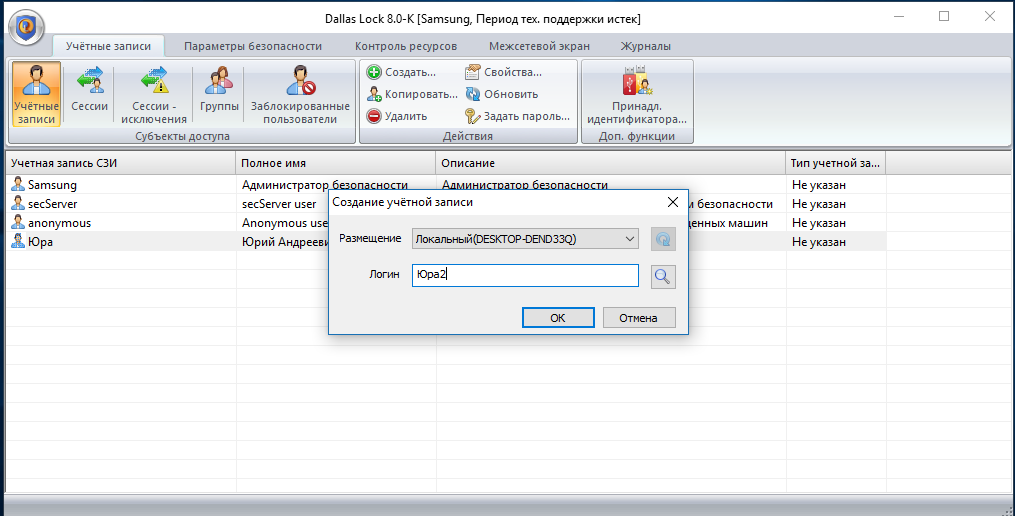


Рис.16 –Создание новой учетной записи с копированием свойств уже созданной.

В появившемся окне ввести имя учетной записи. Далее, в окне свойств, которые будут в точности повторять свойства выделенной учетной записи, их можно отредактировать. Далее необходимо создать пароль. Для создаваемой учетной записи будут скопированы свойства и список групп; установка параметров доступа на ресурсы не копируется и осуществляется индивидуально для данной учетной записи (или для группы, в которую она входит).

Создание учетной записи путем копирования свойств другой, имеет смысл только локальных учетных записей.

* + 1. **Создание и удаление групп пользователей**

Группы предназначены для объединения пользователей, у которых права безопасности могут быть схожими. Такое объединение может упростить работу администратора, при выполнении настроек СЗИ НСД. Группы безопасности упрощают управление доступом к ресурсам. Можно добавлять пользователей к группам безопасности, а затем предоставлять этим группам права доступа, и удалять их оттуда в соответствии с потребностями этих пользователей. Для просмотра и редактирования списка групп системы безопасности в оболочке администратора системы необходимо выбрать категорию «Группы» на вкладке «Учетные записи». В окне системы Dallas Lock автоматически появляется ряд предварительно сконфигурированных групп в локальной операционной системе Windows, в которые можно включать пользователей. Вновь созданные с помощью Dallas Lock группы автоматически создадутся и на локальном ПК. Удаленные локальные группы удалятся и из ОС на локальном ПК.

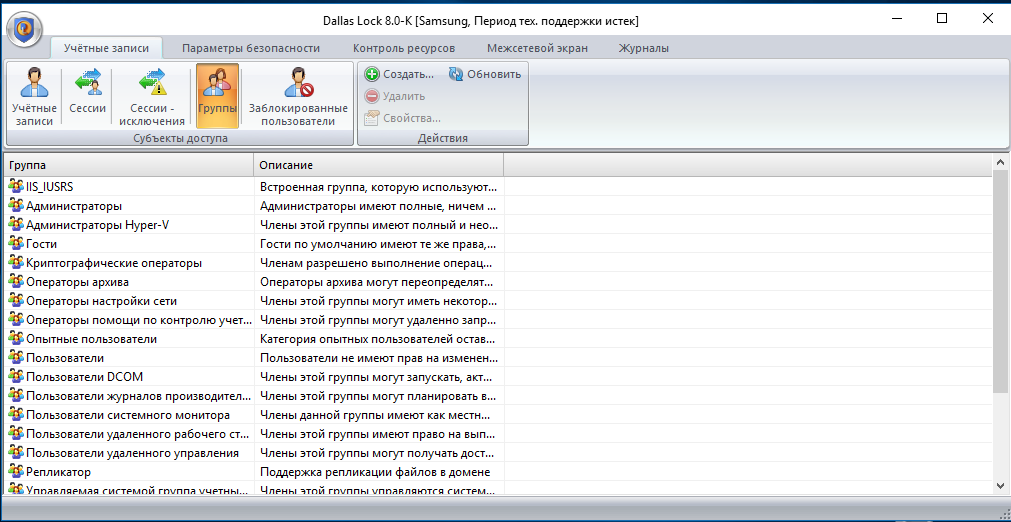


Рис.17 –Общий вид закладки «Группы»

Для создания новой группы необходимо:

**1.** В разделе «Группы» на вкладке «Учетные записи» нажать «Создать» (или выбрать данное действие из контекстного меню). Откроется окно, содержащее два поля: «Группа», «Описание» (Рис.18).

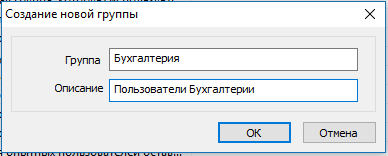


Рис.18 –Окно создания новой группы.

**2.** В поле «Группа» следует ввести название группы, в поле «Описание» − назначение группы или комментарий (необязательное поле). Нажать «ОК».

Изменить описание группы можно, используя кнопку «Свойства» на панели «Действия» или выбрав данное действие из контекстного меню. Назначить все необходимые политики безопасности для созданной группы можно, редактируя параметры безопасности различных категорий параметров. Для удаления группы необходимо выделить группу, которую следует удалить, нажать кнопку «Удалить» на панели «Действия» или выбрать данное действие в контекстном меню. На экране отобразится подтверждение на удаление.

* + 1. **Число разрешенных сеансов**

При настройке свойств учетной записи имеется возможность определить число разрешенных сеансов для данной учетной записи (Рис.19).

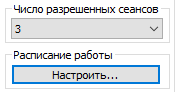


Рис.19 –Свойства учетной записи. Вкладка «Общие». Параметры сеансов доступа.

При установленном значении для каждой учетной записи (локальной или доменной) будет проверяться количество одновременных интерактивных и сетевых сессий (входов). Если число больше установленного – вход пользователя на ПК запрещается. Если стоит ограничение для учетной записи по маске, ограничение будет действовать на каждого доменного пользователя индивидуально. Таким образом, установив параметр «Число разрешенных сеансов» равным 1, можно настроить запрет вторичного (параллельного) входа пользователя в ОС.

* + 1. **Смена пароля пользователя**
       1. **Смена пароля средствами ОС**

Пользователь может самостоятельно сменить пароль для авторизации, для этого необходимо выполнить следующие шаги:

**1.** После входа в операционную систему, пользователю необходимо нажать комбинацию клавиш «Ctrl+-Alt+Del» и в списке операций выбрать «Сменить пароль».

На экране появится диалоговое окно, с полями для заполнения (Рис.20).

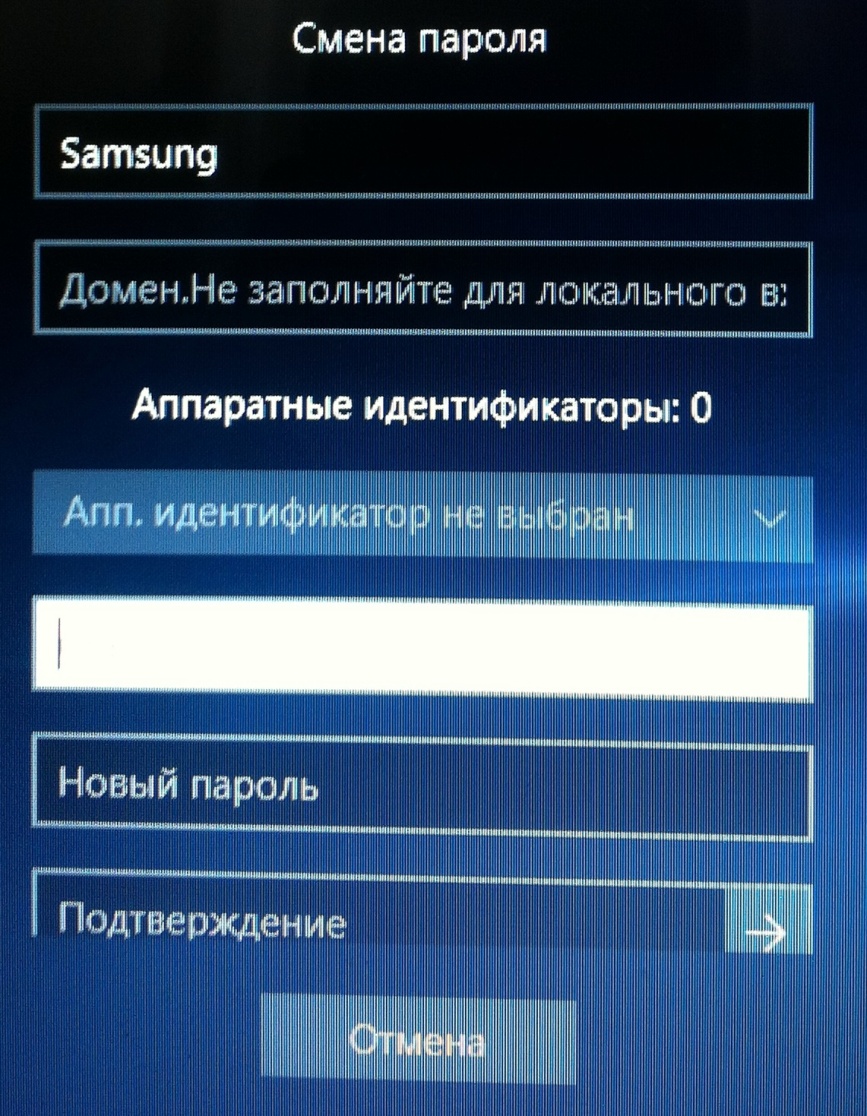


Рис.20 –Поля заполнения при смене пароля.

**2.** В открывшемся окне необходимо ввести имя пользователя, имя домена (для доменного пользователя, для локального – оставить это поле пустым или ввести имя компьютера), старый пароль, новый пароль и подтверждение нового пароля.

**3.** Выбрать назначенный аппаратный идентификатор.

**4.** Для создания пароля, отвечающего всем требованиям параметров безопасности, установленных системой защиты Dallas Lock 8.0, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать поле с надписью «Генерация пароля». Система автоматически создаст случайный пароль, советующий установленным параметрам безопасности, значение которого необходимо ввести в поля «Новый пароль» и «Повтор».

**5.** Далее нажать кнопку «ОК» для сохранения нового пароля или кнопку «Отмена».

В соответствии с политиками безопасности в системе могут быть включены настройки сложности паролей. Сложные пароли при их регулярной смене снижают вероятность успешной атаки на пароль. Поэтому при смене пароля пользователю необходимо иметь информацию о требованиях для установки паролей. В соответствии с тем, какие из параметров включены, при смене пароля пользователем, на экране могут возникать сообщения об ошибках. При возникновении подобных сообщений необходимо изменить пароль в соответствии с требованиями политик безопасности, установленными администратором.

* + - 1. **Смена пароля с помощью оболочки администратора**

В некоторых ситуациях, например, когда пользователь забыл свой пароль, администратору бывает необходимо задать пользователю новый пароль, не зная старого. Для этого в оболочке администратора нужно выбрать соответствующего пользователя в списке и нажать на действие «Задать пароль» (см. рис.15). В появившемся окне нужно ввести новый пароль, его подтверждение и нажать кнопку «ОК». Можно воспользоваться генератором паролей и ввести сформированный СЗИ НСД пароль в соответствующие поля.

* + 1. **Сессии-исключения**

Для корректной работы в режиме совместимости со сторонним программным обеспечением в СЗИ НСД Dallas Lock реализован механизм регистрации сессий, которым в качестве исключения разрешается работа с файловой системой, несмотря на отсутствие явного санкционированного входа. Зарегистрированные в Dallas Lock 8.0 сессии называются сессии-исключения. СЗИ НСД Dallas Lock уже содержит список настроенных сессий первой необходимости. По умолчанию они отключены.

Чтобы просмотреть список сессий-исключений и добавить новые необходимо в оболочке администратора на вкладке «Учетные записи» раскрыть категорию «Сессии-исключения» (Рис.21).

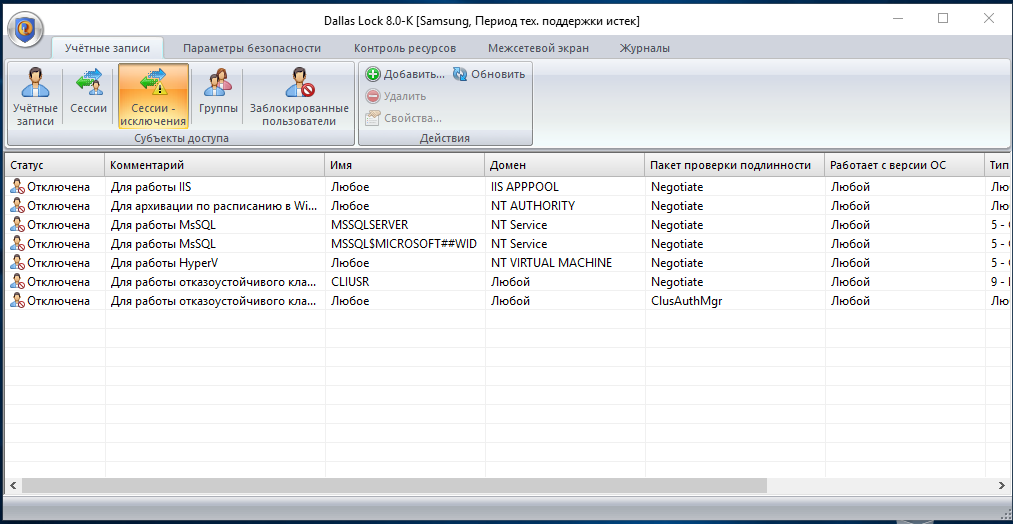
****

Рис.21 –Окно со списком сессий для работы ПО.

Чтобы зарегистрировать в СЗИ НСД сессию необходимо нажать «Добавить». В появившемся окне ввести параметры сессии.

Добавленную в список сессию можно временно отключить, не удаляя из списка, и заново включить. Для этого в окне параметров сессии необходимо отметить флажком поле «Исключение активно» (Рис.22).

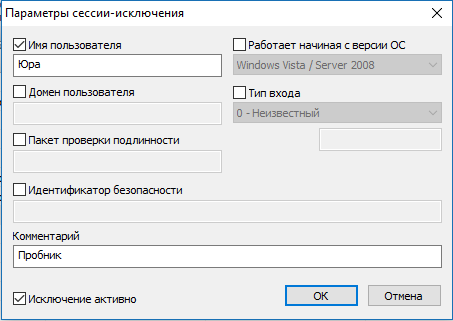


Рис.22 –Редактирование параметров сессии-исключения.

Удалять из списка зарегистрированные по умолчанию в Dallas Lock 8.0 сессии-исключения не рекомендуется.

* 1. **Заблокированные пользователи**

Учетная запись пользователя по разным причинам может быть заблокирована, например, вследствие неправильного ввода пароля несколько раз.

Чтобы открыть список заблокированных пользователей необходимо на вкладке основного меню «Учетные записи» выбрать категорию «Заблокированные пользователи» (Рис.23). В данном списке можно разблокировать отдельно выделенную учетную запись или несколько одновременно выделенных (действие «Разблокировать») и разблокировать все записи одновременно (действие «Разблокировать всех»).

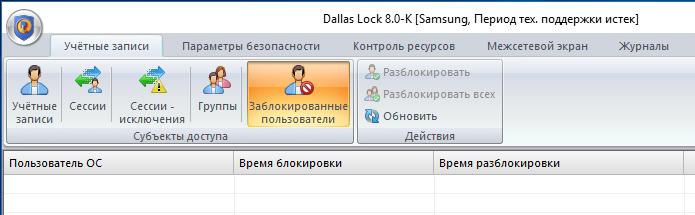
****

Рис.23 –Действия со списком заблокированных пользователей.

* 1. **Параметры входа** 
     1. **Разрешение и запрет интерактивного и удаленного входов в ОС**

СЗИ НСД Dallas Lock 8.0 обеспечивает защиту информации от несанкционированного доступа на ПК в ЛВС через локальный, терминальный и сетевой входы. Выполнить настройку разрешения или запрета интерактивного или удаленного входов в ОС данного ПК можно, развернув на основной вкладке «Параметры безопасности» категорию «Права пользователей». С помощью параметров безопасности «Интерактивный вход: разрешён/запрещён» и «Удаленный вход: разрешён/запрещён» определенным пользователям и группам можно запретить или разрешить локальный или удаленный вход в ОС. Добавить учетные записи в список разрешенных или запрещенных можно, выбрав параметр и нажав кнопку «Свойства». При настройке следует учесть, что установленный параметр запрета имеет более высокий приоритет перед установленным параметром разрешения. Также следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

Правило разрешения и запрета действий следующее(Рисю.24):

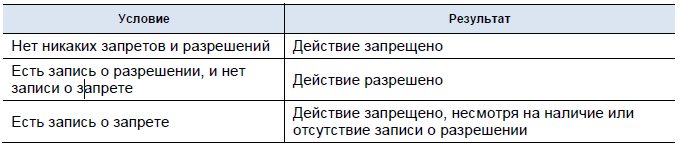


Рис.24 –Правило разрешения и запрета действий.

В списке субъектов, для которых устанавливается запрет или разрешение, определяется иерархия в порядке возрастания: группа «Все» => индивидуальная группа => учетная запись (доменная учетная запись «по маске») => пользователь. Таким образом, чтобы субъекту (например, пользователю) действие было разрешено, то он не должен входить в состав субъекта (например, группы), для которого это действие имеет явный запрет.

* + 1. **Настройка параметров входа**

После установки системы защиты, необходимо произвести ее настройку. Под настройкой системы защиты понимается установка значений параметров системы защиты, удовлетворяющих политикам безопасности предприятия. Для этого необходимо выбрать вкладку «Параметры безопасности».

Настройки, касающиеся входа в систему, установки атрибутов пароля, аппаратных считывателей, регулируются в окне закладки «Вход» (Рис.25).

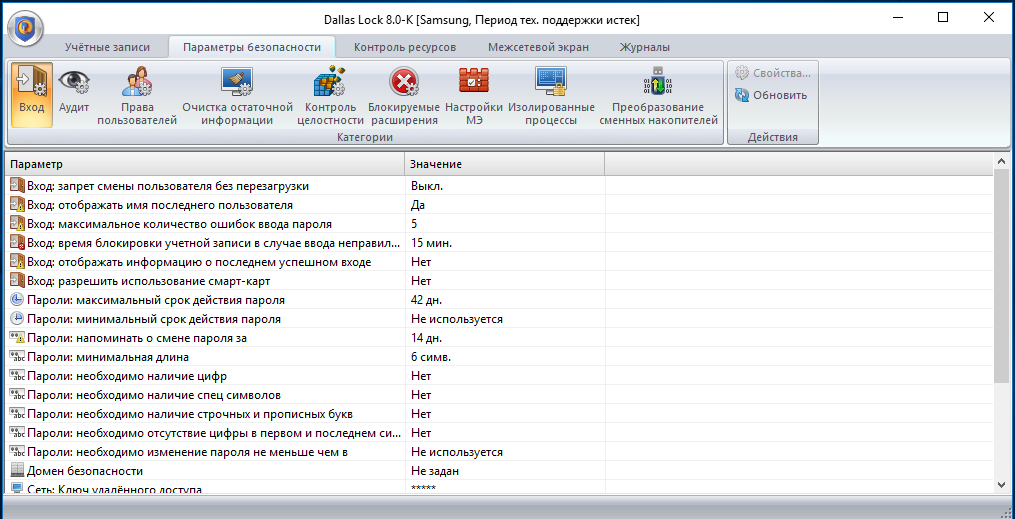
****

Рис.25 –Список параметров входа.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров на вход:

* **Вход: запрет смены пользователя без перезагрузки.**

Включение данного параметра не позволит осуществлять смену учетных записей пользователей без перезагрузки ПК. Если параметр имеет значение «Вкл.», то при выборе завершения сеанса или смены пользователя ПК автоматически уходит в перезагрузку. Если параметр имеет значение «Выкл.», то при выборе завершения сеанса или смены пользователя ПК выйдет из учетной записи и предложит снова ввести авторизационные данные.

* **Вход: отображать имя последнего пользователя.**

Включение данного параметра позволяет отображать в окне авторизации имя учетной записи последнего пользователя, осуществлявшего вход в ОС. Если параметр имеет значение «Да», то в поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет отображаться имя последнего пользователя данного ПК. Если параметр имеет значение «Нет», то поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет пустым.

* **Вход: максимальное количество ошибок ввода пароля.**

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. В выпадающем списке можно выбрать число попыток от 1 до 10. Если при входе на защищенный компьютер или на этапе загрузки ОС пользователь ввел неверный пароль, то система выдаст предупреждение «Указан неверный пароль». Если число ошибок больше допустимого, учетная запись будет заблокирована и пользователь не сможет загрузить компьютер и ОС. При этом система защиты выдаст сообщение «Запись пользователя заблокирована».

Способы блокировки описаны в разделе «Заблокированные пользователи». Если установлено значение «Не используется», то пользователь может вводить неверный пароль неограниченное число раз.

* **Вход: время блокировки учетной записи в случае ввода неправильных паролей (минут).**

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить компьютер и ОС, даже при верном вводе пароля. По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Если при настройке опции выбрано значение «Не используется», то разблокировать учетную запись и тем самым позволить пользователю вновь работать на защищенном компьютере, может только администратор безопасности.

* **Вход: отображать информацию о последнем успешном входе.**

При включении данного параметра входа (значение «Да») после загрузки ОС в области уведомлений Windows на панели задач будет появляться сообщение с информацией о дате последнего входа пользователя на данный компьютер, типе входа: сетевой, локальный, терминальный, неуспешных попытках входа и состоянии параметров учетной записи пользователя.

* **Пароли: максимальный срок действия пароля.**

Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока СЗИ автоматически предложит пользователю сменить пароль при входе в ОС. Если выбрано значение «Не используется», то время действия пароля не ограничено. В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

* **Пароли: минимальный срок действия пароля.**

Данным параметром устанавливается минимальный срок действия пароля для всех пользователей. До истечения установленного срока СЗИ не позволит пользователю сменить свой пароль. При выборе значения «Не используется» минимальный срок действия пароля не ограничен. В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

* **Пароли: напоминать о смене пароля за.**

С помощью данного параметра система защиты позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль. Если при настройке выбрать значение «Не используется», то напоминаний о необходимости смены пароля не будет.

* **Пароли: минимальная длина.**

Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение. При выборе значения «Не используется» устанавливаемый пароль может иметь пустое значение. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

* **Пароли: необходимо наличие цифр.**

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей

* **Пароли: необходимо наличие специальных символов.**

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать специальные символы из следующего списка: "`", "~", "!", "@", "#", "$", "%", "^", "&", "\*", "(", ")", "\_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/". Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

* **Пароли: необходимо наличие строчных и прописных букв.**

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать строчные и прописные буквы. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

* **Пароли: необходимо отсутствие цифры в первом и последнем символе.**

Если данный параметр включен (значение «Да»), то при создании пароля на месте первого и последнего символа в нем не должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

* **Пароли: необходимо изменение пароля не меньше чем в.**

Данным параметром задается количество символов, на которое, как минимум, должен отличаться новый пароль от старого, при его смене.

* **Сеть: Ключ удаленного доступа.**

Данным параметром устанавливается значение ключа удаленного доступа для удаленного входа на другие защищенные компьютеры.

* **Сеть: Время хранения сетевого кэша**

Для увеличения скорости работы по сети система защиты Dallas Lock 8.0 предоставляет возможность сохранения сетевого кэша с информацией об имеющихся в сети тех компьютеров, которые защищены Dallas Lock 8.0, и к которым уже было произведено обращение с данного ПК. В выпадающем списке данного параметра можно выбрать время хранения такого сетевого кэша.

* **Сеть: Список незащищенных серверов.**

С помощью данного параметра для увеличения скорости работы по сети, чтобы сократить количество обращений, СЗИ предоставляет возможность сохранить постоянный список ПК, которые не защищены СЗИ. Вводятся имена ПК и серверов или их IP-адреса через точку с запятой.

* **Блокировать компьютер при отключении аппаратного идентификатора.**

При включении данного параметра всем пользователям, которым назначен аппаратный идентификатор, работа на данном ПК при отключении идентификатора будет заблокирована.

* **Блокировать файл-диски при отключении аппаратного идентификатора.**

Если при создании файл-диска помимо пароля, используется аппаратный идентификатор, то при отключении идентификатора от ПК, файл-диск также будет отключен. По умолчанию данный параметр имеет значение «Включен».

* **Текст сообщения при входе.**

В окне данного параметра имеется возможность ввести текст предупреждения, которое будет отображаться пользователю до входа в операционную систему. Смысл данного текста должен предупреждать о реализации мер по обеспечению безопасности информации, и о необходимости соблюдения установленных правил обработки информации. Нажатие «ОК» пользователем будут означать подтверждение ознакомления.

1. **Эксплуатация системы защиты**

После установки и настройки системы защиты информации, наступает стадия обслуживания. Как при установке и настройке системы, так и при обслуживании ответственным лицом является администратор безопасности. Администратор безопасности информации назначается из числа сотрудников и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации.

Основные функции администратора:

* Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом;
* Контроль доступа лиц в помещение, где установлена СЗИ, в соответствии со списком сотрудников, допущенных к работе;
* Контроль над ежемесячным проведением смены паролей для доступа;
* Контроль целостности эксплуатируемой СЗИ, с целью недопущения и выявления несанкционированных модификаций;
* Контроль за отсутствием на магнитных носителях остаточной информации по окончании работы пользователей;
* Проводить обучение пользователей СЗИ, правилам работы с ней;
* Настройка и сопровождение подсистемы регистрации и учета действий пользователей;
* Ведение двух копий программных средств СЗИ и контроль их работоспособности.
* Введение в базу данных описания событий, подлежащих регистрации в системном журнале;
* Регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
* Своевременное информирование Начальника спецотдела о несанкционированных действиях персонала и проведение расследования попыток НСД;
* Периодическое тестирование функций СЗИ, особенно при изменении программной среды и полномочий исполнителей.
* Производить обновление СЗИ;
* Контролировать актуальность сертификата соответствия (сертификат данного продукта действителен до 25 сентября 2018г.)
* Восстановление программной среды, программных средств и настроек СЗИ при сбоях;

**Заключение**

В результате данной курсовой работы была изучена «Система защиты информации от несанкционированного доступа Dallas Lock 8.0» и написано руководство по настройке и эксплуатации, включающее в себя подсистему управления доступом. Dallas Lock имеет большой функционал. Обладает дружелюбным интерфейсом и производит впечатление надёжного продукта. Она подходит для защиты информации вплоть до совершенно секретной. Продукт Dallas-Lock привлекателен по цене. 7500 рублей за дистрибутив и право на использования до 9 компьютеров.

# **Список использованной литературы**

1. СЗИ Dallas Lock 8.0-K– URL: https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/ (дата обращения 27.11.2017, 28.11.2017).
2. Руководство по эксплуатации – URL: https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/(дата обращения 29.11.2017, 30.11.2017).
3. Курс по настройке СЗИ DallasLock 8.0– URL: https://ipiskunov.blogspot.ru/2016/02/dallaslock-8.html (дата обращения 29.11.2017).
4. Цены на продукт – URL: http://xn--h1anfb.xn--p1ai/szi-ot-nsd/Dallas-Lock/DLp/ (дата обращения 30.11.2017).
5. Цены на продукт – URL: http://www.4systems.ru/catalog/good/dnd/Confident/Dallas\_Lock\_8\_0\_K (дата обращения 1.12.2017).
6. РД Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации от 30.03.1992 г.;
7. URL: http://securitypolicy.ru /аттестация\_ас/инструкция\_аб (дата обращения 5.12.2017).
8. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 5.12.2017).
9. Государственный реестр ФСТЭК РФ–URL:http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения 6.12.2017).