

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА



ARMlock

**Руководство администратора
Сервера управления и контроля**

Содержание

ВВЕДЕНИЕ	4
1 ОБЩИЕ СВЕДЕНИЯ О СЕРВЕРЕ ARMLOCK.....	5
1.1 Назначение Сервера «ARMlock».....	5
1.2 Условия работы.....	5
2 УСТАНОВКА И УДАЛЕНИЕ СЕРВЕРА «ARMLOCK»	7
2.1 Требования к аппаратному и программному обеспечению	7
2.2 Способы установки Сервера «ARMlock»	8
2.3 Использование LiveCD	8
2.4 Использование .deb-пакета.....	11
2.5 Первоначальная настройка системы защиты «ARMlock»	11
3 НАЧАЛО И ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ В СРЕДЕ АДМИНИСТРИРОВАНИЯ СЕРВЕРА.....	18
3.1 Порядок действий при входе в среду администрирования	18
3.2 Возможные ошибки при входе.....	19
3.3 Завершение сеанса работы в среде администрирования.....	19
4 СМЕНА ПАРОЛЯ	20
5 ОПИСАНИЕ СРЕДЫ АДМИНИСТРИРОВАНИЯ СЕРВЕРА ARMLOCK.....	21
5.1 Элементы управления web-консоли.....	21
6 УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ СЕРВЕРА ARMLOCK.....	23
6.1 Просмотр, создание и удаление учетных записей администраторов	23
7 ПОЛИТИКИ ДОСТУПА.....	25
7.1 Просмотр, создание и редактирование политики безопасности.....	25
7.2 Удаление политики безопасности.....	26
7.3 Политика безопасности по умолчанию.....	26
8 ЖУРНАЛИРОВАНИЕ	27
8.1 Настройка параметров журналирования.....	27
8.2 Работа с журналом событий.....	28
9 НАСТРОЙКА СЕРВЕРОВ «ARMLOCK».....	29
9.1 Описание типов серверов взаимодействия	29
9.2 Просмотр и добавление серверов взаимодействия.....	29
9.3 Удаление серверов взаимодействия.....	31
10 НАСТРОЙКА ПАРАМЕТРОВ КЛИЕНТОВ	32
10.1Просмотр и добавление параметров клиентов	32
10.2Удаление параметров клиентов.....	33

10.3	Параметры по умолчанию	33
11	КОНТРОЛЬ ЦЕЛОСТНОСТИ.....	34
11.1	Описание механизма контроля целостности	34
11.2	Просмотр, создание и редактирование правил контроля целостности.....	34
11.3	Добавление объектов на контроль целостности в правило контроля целостности	35
11.4	Удаление правила контроля целостности.....	36
12	ОБЪЕКТЫ.....	37
12.1	Назначение механизма работы с объектами.....	37
12.2	Просмотр, добавление и редактирование объектов вручную	37
12.3	Удаление объекта.....	38
12.4	Добавление объекта из меню просмотра журналов событий	38
13	ПОЛЬЗОВАТЕЛИ	40
13.1	Назначение инструментария работы с пользователями	40
13.2	Просмотр, добавление и редактирование Пользователей.....	40
14	КОМПЬЮТЕРЫ	41
14.1	Назначение инструментария работы с компьютерами.....	41
14.2	Просмотр, добавление и редактирование Компьютеров.....	41
15	ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ И КОМПЬЮТЕРОВ	43
15.1	Назначение групп пользователей и компьютеров	43
15.2	Управление группами пользователей и компьютеров	44
16	ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	45
17	ИЗМЕНЕНИЯ	46

Введение

Данное руководство предназначено для администраторов Сервера управления и контроля системы защиты информации от несанкционированного доступа «ARMlock» (далее по тексту – Сервер «ARMlock»).

В руководстве содержатся сведения, необходимые администраторам для работы с Сервером «ARMlock».

Руководство подразумевает наличие у администратора базовых навыков работы с ПК, ОС Windows и Сетями ЭВМ.

В руководстве представлены элементы графических интерфейсов Сервера «ARMlock».

1 ОБЩИЕ СВЕДЕНИЯ О СЕРВЕРЕ ARMlock

1.1 Назначение Сервера «ARMlock»

Сервер «ARMlock» представляет собой программное средство для мониторинга и централизованного управления АРМ, на которых установлена Программа защиты информации от несанкционированного доступа «ARMlock» (ПЗИ НСД ARMlock), объединенных в локально-вычислительную сеть.

Сервер устанавливается на специально выделенную ПЭВМ для осуществления централизованного управления настройками АРМ с установленными ПЗИ НСД «ARMlock» и мониторинга событий безопасности системы защиты информации.

Функционал Сервера в частности позволяет:

- Осуществлять централизованное управление клиентской частью путём передачи конфигурационных файлов с подтверждением их достоверности;

- Осуществлять идентификацию и аутентификацию пользователей клиентской части; осуществлять регистрацию и учёт на сервере событий безопасности, зарегистрированных клиентской частью.

- Объединять АРМ и пользователей в группы, назначать им списки объектов доступа с заданными правами доступа.

- Назначать различным группам или отдельным АРМ политики авторизации (параметры клиента), указывая порядок осуществления проверки пароля пользователя и атрибутов двухфакторной аутентификации.

- Настраивать параметры журналирования событий безопасности.

Лицом, ответственным за управление системой защиты, рекомендуется назначать администратора информационной безопасности. Эту функцию могут выполнять и несколько сотрудников подразделения по защите информации организации.

1.2 Условия работы

1.2.1 Данные для учетной записи

Чтобы получить доступ в среду администрирования Сервера «ARMlock» необходимо иметь зарегистрированную на Сервере «ARMlock» учетную запись администратора.

Учетная запись имеет набор атрибутов, которые необходимы непосредственно для входа в среду администрирования Сервера «ARMlock». (Таблица 1.1)

Таблица 1.1 - Список атрибутов доступа, используемых в Сервере ПЗИ НСД ARMlock

Наименование	Описание
Имя (логин)	За пользователем закрепляется условное имя (идентификатор), необходимое для идентификации его в системе защиты
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (происходит аутентификация)

Значение имени и пароля администратора по умолчанию, используемые для подключения к вновь установленному Серверу «ARMlock» будут приведены в разделе 2 настоящего Руководства.

Идентификация и аутентификация по логину и паролю пользователя осуществляется при каждом входе. Имена и пароли учетных записей должны отвечать требованиям, приведенным в Таблице 1.2.

Таблица 1.2 - Требования к имени и паролю

Атрибут	Описание
Для имени:	максимальная длина имени – 32 символа; имя может содержать латинские символы, символы кириллицы, цифры и специальные символы; 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).
Для пароля:	максимальная длина пароля 32 символа; пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы; разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (Password и password являются разными паролями).

**Внимание!**

Не допускается сообщать атрибуты доступа учетных записей другим лицам. В случае компрометации любого из атрибутов доступа учетной записи, необходимо немедленно принять меры по их замене.

2 УСТАНОВКА И УДАЛЕНИЕ СЕРВЕРА «ARMlock»

2.1 Требования к аппаратному и программному обеспечению

Сервер «ARMlock» может быть установлен на отдельную персональную или серверную платформу, удовлетворяющую следующим минимальным требованиям:

- Процессор с архитектурой **x86-64** (Intel с поддержкой EM64T, AMD с поддержкой AMD64).
- Оперативная память **2048 Мб** и выше (для ЛВС с количеством АРМ более 100 – рекомендуется не менее 8 Гб оперативной памяти)
- Жесткий диск 2 Гб и выше (без учёта пространства для хранения журналов аудита, которое пользователь должен предусмотреть в зависимости от требований политики аудита событий безопасности)
- Наличие устройства чтения компакт-дисков.

При расширении ЛВС организации в процессе работы системы защиты «ARMlock» аппаратная конфигурация сервера может модернизироваться с учётом её реальной загруженности. Оценить фактическую загруженность аппаратной платформы можно с помощью встроенных утилит ОС Linux, например утилиты **top**. При реальной загруженности аппаратной платформы в часы наибольшей нагрузки более 50 процентов по процессорной мощности или используемой памяти – рекомендуется принять решение о модернизации аппаратной платформы и увеличении её вычислительной мощности либо объёма памяти соответственно.

Необходимо также осуществлять регулярный мониторинг фактически используемого объёма дискового пространства и принять решение о модернизации дисковой подсистемы при заполненности жесткого диска более чем на 50%. Оценить объём используемого дискового пространства можно с помощью встроенных утилит ОС Linux, например утилиты **df**.

Сервер может устанавливаться и на соответствующую виртуальную машину, с учётом вышеуказанных требований.

В случае, если пользователь желает установить Сервер «ARMlock» на существующую операционную систему, то на ЭВМ, на которой будет установлен Сервер «ARMlock» должна быть установлена 64-битная версия ОС Linux. Производителем протестирована работа Сервера «ARMlock» в 64-битных версиях дистрибутивов Linux Ubuntu 12 и 14 версий, а также Debian Wheezy, однако Сервер «ARMlock» способен работать и в других дистрибутивах ОС Linux.

Для установки на существующую ОС в ней должны присутствовать следующие пакеты и утилиты (ниже приведена команда, необходимая для установки указанных утилит в системах Debian или Ubuntu):

```
apt-get install mysql-server mysql-client nginx php5 php5-fpm php5-mysqld  
php5-apcu php5-curl php5-memcache
```

Производителем Сервера «ARMlock» протестирована корректная работа с веб-сервером nginx версии 1.1.19 и СУБД mysql версии 5.5.52. Рекомендуется использовать последнюю версию СУБД mysql из линейки 5.5.x.



В случае если при установке пакета php5-apcu система выдаст сообщение об ошибке, попробуйте добавить в список репозиториев /etc/apt/sources.list следующие строки:

```
deb http://packages.dotdeb.org wheezy-php55 all
```

```
deb-src http://packages.dotdeb.org wheezy-php55 all
```

Дополнительно рекомендуется установить пакет *git-core* и предоставить на сервер возможность подключаться к репозиторию *github.com* для получения обновлений версий Сервера «ARMlock», путём внесения соответствующих разрешающих правил в межсетевые экраны Вашей организации.

Кроме того, для работы с пакетом установки Сервера а также для получения возможности применения дополнительных скриптов в процессе жизненного цикла Сервера «ARMlock» и взаимодействия с компанией, осуществляющей поддержку Сервера «ARMlock», рекомендуется установить пакет *php5-cli* для запуска php-скриптов из командной строки bash.

apt-get install git-core php5-cli

2.2 Способы установки Сервера «ARMlock»

Сервер «ARMlock» поставляется в виде CD или DVD-диска с предустановленной операционной системой, а также минимальным набором необходимого системного и прикладного ПО: ARMlock LiveCD (LiveDVD).

Дополнительно к LiveCD в комплект поставки входит диск с отдельным дистрибутивом Сервера «ARMlock», собранного в виде *.deb*-пакета для установки в Debian-подобных дистрибутивах ОС Linux.

Самый быстрый способ развёртывания сервера – это использование LiveCD, т.к. за короткий срок позволяет получить работающий Сервер системы защиты информации, не тратя время на установку системы и решение проблем совместимости и зависимостей пакетов существующего дистрибутива ОС.

Второй способ – это использование *.deb*-пакета. Достоинством данного способа является возможность использования существующего дистрибутива ОС Linux, более привычного для администраторов Вашей организации.

2.3 Использование LiveCD

Для того, чтобы запустить Сервер «ARMlock» с LiveCD, входящего в комплект поставки, достаточно вставить данный компакт (или DVD) диск в соответствующий считыватель и настроить BIOS аппаратной платформы для загрузки с компакт-диска.

Произойдёт загрузка операционной системы и будут запущены необходимые для работы и администрирования Сервера «ARMlock» службы, в т.ч. веб-сервер *nginx*, СУБД *mysql*, сервер *armlock*, обрабатывающий сетевые соединения от клиентов, находящихся в ЛВС, и сервер *sshd*, предназначенный для администрирования операционной системы по протоколу SSH.

Кроме того, система произведёт необходимые настройки пакетного фильтра *netfilter*, являющегося частью ядра ОС Linux. По умолчанию система оставит открытыми только необходимые для работы Сервера «ARMlock» tcp-порты:

- 22 порт (для удалённого управления по протоколу SSH).
- 80 порт (консоль управления Сервером «ARMlock» по протоколу HTTP. С данного порта осуществляется redirect на http-ssl-порт 443).
- 88 порт (основной порт взаимодействия Сервера «ARMlock» с клиентскими программами ПЗИ НСД «ARMlock»).
- 89 порт (порт, на котором запускается по умолчанию сервер, обрабатывающий сообщения журналов аудита и событий безопасности, поступающих от ПЗИ НСД «ARMlock»).
- 443 порт (защищённая консоль управления Сервером «ARMlock»).

Для осуществления дальнейших настроек необходимо осуществить вход в операционную систему. Сделать это можно с помощью локальной консоли или с использованием любого ssh-клиента (например, putty).

По умолчанию для входа в операционную систему установлены следующие атрибуты доступа:

Имя пользователя: *root*

Пароль: *ARMlock!*

(пароль – вводится через «ноль» и должен заканчиваться восклицательным знаком)

2.3.1 Настройка сети

По умолчанию сервер пытается получить настройки сетевой подсистемы по протоколу DHCP. Самый простой способ выдать серверу правильный IP-адрес – это настроить соответствующим образом ваш сервер DHCP.

Если в Вашей организации DHCP не используется – вы можете задать статический IP-адрес. Для этого необходимо после осуществления входа в операционную систему отредактировать файл `/etc/network/interfaces` (для Debian-подобных ОС), например, добавив туда следующие настройки:

auto eth0

iface eth0 inet static

address 192.168.1.235

netmask 255.255.255.0

gateway 192.168.1.1

dns-nameservers 8.8.8.8 8.8.4.4

Где 192.168.1.235 – IP-адрес Сервера «ARMlock»,

192.168.1.1 – IP-адрес шлюза «по умолчанию»,

255.255.255.0 – маска IP-подсети,

8.8.8.8 и 8.8.4.4 – список DNS-серверов.

2.3.2 Настройки жёсткого диска

После загрузки с LiveCD операционная система Сервера «ARMlock» монтирует временный виртуальный диск в оперативной памяти ЭВМ, что позволяет работать системе в режиме чтения-записи (т.к. запись на компакт-диск невозможна). Однако дальнейшая работа системы в таком режиме приведёт к потере данных и всех сделанных настроек после перезагрузки Сервера.

Для того, чтобы все изменения, производимые в системе, сохранялись на жёстком диске, необходимо подготовить соответствующий раздел (так называемый persistence-раздел).

Для начала необходимо выделить соответствующий раздел на жёстком диске. Если таблица разделов ещё не создана или раздел ещё не выделен, это можно сделать с помощью встроенных в ОС Linux утилит. Например, утилиты `cfdisk`.

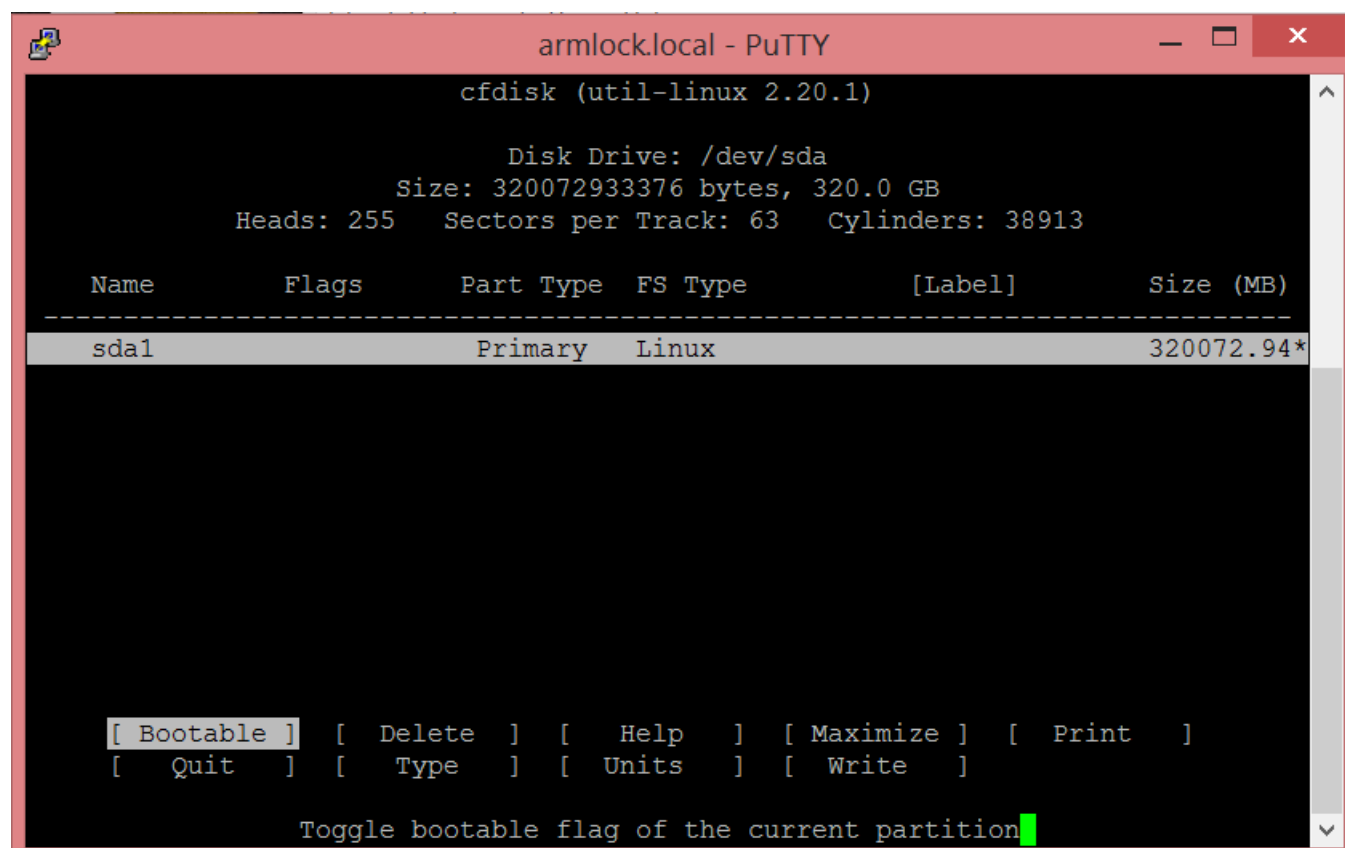


Рисунок 2.1 – пример разбиения диска на разделы с помощью утилиты cfdisk

Можно, например, создать единственный первичный раздел на весь диск и сохранить изменения в таблице разделов.

После этого, диск необходимо отформатировать. Например, с помощью утилиты *mkfs.ext3*.

mkfs.ext3 /dev/sda1

где *sda1* – раздел жёсткого диска, который мы выделили Выше для работы Сервера «ARMlock».

После окончания процедуры форматирования разделу нужно присвоить определённую метку («live-rw»), которая скажет операционной системе, что данный раздел должен быть использован операционной системой для сохранения всех изменений.

Для этого необходимо запустить утилиту *e2label*. Например:

e2label /dev/sda1 live-rw

В результате, после перезагрузки компьютера данный раздел автоматически будет подмонтирован в систему и будет использован для сохранения всех изменений, производимых в системе, а также для хранения реального содержимого базы данных Сервера «ARMlock».

Теперь Ваша операционная система настроена. После осуществления перезагрузки системы рекомендуем сменить пароль пользователя *root* с помощью утилиты *passwd*, и Вы можете перейти к разделу настройки Системы защиты информации «ARMlock» в разделе 2.5.

2.4 Использование .deb-пакета

Для того, чтобы установить Сервер «ARMlock» из дистрибутива, входящего в комплект поставки, достаточно скопировать .deb-пакет с дистрибутивом Сервера «ARMlock» в существующую систему на базе ОС «Linux» и проделать следующую последовательность команд:

```
dpkg -i armlock_1.57.0-1_amd64.deb
```

где 1.57.0-1 – версия Сервера «ARMlock» и номер сборки дистрибутива. В случае, если при установке возникла ошибка отсутствия необходимых зависимостей в системе, попробуйте выполнить одну следующие команды:

```
apt-get -f install
```

После выполнения данной команды должны автоматически установиться необходимые зависимости и сам «Сервер «ARMlock»». Проверьте это убедившись, что в системе появилась папка /home/armlock и пользователь armlock.

Если зависимости не установились – попробуйте сделать это вручную:

```
apt-get install mysql-server mysql-client nginx php5 php5-fpm php5-mysqldb  
php5-apcu php5-curl php5-memcache php5-cli git-core
```

после этого попробуйте повторно установить .deb-пакет командой

```
dpkg -i armlock_1.57.0-1_amd64.deb
```

Если установке прошла успешно – создайте первоначальную структуру и наполнение базы данных:

```
/home/armlock/armlock/install/create_database
```

И запустите необходимые сетевые сервисы:

```
service mysql start
```

```
service nginx start
```

```
service armlock start
```

Проконтролируйте статус процесса armlock:

```
armlock status
```

2.5 Первоначальная настройка системы защиты «ARMlock»

Первоначальная настройка системы защиты «ARMlock» осуществляется с помощью WEB-консоли.

Для того, чтобы войти в web-консоль необходимо воспользоваться любым web-браузером. Рекомендуется использовать Firefox, Chrome или Opera.

В url-строке введите ip-адрес, назначенный Серверу «ARMlock».

Согласитесь с предупреждением о сертификате, добавьте исключение безопасности (при необходимости).

Для того, чтобы устранить ошибку сертификата необходимо прописать на Вашем DNS-сервере запись вида

X.X.X.X A armlock.local

где X.X.X.X – IP-адрес Сервера «ARMlock»



Кроме того, необходимо установить сертификат wellsrv-ca.cer в перечень доверенных сертификатов Вашего браузера. (для IE сертификат устанавливается в перечень доверенных корневых сертификатов при установке ПЗИ НСД «ARMlock»).

После этого в url-строке браузера можно набирать адрес <http://armlock.local>

При этом ошибки сертификата возникать не будет.

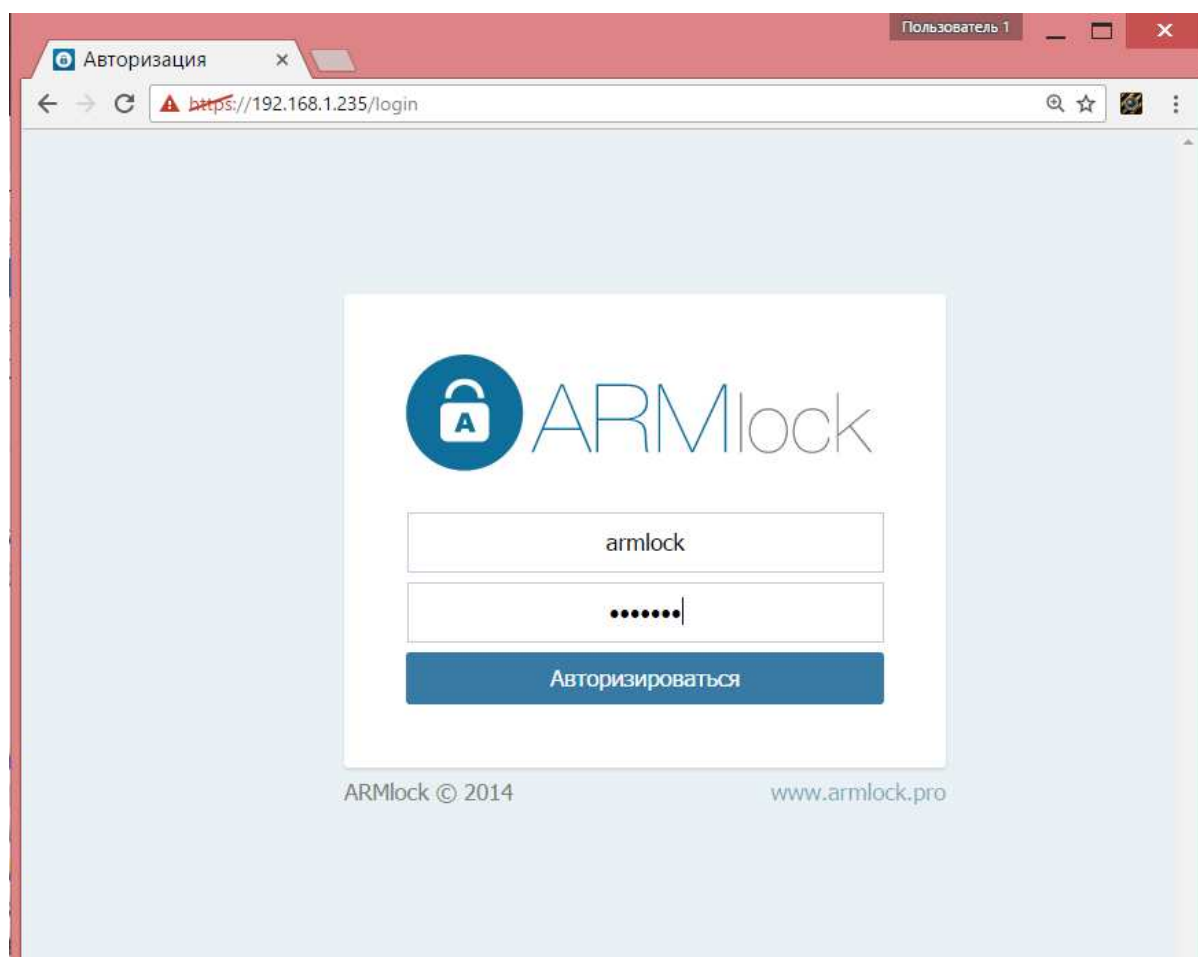



Рисунок 2.2 – ввод имени и пароля в web-консоли

По умолчанию в консоли установлены следующие атрибуты доступа:

Имя пользователя: ***armlock***

Пароль: ***armlock***

Вы попадёте в сетевую консоль администрирования. Здесь необходимо добавить записи о уже существующих серверах конфигурации и журналирования. Для этого перейдите в раздел

«Серверы» в правом верхнем углу консоли. На странице Серверы нажмите иконку со знаком  (добавить сервер).

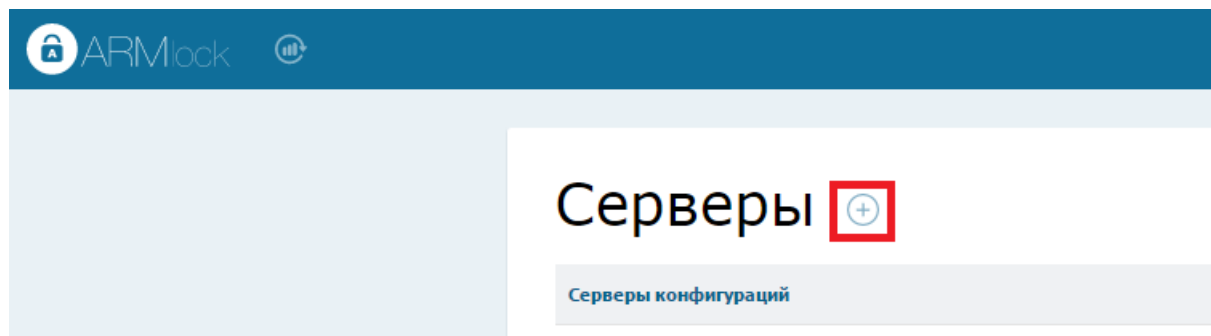


Рисунок 2.3 – добавление серверов

Сначала добавим сервер конфигурации, как показано на рисунке ниже:

Серверы » Создание нового сервера

Имя сервера:	<input type="text" value="Configuration"/>
Тип сервера:	<input type="text" value="Сервер конфигураций"/>
HTTP адрес сервера:	<input type="text" value="192.168.1.235"/>
HTTP порт сервера:	<input type="text" value="88"/>
	<input checked="" type="checkbox"/> Первичный сервер
	<input type="checkbox"/> Выключить сервер
	<input type="button" value="Добавить сервер"/>

Рисунок 2.4 – добавление сервера конфигурации

В поле HTTP адрес сервера указывается IP-адрес либо доменное имя сервера «ARMlock».

HTTP порт сервера можно оставить 88 (по умолчанию).

Признак «первичный сервер» определяет порядок сортировки серверов в конфигурации, выгружаемой пользователю. Он необходим для балансировки нагрузки между несколькими серверами. Для случая единственного сервера значение этого поля не принципиально.

Признак «выключить сервер» предназначен для временного исключения сервера из конфигурации пользователей без потери настроек сервера.

Теперь добавим сервер журналирования:


Серверы » Создание нового сервера

Имя сервера:	<input type="text" value="HTTP адрес сервер"/>
Тип сервера:	<input type="text" value="Сервер журналирования"/>
HTTP адрес сервера:	<input type="text" value="192.168.1.235"/>
HTTP порт сервера:	<input type="text" value="89"/>
	<input checked="" type="checkbox"/> Первичный сервер
	<input type="checkbox"/> Выключить сервер
<input type="button" value="Добавить сервер"/>	

Рисунок 2.5 – добавление сервера журналирования

HTTP-порт сервера рекомендуем оставить в значении «89», т.к. именно на этом tcp-порту по умолчанию запускается сервер журналирования.

После сохранения изменений перейдите на главную страницу консоли, нажав в левом верхнем углу на эмблему ARMlock. Перейдите в раздел «Компьютеры».

Нажмите на кнопку  для добавление компьютера по умолчанию (если требуется). Добавление компьютера «по умолчанию» требуется для того, чтобы выдавать конфигурацию клиентам с установленной ПЗИ НСД «ARMlock», имена которых не заведены на Сервере «ARMlock». Если компьютер по умолчанию не заведён в системе, Сервер откажет клиенту, пришедшему за конфигурацией в обработке запроса.

Компьютер «по умолчанию» имеет предустановленное имя «Default» отделённое с каждой стороны двумя идущими подряд символами подчёркивания «».



Используется именно два идущих подряд подчёркивания с каждой стороны:
 {подчеркивание} {подчеркивание}Default {подчеркивание} {подчеркивание}

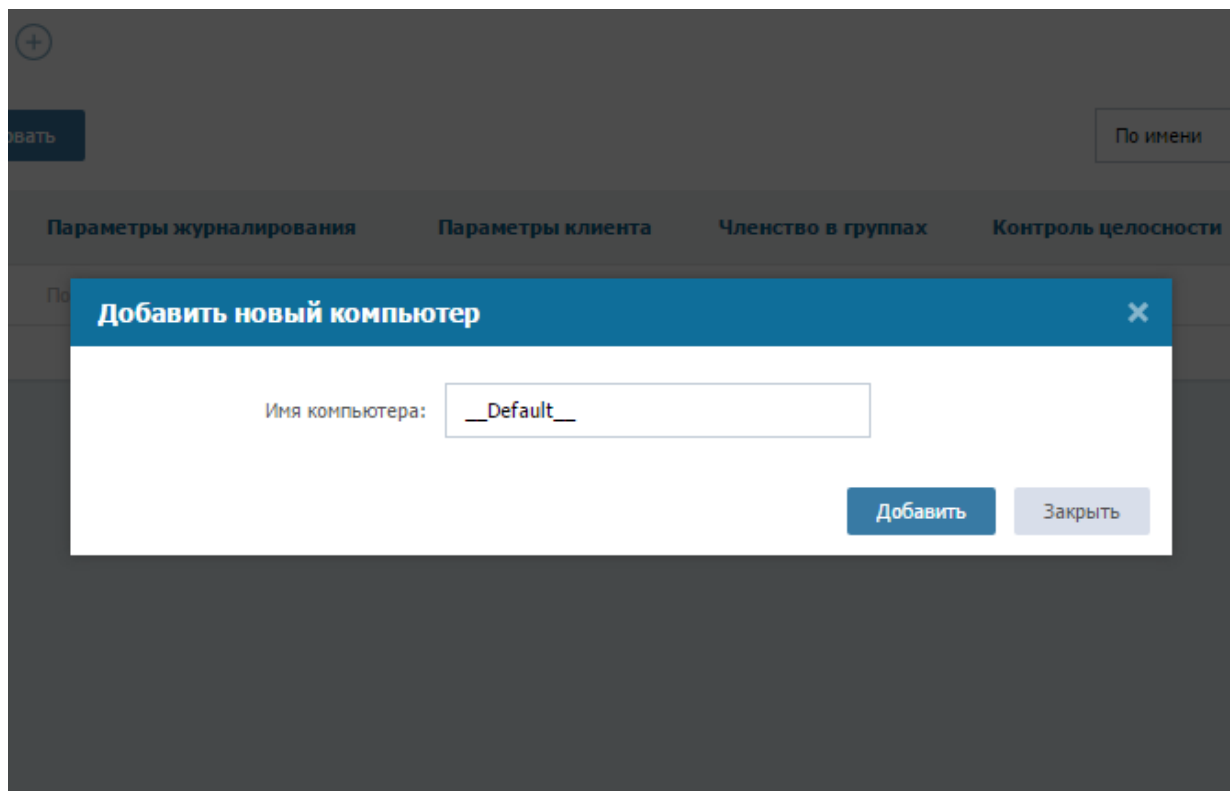



Рисунок 2.6 – создание компьютера «по умолчанию».

После создания компьютера по умолчанию снова перейдите на главную страницу консоли, нажав в левом верхнем углу на эмблему «ARMlock».

Перейдите в раздел «Пользователи».

Создайте первого пользователя, нажав на .

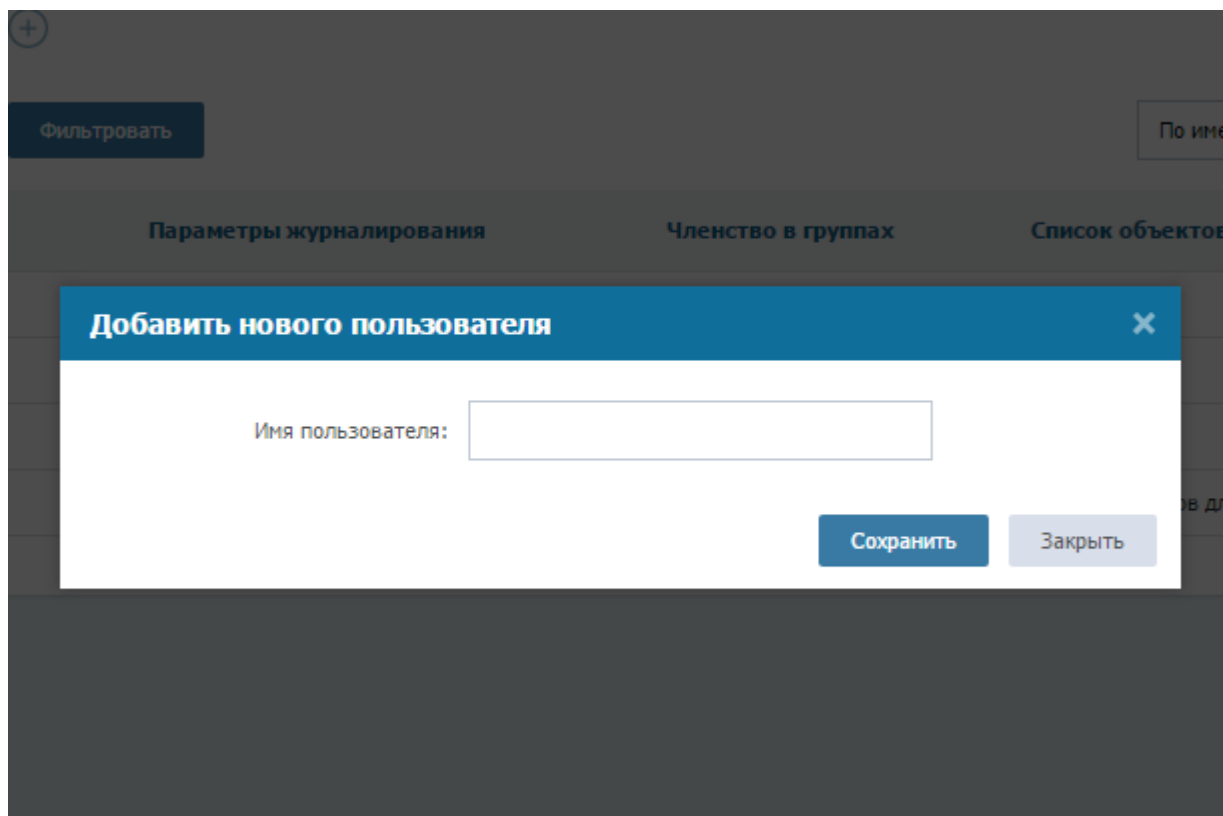


Рисунок 2.7 – создание пользователя.

После нажатия на кнопку «Сохранить», войдите в меню редактирования пользователя, нажав на имени его учетной записи.

Смените ему пароль, как показано на рисунке 2.8. При необходимости, присвойте пользователю статус «Локального администратора». Локальные администраторы обладают правами на запуск локальной консоли администратора и просмотр настроек пользователей, событий безопасности. А также на удаление ПЗИ НСД «ARMlock» с компьютера.

Пользователь » User1
✕

Статус: Офлайн

Версия конфига: Старая версия

Версия ARMlock: Неизвестно

Имя пользователя:

User1

Учетная запись заблокирована

Новый пароль:

••••••

Требуется смену пароля

Еще раз:

••••••

Локальный администратор

Обязательный

Новая карта:

У пользователя нет карт

Добавить

Имя:

Отчество:

Фамилия:

Должность:

Политика безопасности:

По умолчанию ↻ ▼

Параметры журналирования:

По умолчанию ↻ ▼

Списки объектов:

По умолчанию ▼

Группы пользователя:

Компьютер не состоит в группах. Добавить?

Удалить пользователя

Сохранить

Закрыть

Рисунок 2.8 – задание пароля пользователя

Нажмите на кнопку «Сохранить».

По умолчанию в «Параметрах клиента» указана политика проверки пароля «На сервере ARMlock», поэтому, если Вы ещё не успели отредактировать эти настройки, клиенты с установленной в сетевом режиме ПЗИ НСД «ARMlock» теперь смогут входить в систему под только что созданной на сервере учетной записью, вводя заданный пароль.

Более подробно о имеющихся возможностях и настройках системы смотрите последующие разделы настоящего руководства.

3 НАЧАЛО И ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ В СРЕДЕ АДМИНИСТРИРОВАНИЯ СЕРВЕРА

3.1 Порядок действий при входе в среду администрирования

Для входа в консоль управления необходимо в строке браузера ввести IP-адрес или доменное имя Сервера «ARMlock». Появится меню авторизации (Рисунок 3.1) с полями для ввода атрибутов доступа ученой записи.



Рисунок 3.1 - меню авторизации в среду администрирования Сервера

Для входа в среду администрирования Сервера «ARMlock» необходимо:

1. Заполнить поле «Имя пользователя», в соответствии именем пользователя, под которым он зарегистрирован в системе.
2. Ввести пароль. Поле ввода пароля является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
3. Кликнуть ЛКМ по кнопке «Авторизоваться».

После нажатия кнопки «Авторизоваться» осуществляется проверка введенных атрибутов доступа учетной записи.



Примечание. При вводе имени и пароля переключение раскладки клавиатуры (русская/латинская) производится нажатием комбинации клавиш, установленной при настройке свойств клавиатуры. Текущий язык отображается индикатором клавиатуры.


3.2 Возможные ошибки при входе

Если неверно введен один из атрибутов доступа учетной записи, то на экране появится сообщение об ошибке, после чего система предоставит возможность повторно ввести логин и пароль (Рисунок 3.2)



Рисунок 3.2 - Сообщение при вводе неверного логина или пароля

3.3 Завершение сеанса работы в среде администрирования

Для завершения сеанса работы на Сервере ARMlock необходимо нажать ЛКМ на кнопке выхода , расположенной в правом верхнем углу главного меню среды администрирования Сервера.

4 СМЕНА ПАРОЛЯ

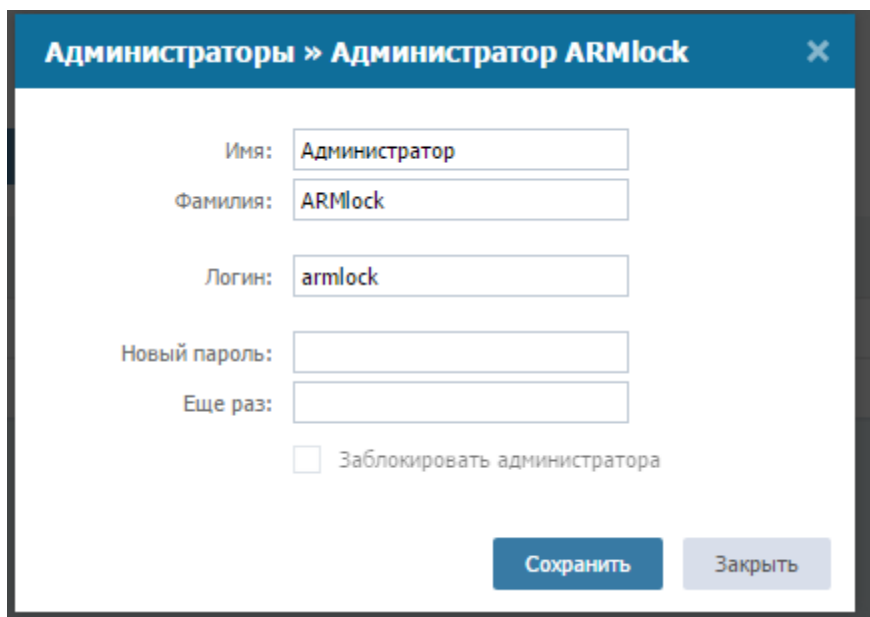
Администратор может самостоятельно сменить свой пароль для аутентификации в среде администрирования (web-консоли).

Для этого необходимо выполнить вход в среду администрирования Сервера «ARMlock» и нажать в правом верхнем углу главного меню на кнопку с именем текущей учетной записи (в

данном примере имя учетной записи - «Администратор ARMlock»):

Администратор ARMlock

На экране появится форма, с полями для смены пароля (Рисунок 4.1).

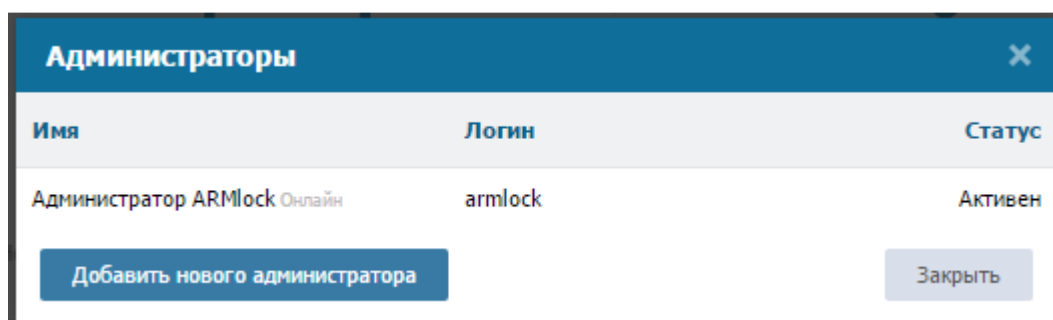


The screenshot shows a web form titled "Администраторы > Администратор ARMlock". It contains several input fields: "Имя" (Name) with "Администратор", "Фамилия" (Surname) with "ARMlock", "Логин" (Login) with "armlock", "Новый пароль" (New password), and "Еще раз" (Repeat). There is also a checkbox for "Заблокировать администратора" (Lock administrator) which is unchecked. At the bottom, there are two buttons: "Сохранить" (Save) and "Закреть" (Close).

Рисунок 4.1 - форма смены пароля

Для изменения пароля необходимо в полях «Новый пароль» и «Еще раз» ввести требуемое значение пароля и нажать кнопку «Сохранить».

Если все требования соблюдены, то пароль пользователя будет успешно сменен, и появится окно с перечнем учетных записей администраторов (Рисунок 4.2).



Администраторы		
Имя	Логин	Статус
Администратор ARMlock Онлайн	armlock	Активен

Buttons: "Добавить нового администратора" (Add new administrator), "Закреть" (Close)

Рисунок 4.2 - форма с информацией об учетных записях Сервера

5 ОПИСАНИЕ СРЕДЫ АДМИНИСТРИРОВАНИЯ СЕРВЕРА ARMlock

5.1 Элементы управления web-консоли

Централизованное управление компьютерами, на которых установлена «ПЗИ НСД ARMlock», осуществляются с помощью среды администрирования Сервера «ARMlock».

Для входа в среду администрирования (в web-консоль) необходимо выполнить действия, описанные в разделе 3 Настоящего руководства.

Элементы главного меню среды администрирования приведены на Рисунке 6.1.

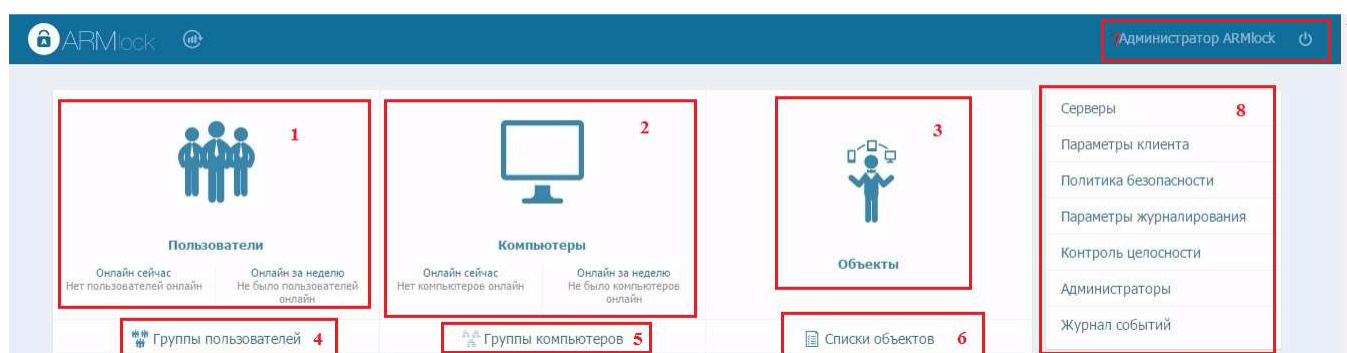


Рисунок 6.1 - Интерфейс среды администрирования Сервера

Функциональное назначение элементов интерфейса консоли администрирования описано в (Нумерация в таблице приведена в соответствии с нумерацией на Рисунок 6.)

Таблица 6.2. - Описание элементов среды администрирования

№	Наименование	Назначение
1	Меню «Пользователи»	Работа с учетными записями пользователей АРМ под управлением ПЗИ НСД ARMlock
2	Меню «Компьютеры»	Работа (просмотр/добавление/редактирование) с АРМ под управлением ПЗИ НСД ARMlock
3	Меню «Объекты»	Работа (просмотр/добавление/редактирование) с объектами доступа АРМ. (CD-диски, floppy, USB-накопители и т.п.)
4	Группы пользователей»	Просмотр, создание и редактирование групп пользователей
5	Группы компьютеров	Создание и редактирование групп компьютеров
6	Списки объектов	Создание, добавление и редактирование списков из объектов разного типа (CD-дисков, USB-накопителей, специфичных USB-устройств) с присвоением таким объектам типа доступа (блокировка, только чтение, чтение-запись). Впоследствии созданные в данном разделе списки доступа можно присваивать отдельным пользователям, компьютерам или группам.
7	Имя учетной записи текущего пользователя и кнопка выхода из среды администрирования	Информация о текущем пользователе администраторе Сервера «ARMlock», осуществляющем работу в консоли и кнопка выхода

8	Блок меню настроек системы защиты информации «ARMlock»	Настройка параметров системы защиты «ARMlock»: политик безопасности по умолчанию, политик проверки пароля, журналирования, контроля целостности.
---	--	--

6 Управление учетными записями Сервера ARMlock

6.1 Просмотр, создание и удаление учетных записей администраторов

Для создания учетной записи нажмите на кнопку «Администраторы» в блоке меню настроек системы защиты «ARMlock» (Рисунок 6.1)

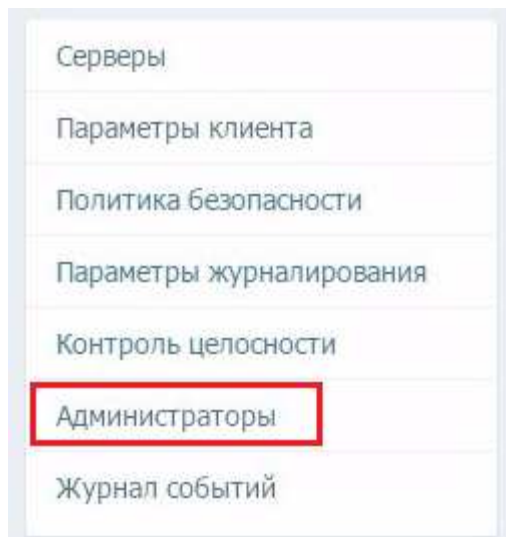


Рисунок 6.1 - Создание новой учетной записи

Появится форма просмотра учетных записей администраторов. (Рисунок 6.2)

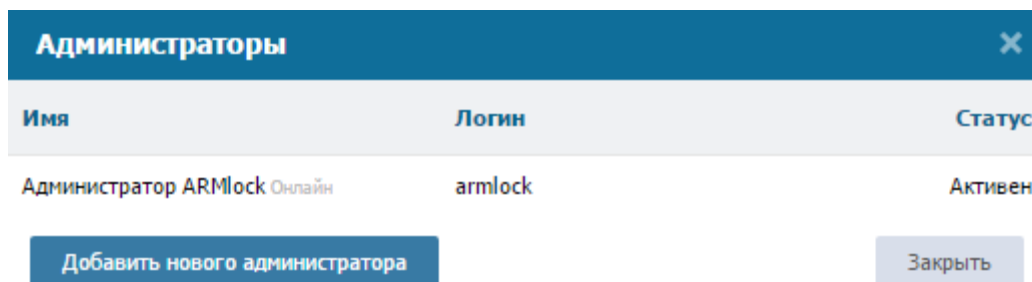


Рисунок 6.2 - Форма просмотра учетных записей администраторов

Для создания новой учетной записи необходимо нажать на кнопку «Добавить нового администратора». Появится форма создания новой учетной записи.

В полях формы необходимо ввести или выбрать следующие соответствующие учетной записи атрибуты доступа. Описание полей приведено в Таблице 6.1.

Таблица 6.1 - Описание полей формы создания учетной записи администратора

Наименование поля/параметра	Описание
Имя	Имя сотрудника, который будет работать под учетной записью
Фамилия	Фамилия сотрудника, который будет работать под учетной записью
Логин	Имя учетной записи, под которой идентифицируется пользователь
Пароль	Комбинация символов, по которой осуществляется аутентификация пользователя

Еще раз	Поле повторного ввода пароля, необходимо для проверки соответствия задуманной и реально введенной парольной комбинации символов
Заблокировать администратора	В случае активации данного поля вновь созданная учетная запись будет заблокирована. Данное поле создано с целью временной блокировки пользователя с сохранением всех его настроек для случаев, когда удаление учетной записи администратора не целесообразно.

После ввода аутентификационных данных необходимо нажать кнопку

Создать администратора

Учетная запись будет создана и появится в форме просмотра учетных записей администраторов.

6.1.1 Блокирование/разблокирование учетных записей администраторов

Для блокирования учетной записи администратора необходимо щелкнуть левой кнопкой мыши на имени блокируемой учетной записи в форме просмотра учетных записей администраторов. В панели появившейся формы откроются параметры учетной записи.

Необходимо поставить галочку в поле «Заблокировать администратора». (Рисунок 6.3)

The screenshot shows a web form titled "Администраторы >> Тест Тест". It contains the following fields and controls:

- Имя:
- Фамилия:
- Логин:
- Новый пароль:
- Еще раз:
- Заблокировать администратора

At the bottom of the form, there are three buttons: "Удалить администратора" (disabled), "Сохранить" (active), and "Закреть" (disabled).

Рисунок 6.3 - блокировка учетной записи

После выставления параметра необходимо нажать на кнопку «Сохранить».

Для разблокирования учетных записей необходимо выполнить все вышеуказанные действия, но выставив значение параметра «Заблокировать администратора» в значение «V».

6.1.2 Удаление учетных записей администраторов

Для удаления учетной записи администратора необходимо выбрать запись, подлежащую удалению, в форме просмотра учетных записей администраторов и нажать на кнопку

Удалить администратора

В появившейся форме подтверждения необходимо подтвердить удаление и нажать кнопку «Да». После этого выбранная учетная запись будет удалена

7 Политики доступа

7.1 Просмотр, создание и редактирование политики безопасности

Для просмотра, создания и редактирования политики по умолчанию доступа к объектам безопасности необходимо нажать на «Политика безопасности» в блоке меню настроек системы защиты информации «ARMlock». (Рисунок 7.1)

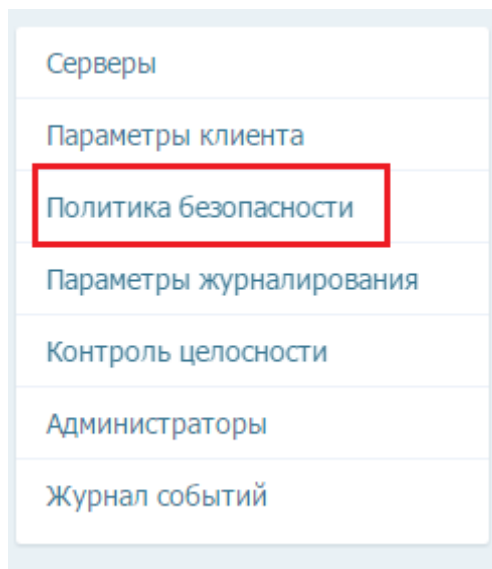


Рисунок 7.1

Появится форма просмотра и редактирования политик безопасности

Таблица 7.1 - Описание параметров политики безопасности

Наименование параметра	Описание
Имя	Имя политики
По умолчанию	Сделать политикой по умолчанию
USB флеш-карты	Настройка правила по умолчанию доступа к USB флеш-дискам
USB устройства	Настройка правила по умолчанию доступа к USB устройствам
Дискеты	Настройка правила по умолчанию доступа к дискетам
CD диски	Настройка правила по умолчанию доступа к CD дискам
Принтеры	Настройка доступности подсистемы печати принтерам
Файлы и папки	Настройка правила по умолчанию доступа к файлам и папкам
Минимальная длина пароля	Требования к длине пароля учетных записей АРМ под управлением ПЗИ ARMlock

Для параметров доступа к объектам можно установить следующие значения:

- Разрешить;
- Только чтение;
- Блокировать.

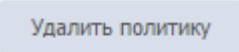


Примечание. При использовании новой политики «По умолчанию» , значение «По умолчанию» предыдущей политики сбрасывается. Политика остается в списке под именем «По умолчанию»



Категорически не рекомендуется изменять разрешающую политику доступа к файлам и папкам по умолчанию, т.к. это может привести к неработоспособности операционной системы на компьютерах с установленной ПЗИ НСД «ARMlock». Оставьте этот параметр в значении, разрешающем полный доступ, если только Вы предварительно не создали разрешающего специального правила доступа к системным объектам, например, с маской %WINDIR% или C:****

7.2 Удаление политики безопасности

Для удаления политики безопасности необходимо в форме просмотра политик открыть политику, подлежащую удалению, и нажать кнопку  .

В появившемся окне подтвердить удаление, нажав кнопку «Да».

7.3 Политика безопасности по умолчанию

Политика безопасности, отмеченная в качестве политики «по умолчанию» применяется во всех случаях, когда в настройках компьютера, пользователя или группы не указаны явно другие политики.

8 Журналирование

8.1 Настройка параметров журналирования

В зависимости от требований к системе защиты информации в организации и условий функционирования ПЗИ НСД ARMlock можно указать параметры журналирования.

Для этого необходимо войти в среду администрирования. Далее, нажатием ЛКМ открыть «Параметры журналирования». (Рисунок 8.1).

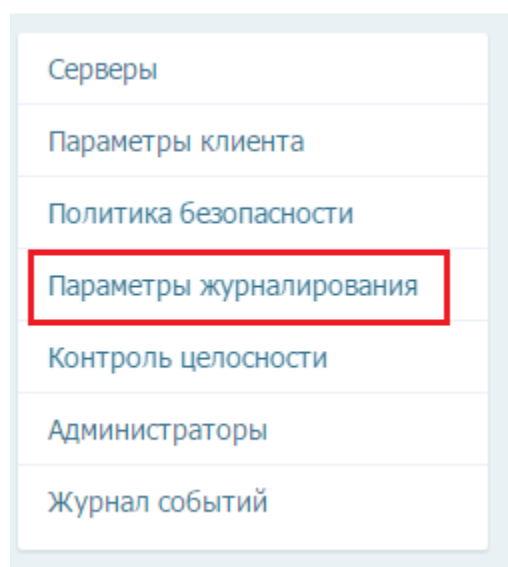


Рисунок 8.1 - Параметры журналирования

Появится форма просмотра параметров журналирования

Описание назначения параметров журналирования приведено в Таблице 8.1

Таблица 8.1 - Описание параметров журналирования

Наименование параметра	Описание
Уровень локального журнала	Уровень событий, согласно RFC 6587 (syslog), начиная с которого события будут сохраняться в локальный журнал на компьютере с установленной ПЗИ НСД «ARMlock». Впоследствии просмотр таких журналов будет возможен только непосредственно на указанном компьютере с помощью локальной консоли администратора либо текстового редактора.
Максимальный размер локальных логов	Ограничение максимального размера файла с журналом в мегабайтах.
Максимальный размер документа	Ограничение максимального размера файла, содержащего теньевую копию распечатываемого пользователем документа, в мегабайтах.
Уровень отправки на сервер ARMlock	Уровень событий, согласно RFC 6587 (syslog), начиная с которого события будут отправляться на сервер журналирования «ARMlock».
Уровень syslog журнала	Если уровень важности события меньше данного значения, событие отправляется для записи на syslog-сервер.
Уровень eventlog журнала	Если уровень важности события меньше данного значения, событие отправляется для записи в системный журнал ОС Windows.

Каждое из событий имеет уровень важности в соответствии со стандартом RFC 6587. Таким образом указывая минимальный уровень важности событий можно управлять записью событий в журнал в зависимости от их уровня важности. Чем меньше число в уровне важности события, тем более значимым оно считается. Указание нуля («0») в качестве минимального уровня события, попадающего в соответствующий канал журналирования, выключит такой канал. Например, если указать в качестве уровня локального журнала ПЗИ НСД ARMlock «0», то в локальный журнал событий не будет попадать ни одного события безопасности.

Уровни и разделы журнала задаются в соответствии с RFC 5424 (от Debugging (7) до Emergency (0)).



Примечание. Рекомендуем использовать следующие настройки журналирования: уровень локального журнала – Informational, уровень серверного журнала – Notice, уровень SYSLOG и EVENTLOG – 0 (отключить).

8.2 Работа с журналом событий

8.2.1 Просмотр журнала

Для просмотра записей о событиях в журнале необходимо открыть нажатием ЛКМ «Журнал событий» в блоке меню настроек главного меню. (Рисунок 8.2)

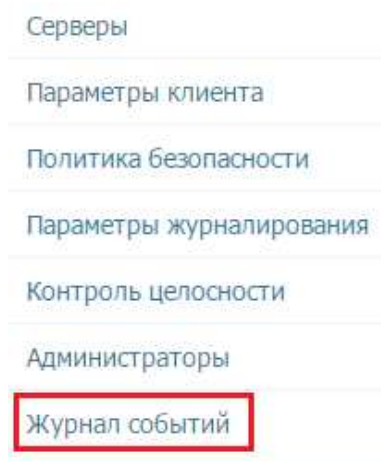


Рисунок 8.2 -Открытие журнала событий

Появится меню настроек просмотра журналов. В данном меню можно задать критерии по которым будут отфильтровываться отображаемые записи в журналах. Такими критериями могут быть время, Имя пользователя, имя устройства и т.п.

9 Настройка серверов «ARMlock»

9.1 Описание типов серверов взаимодействия

Для среды администрирования ПЗИ НСД ARMlock существуют 2 типа серверов:

- Сервер конфигураций.
- Сервер логирования;

Сервер конфигураций предназначен для обработки запросов от ПЗИ НСД «ARMlock», установленных в ЛВС, на конфигурацию системы безопасности. Данный сервер генерирует индивидуальные настройки для каждого компьютера, в зависимости от того, какой пользователь осуществляет вход на данный компьютер, а также от того, в каких группах состоят эти пользователи и компьютер и какие списки доступа и настройки присвоены указанным субъектам, компьютерам и группам.

Сервер логирования осуществляет сохранение событий безопасности, поступающих от компьютеров с установленной ПЗИ НСД «ARMlock», и сохранение их в СУБД mysql на Сервере «ARMlock».



Примечание. Важно понимать, что редактируя параметры серверов конфигурации и логирования через административную консоль, вы не меняете настройки этих серверов. Вы только меняете их описание, попадающее в настройки безопасности, выгружаемые «клиентскому» компьютеру с установленной ПЗИ НСД «ARMlock». Таким образом, задача администратора состоит в том, чтобы записи, созданные им в разделе «Серверы» отражали реальные настройки серверов безопасности. Фактическое же управление запуском, остановом, номерами портов и прочими настройками серверов конфигурации и логирования осуществляется через системную консоль ОС Linux. Для этого нужно войти в неё под пользователем «root» и запустить команду *armlock* с необходимыми параметрами. Список параметров можно посмотреть с помощью *armlock -h*

9.2 Просмотр и добавление серверов взаимодействия

Для добавления сервера необходимо в главном меню среды администрирования открыть нажатием ЛКМ «Серверы» в блоке настроек Сервера (Рисунок 9.1)

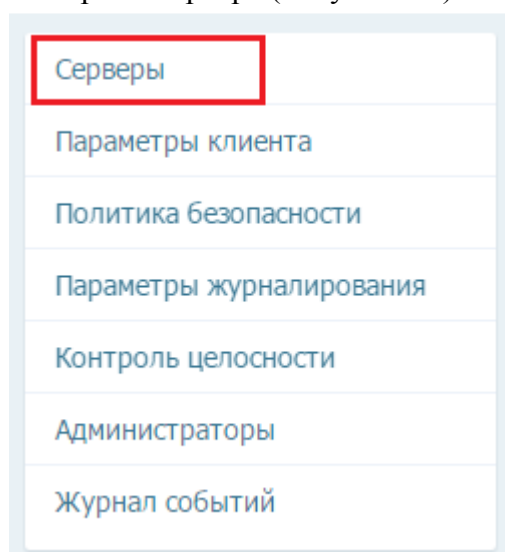



Рисунок 9.1 -Открытие формы просмотра и редактирования серверов

Появится форма просмотра серверов взаимодействия, в которой будут отображены записи о ранее созданных серверах.

Для добавления серверов необходимо нажать кнопку . Появится форма добавления сервера. (Рисунок 9.2)

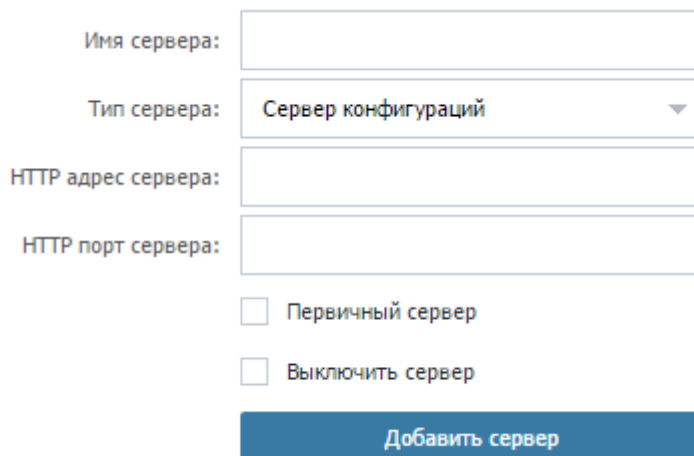


Рисунок 9.2 -форма добавления серверов

Описание полей формы добавления сервера приведено в Таблице 9.1

Таблица 9.1 - Описание параметров журналирования

Наименование поля	Описание
Имя сервера	Имя, под которым сервер будет отображаться в форме просмотра серверов взаимодействия
Тип сервера	В выпадающем списке можно выбрать тип сервера (см. раздел 9.1)
HTTP адрес сервера	В данном поле указывается доменное имя или IP-адрес добавляемого сервера. Адрес нужно указать таким способом, чтобы он мог разрешиться в указанном виде на любом клиенте с установленной ПЗИ НСД «ARMlock». Для проверки правильности указанного имени можно выполнить на клиенте команду <i>ping <HTTP-адрес-сервера></i> , указав в точности адрес из данного поля.
HTTP порт сервера	В данном поле указывается tcp-порт, по которому соответствующий сервер будет ожидать входящие соединения. По умолчанию для сервера конфигураций указывается порт 88, а для сервера логирования – 89. Рекомендуется использовать настройки по умолчанию.
Первичный сервер	Данное поле используется в случае наличия в сети нескольких серверов соответствующего типа. Первичные серверы будут приоритетными при выгрузке конфигурации клиентскому компьютеру с установленной ПЗИ НМД «ARMlock». Эта настройка может использоваться для балансирования нагрузки. При наличии в системе лишь по одному серверу каждого типа значение данного поля не важно.
Выключить сервер	Если отмечено данное поле, сервер не будет указан в передаваемых на АРМ под управлением ПЗИ НСД «ARMlock» конфигурациях системы безопасности, однако все его настройки сохраняться, он продолжит отображаться в форме просмотра серверов и его можно будет впоследствии легко активировать, не вводя настройки заново.

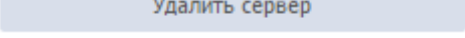
После ввода параметров добавляемого сервера взаимодействия необходимо нажать кнопку



Добавить сервер

9.3 Удаление серверов взаимодействия

Для удаления серверов необходимо из главного меню среды администрирования Сервера открыть форму просмотра серверов взаимодействия и нажать ЛКМ на имени удаляемого сервера.

Далее необходимо нажать кнопку  и в появившейся форме подтвердить удаление, нажав кнопку «Да».

10 Настройка параметров клиентов

10.1 Просмотр и добавление параметров клиентов

Для просмотра параметров клиентов необходимо открыть нажатием ЛКМ в главном меню среды администрирования «Параметры клиента» (Рисунок 10.1)

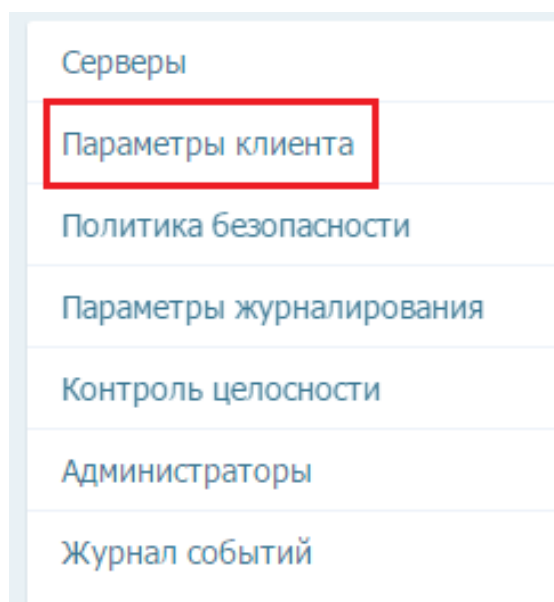


Рисунок 9.2 - открытие меню «параметры клиента»

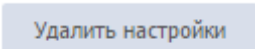
Появится форма просмотра и редактирования существующих параметров клиентов. Описание значения полей приведены в Таблице 10.1.

Таблица 9.1 - Описание параметров клиентов

Наименование поля	Описание
Имя	Имя набора параметров, под которым данный набор будет отображаться в меню просмотра параметров клиентов
По умолчанию	Если отметить данное поле, то набор параметров будет использоваться в качестве набора параметров «по умолчанию», т.е. в тех случаях, когда не указан другой, специальный набор параметров клиента
Проверка карты	Настройка проверки аппаратного идентификатора при применении двухфакторной аутентификации. Если двухфакторная аутентификация не применяется, следует выбирать в выпадающем списке значение «не проверять». Более подробно о доступных алгоритмах осуществления проверки аппаратного идентификатора можно ознакомиться в руководстве администратора ПЗИ НСД «ARMlock»
Проверка пароля	Настройка проверки пароля пользователя. В данном поле можно указать, каким образом необходимо осуществлять проверку пароля пользователя. Имеется возможность проверки пароля средствами ОС Windows, на сервере «ARMlock» или локально, средствами ПЗИ НСД «ARMlock». Более подробно о доступных алгоритмах осуществления проверки пароля пользователя можно ознакомиться в руководстве администратора ПЗИ НСД «ARMlock»
Автовход	Автоматический вход в систему при прикладывании карты пользователя (в

	случае использования двухфакторной аутентификации)
Авторазблокировка	Автоматическая разблокировка при повторном предъявлении снятого аппаратного идентификатора
Переподключение	Период между попытками переподключения к Серверу «ARMlock» в случае, если Сервер был недоступен
Считыватель не подключен	Сообщение, которое будет выведено пользователю в случае, если не подключен считыватель, но требуется осуществить проверку аппаратного идентификатора
Телефон для связи	Номер телефона технической поддержки, который будет показан в сообщении пользователю АРМ в случае ошибки работы ПЗИ ARMlock или сообщений системы безопасности, отображаемых пользователю. Поле допускается оставить пустым. В случае, если требуется отображать телефон, то необходимо указывать предложение целиком, например: «Телефон для связи: 22-88»
Период контроля целостности	Периодичность выполнения контроля целостности объектов, которые заданы в настройках контроля целостности. Указывается в минутах. Если оставить 0 – то контроль целостности будет осуществляться только при запуске системы защиты и при смене аппаратной конфигурации (входах-выходах пользователей на АРМ).
Период опроса карты	Период времени в секундах, через который считыватель будет активно проверять наличие карты на считывателе. В случае, если оставить значение равное нулю, считыватель будет только генерировать события прикладывания и снятия карты со считывателя. Рекомендуется установить в ноль. Однако при наличии ошибок на старых версиях ОС «Windows» (в частности, Vista с определёнными service pack), можно выставить поле в определённое целое значение, например 5, означающее периодический опрос карты раз в 5 секунд.
Журналирование процессов	Параметр влияет на то, будут ли добавляться в журнал аудита события, связанные с запуском и завершением процессов ОС
Проверка подписи	Необходимость проверки цифровой подписи процессов ОС при запуске. Рекомендуемое значение - 0
Обнуление памяти	Заполнение памяти нулями после завершения процессов ОС. (Очистка остаточной информации в оперативной памяти). Может снизить производительность компьютеров. При отсутствии требований к очистке остаточной информации - рекомендуемое значение – 0.

10.2 Удаление параметров клиентов

Для удаления параметров необходимо открыть форму отображения параметров Клиента и нажать ЛКМ на имени удаляемого набора. Далее необходимо нажать кнопку  и подтвердить удаление, нажав в появившемся окне кнопку «Да».

10.3 Параметры по умолчанию

Политика, отмеченная в качестве политики «по умолчанию» применяется во всех случаях, когда в настройках не указаны явно другие параметры. Редактирование осуществляется также как редактирование обычной политики - путем выбора и редактирования в форме просмотра политик под именем «По умолчанию».

11 Контроль целостности

11.1 Описание механизма контроля целостности

Контроль целостности осуществляется согласно заведённым в системе правилам. Каждое правило представляет собой имя файла или маску (относительный путь), задающую список файлов для контроля целостности.

В случае добавления маски в правило контроля целостности «по умолчанию», файлы по указанной маске будут добавлены на контроль целостности на всех АРМ, подключенных к серверу, для которых не заданы специальные правила контроля целостности.

11.2 Просмотр, создание и редактирование правил контроля целостности

Для просмотра параметров контроля целостности необходимо открыть нажатием ЛКМ в главном меню «Контроль целостности» (Рисунок 11.1)

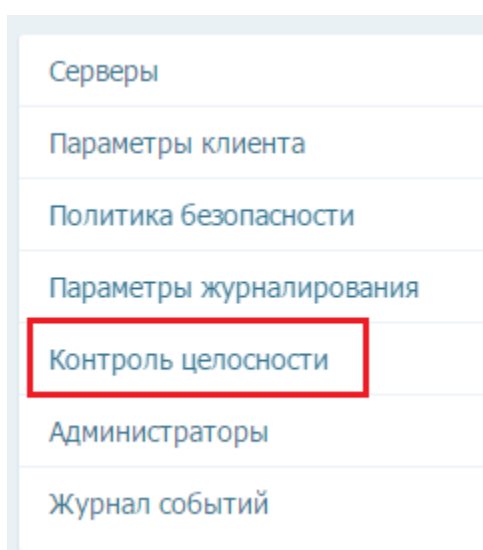


Рисунок 11.1 -Контроль целостности

После этого появится форма просмотра имеющихся на Сервере правил контроля целостности. (Рисунок 11.2)

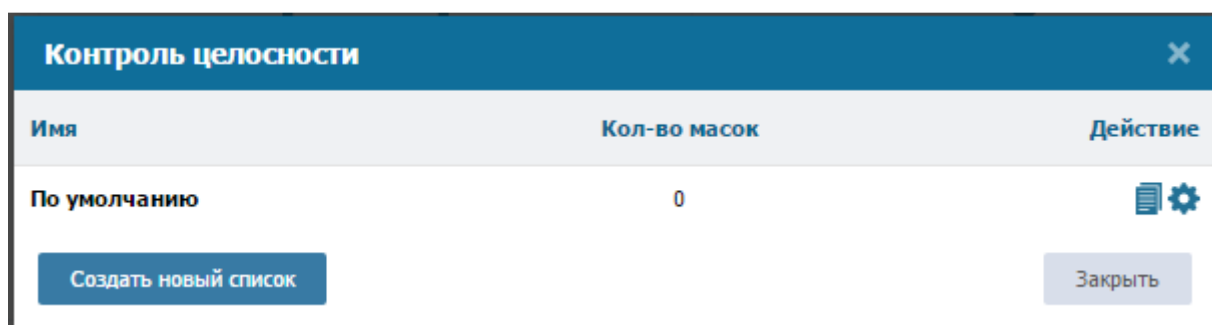


Рисунок 11.2 -Контроль целостности

Для создания нового списка правил контроля целостности необходимо нажать кнопку

Создать новый список

Появится форма создания нового списка правил контроля целостности. (Рисунок 11.3). Необходимо ввести имя нового списка для контроля целостности и нажать кнопку

Создать новый список

. Если установить галочку в поле «По умолчанию», список контроля

целостности будет использоваться как список «по умолчанию» для всех АРМ, т.е. переменные из создаваемого список контроля целостности будут автоматически добавлены на контроль на всех АРМ, подключенных к Серверу, которым не присвоен специальный список контроля целостности.

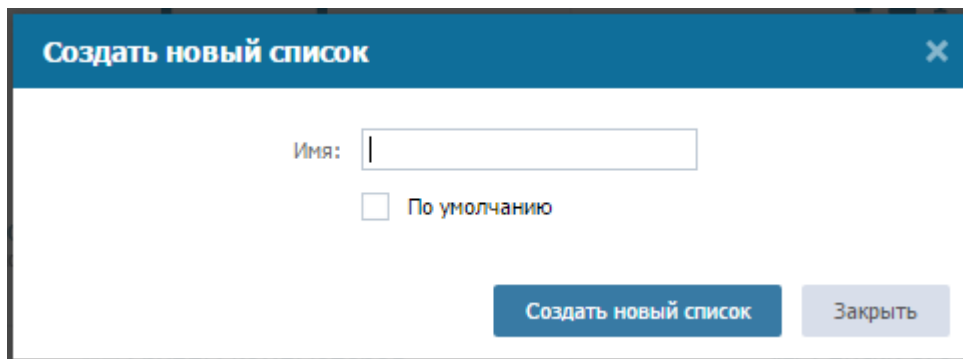



Рисунок 11.3 - Создание правила контроля целостности

Для редактирования (изменения имени, установки как списка по умолчанию) имеющихся правил контроля целостности необходимо открыть форму просмотра параметров контроля целостности и нажать на кнопку  справа от правила в списке, которое требует отредактировать.

11.3 Добавление объектов на контроль целостности в правило контроля целостности

Для добавления правила контроля целостности в список правил необходимо открыть имеющийся список, нажав на его имени ЛКМ. Появится форма добавления объектов на контроль. (Рисунок 11.4)

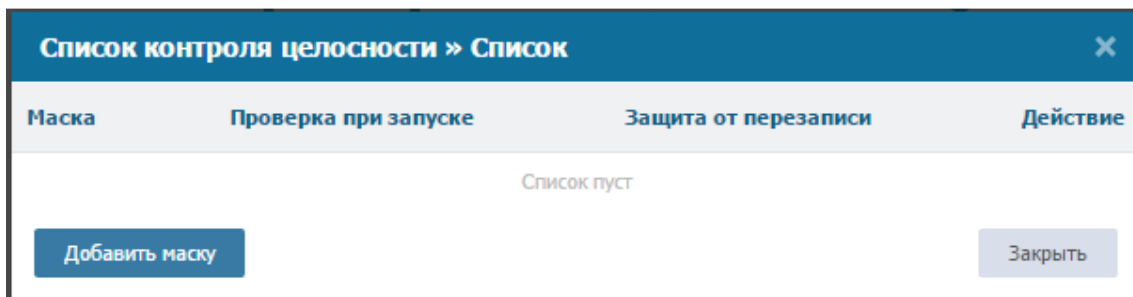
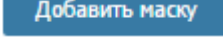


Рисунок 11.4 - Создание правила контроля целостности

Далее необходимо нажать ЛКМ по кнопке . Появится форма (Рисунок 11.5).

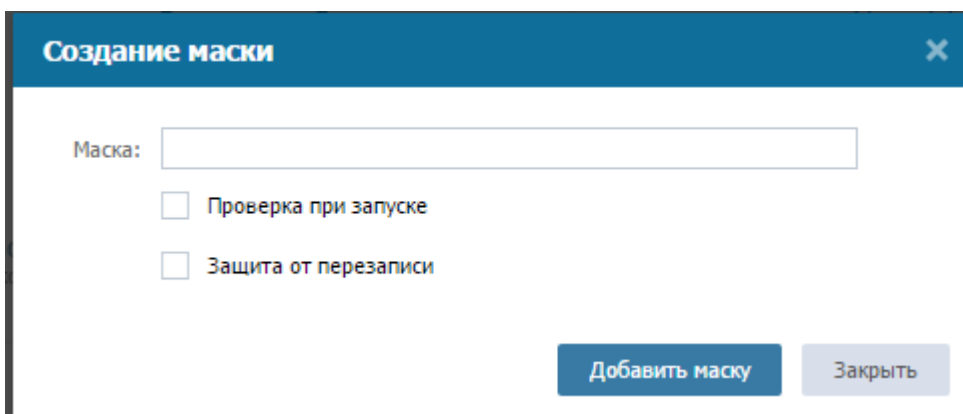


Рисунок 11.5 - Создание правила контроля целостности

В поле маска необходимо задать путь к контролируемому файлу или набору файлов. Допускается использование системных переменных вида %WINDIR%, %ARMLOCK% для указания относительного пути к файлу.

Также можно указать только путь к папке. Контролироваться при этом будут все файлы в указанной папке и её подкаталогах, т.к. по умолчанию к поисковой строчке с путём к папке добавляется маска «**». Чтобы указать конкретный файл в папке – замените маску «**» на требуемое имя файла. Если вы хотите, чтобы в маску не входили подкаталоги указанной папки – замените две звёздочки в маске на одну «*».




Допускается использование только тех системных переменных, которые содержат единственный уникальный путь к файлу или папке. Например, нельзя использовать переменную %PATH%, т.к. в ней содержатся перечисленные пути.


Пример корректного заполнения маски: **%WINDIR%\system32*.dll**

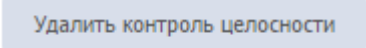
В случае установки галочки в поле «Проверка при запуске» целостность объектов контроля будет контролироваться при запуске ОС.

В случае установки галочки в поле «Защита от перезаписи», будут блокироваться попытки изменить файл, поставленный на контроль.

После указания параметров объектов контроля в списке, необходимо нажать ЛКМ на кнопке .

11.4 Удаление правила контроля целостности

Для удаления правила контроля целостности необходимо открыть форму просмотра правил контроля целостности и нажать на кнопку  справа от правила, которое требуется удалить.

Далее необходимо нажать кнопку  и подтвердить удаление.

12 Объекты

12.1 Назначение механизма работы с объектами

Данная оснастка среды администрирования Сервера «ARMlock» позволяет добавлять, удалять, редактировать данные о контролируемых объектах (USB-flash дисках, floppy-дисках, CD-DVD-дисках, специфичных USB-устройствах, файлах и папках по маске), для которых с помощью оснастки политика безопасности можно задавать правила доступа.

12.2 Просмотр, добавление и редактирование объектов вручную

Для создания, редактирования или удаления объектов доступа, необходимо в главном меню нажать ЛКМ по пиктограмме оснастки работы с объектами. (Рисунок 12.1)



Рисунок 12.1 - Пиктограмма для входа в меню работы с объектами

Откроется меню со списком всех объектов, заведенных в систему.

Описание полей отображаемых данных об объектах приведено в Таблице 12.1.

Таблица 12.1 - Описание параметров объектов

Наименование поля	Описание
Идентификатор	Имя объекта
Тип	Тип объекта (CD--диск, USB-накопитель и т.п.)
Описание	Краткая характеристика объекта, указанная при добавлении

Для добавления объекта необходимо нажать ЛКМ по кнопке .

Появится форма добавления объекта. (Рисунок 12.2)


Добавить новый объект ×

Тип объекта:

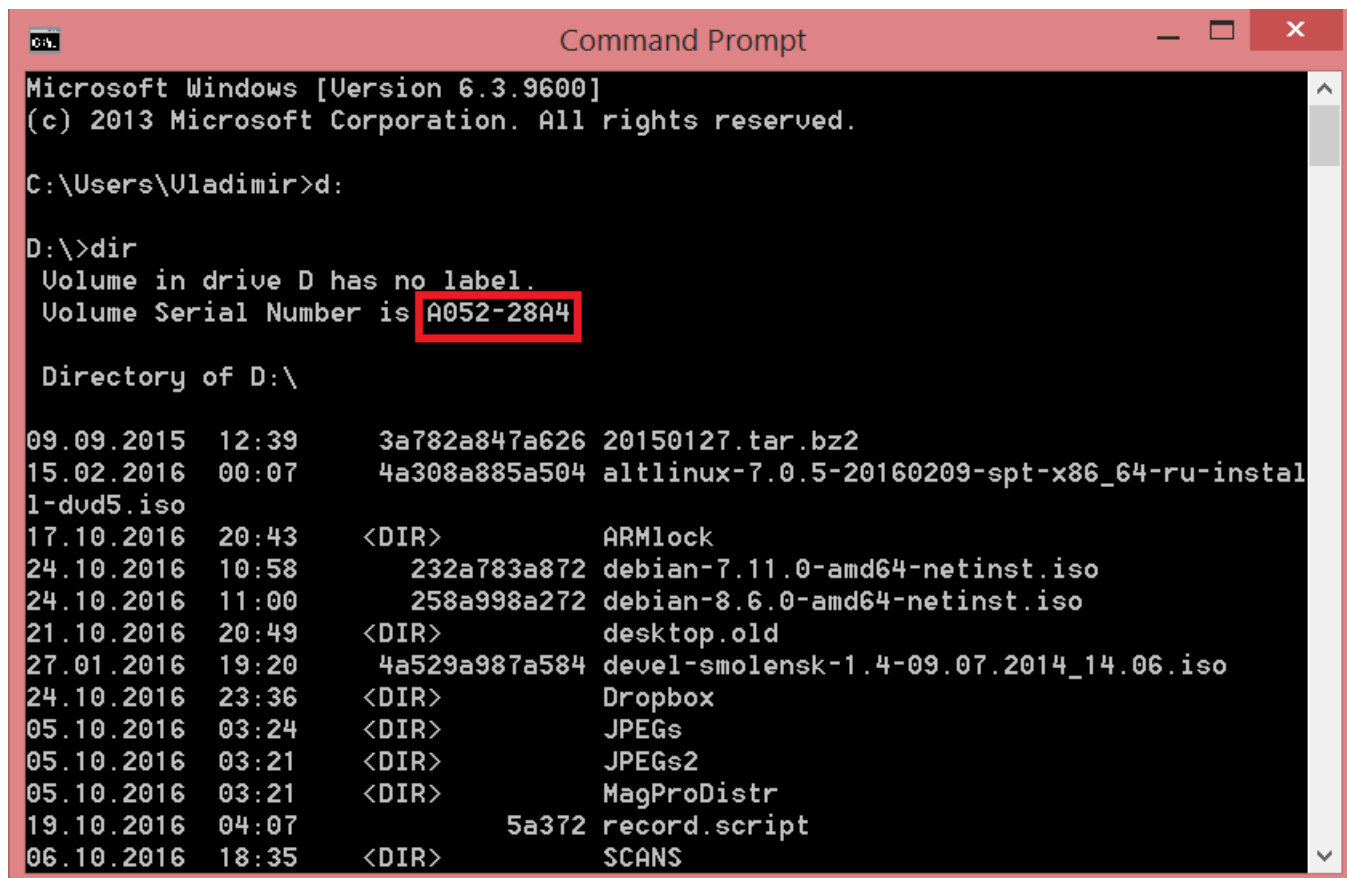
Идентификатор:

Описание:

Рисунок 12.2 - Форма добавления нового объекта

Необходимо в выпадающем списке указать тип объекта, ввести его идентификатор и ввести краткое описание. После этого нажать ЛКМ .

Идентификатор объекта при добавлении вручную можно получить копированием из локальной консоли администратора или воспользовавшись системной утилитой *dir* на одном из рабочих мест с установленной ПЗИ НСД «ARMlock» (для CD/DVD и floppy-дисков). Пример с получением идентификатора диска с помощью утилиты *dir* показан на рисунке 12.3 (идентификатор диска выделен красным цветом).



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Vladimir>d:

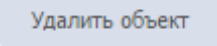
D:\>dir
Volume in drive D has no label.
Volume Serial Number is A052-28A4

Directory of D:\

09.09.2015  12:39      3a782a847a626  20150127.tar.bz2
15.02.2016  00:07      4a308a885a504  altlinux-7.0.5-20160209-spt-x86_64-ru-instal
1-dvd5.iso
17.10.2016  20:43      <DIR>          ARMlock
24.10.2016  10:58      232a783a872  debian-7.11.0-amd64-netinst.iso
24.10.2016  11:00      258a998a272  debian-8.6.0-amd64-netinst.iso
21.10.2016  20:49      <DIR>          desktop.old
27.01.2016  19:20      4a529a987a584  devel-smolensk-1.4-09.07.2014_14.06.iso
24.10.2016  23:36      <DIR>          Dropbox
05.10.2016  03:24      <DIR>          JPEGs
05.10.2016  03:21      <DIR>          JPEGs2
05.10.2016  03:21      <DIR>          MagProDistr
19.10.2016  04:07      5a372 record.script
06.10.2016  18:35      <DIR>          SCANS
```

Рисунок 12.3 – определение идентификатора DVD-диска с помощью утилиты *dir*

12.3 Удаление объекта

Для удаления объекта необходимо в форме просмотра объектов нажать на имени удаляемого объекта и в появившейся форме нажать кнопку  и подтвердить удаление.

12.4 Добавление объекта из меню просмотра журналов событий

Функционал меню просмотра журнала событий Сервера ARMlock позволяет добавлять устройства как объект прямо из записи о событии в журнале, связанного с устройством.

Журнал событий

От 25 Октября 2016	0 : 00	Имя пользователя	Тип устройства	Имя процесса	Уровень логирования
До 25 Октября 2016	23 : 55	Имя компьютера	ID устройства	Сообщение	Фасилити
Время сервера	Информация	Получить логи	Настроить поля	IP адрес	Код операции

Время клиента	Время сервера	Пользователь	Компьютер	IP Адрес	Уровень журналирования	Фасилити	Код операции	Имя процесса	Устройство	Сообщение	Файлы
25.10.2016 02:42:15	25.10.2016 01:42:14	sailor	WIN-A8FHJQCNT41	192.168.1.2	NOTICE	DEVICES	CDEVICEIN	C:\ARMlock2015\Proj10Service.exe	UFD 3.0	Устройство подключено к системе	
25.10.2016 02:42:12	25.10.2016 01:42:11	sailor	WIN-A8FHJQCNT41	192.168.1.2	NOTICE	DEVICES	CDEVICEIN	C:\ARMlock2015\Proj10Service.exe	USB флеш карты: UFD 3.0 Silicon-Power64G USB Device UFD P1401562000000199978&0	Запоминающ.. подключено к системе	
25.10.2016 02:42:12	25.10.2016 01:42:11	sailor	WIN-A8FHJQCNT41	192.168.1.2	NOTICE	DEVICES	CDEVICEIN	C:\ARMlock2015\Proj10Service.exe	UMBus пере..	Устройство подключено к системе	
25.10.2016 02:42:02	25.10.2016 01:41:59	sailor	WIN-A8FHJQCNT41	192.168.1.2	NOTICE	DEVICES	CDEVICEIN	C:\ARMlock2015\Proj10Service.exe	Kingston D..	Устройство подключено к системе	

Рисунок 12.4 – сообщение о подключенном USB-flash устройстве в журнале аудита

Для добавления идентификатора устройства из журнала аудита необходимо в меню просмотра журналов отобразить необходимые события и нажать ЛКМ на имени устройства, которое требуется добавить как объект. (Рисунок 12.5)

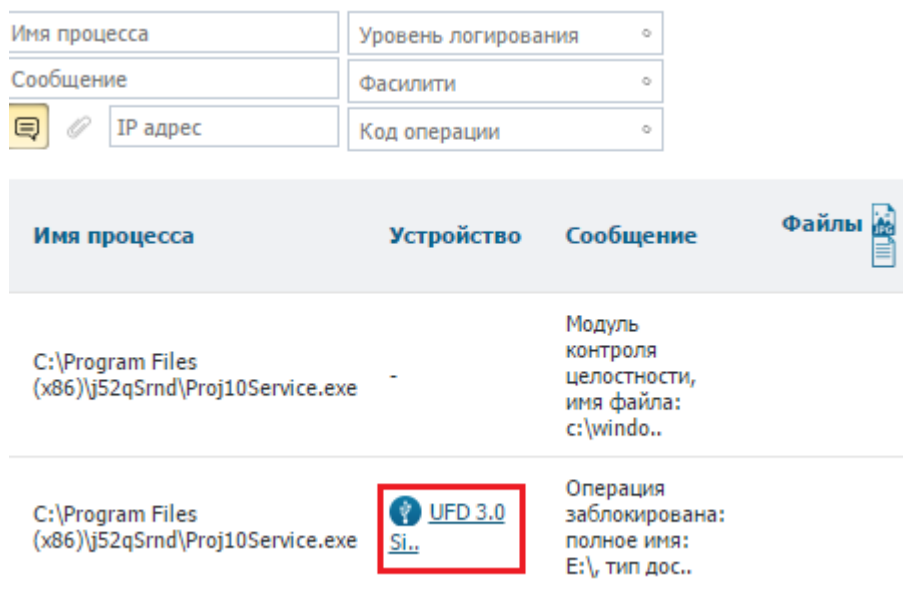


Рисунок 12.5 - добавление нового объекта из журнала

После нажатия по имени устройства появится форма «Добавить новый объект».



Примечание. Для удобства нахождения сообщения о подключенном пользователем устройстве рекомендуем осуществить фильтрацию событий безопасности по имени компьютера и/или имени пользователя, а также коду события: CDEVICEIN.

13 Пользователи

13.1 Назначение инструментария работы с пользователями

Данная оснастка среды администрирования Сервера ARMlock позволяет просматривать информацию о пользователях АРМ под управлением ПЗИ НСД «ARMlock» и редактировать для них политики безопасности, задавать правила доступа, смотреть активность пользователей.

13.2 Просмотр, добавление и редактирование Пользователей


Для входа в оснастку, необходимо в главном меню нажать ЛКМ по пиктограмме оснастки работы с учетными записями Пользователей. (Рисунок 13.1)



Пользователи

Рисунок 13.1 - Пиктограмма для входа в меню работы с учетными записями пользователей АРМ

После входа в оснастку будут отображены данные о заведенных на Сервере ARMlock учетных записях пользователей АРМ под управлением ARMlock, объединенных в локально-вычислительную сеть.

Для добавления нового пользователя необходимо нажать ЛКМ на кнопке .

В появившейся форме ввести имя новой учетной записи и нажать кнопку Сохранить.

В следующей форме ввести параметры учетной записи Пользователя и нажать кнопку

Сохранить

Для редактирования учетной записи Пользователя АРМ необходимо нажать ЛКМ по его имени и в появившейся форме отредактировать параметры, после чего сохранить их.

14 Компьютеры

14.1 Назначение инструментария работы с компьютерами

Данная оснастка среды администрирования Сервера «ARMlock» позволяет просматривать информацию об АРМ под управлением ПЗИ НСД «ARMlock», создавать и редактировать для них политики безопасности, задавать правила доступа.

Каждый компьютер может быть задан по уникальному системному имени, которое можно посмотреть на рабочей станции в «свойствах системы» (Рисунок 14.1)

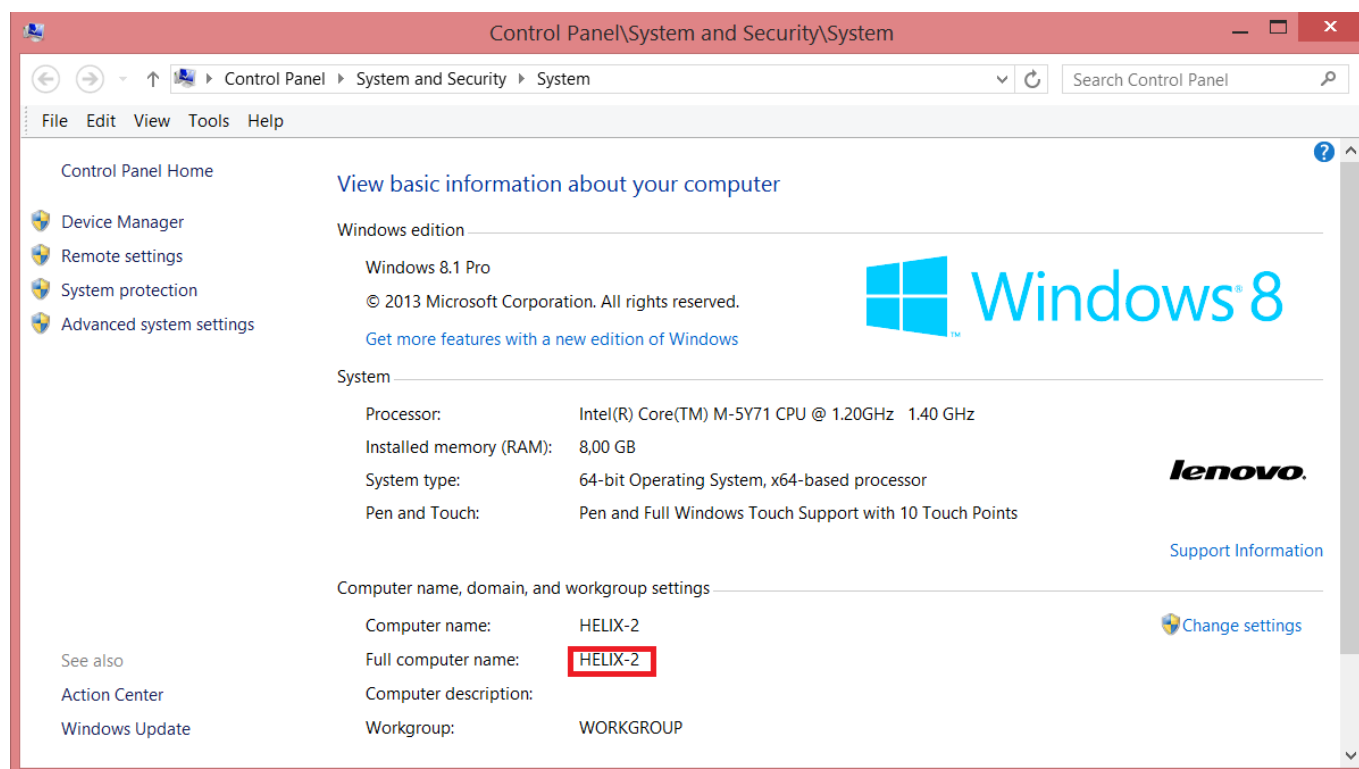


Рисунок 14.1 – Определение имени компьютера в свойствах системы

После того, как рабочая станция заведена в разделе «Компьютеры», ей можно назначать специальные настройки, политики и списки. В ином случае, если компьютер в данном разделе не заведён, но подключается к серверу конфигурации с запросом на получение конфигурации безопасности, сервер ответит конфигурацией для компьютера со специальным именем «__Default__» (по два нижних подчеркивания с каждой стороны). Если такой компьютер в системе не задан – сервер ответит отказом в выдаче конфигурации.

14.2 Просмотр, добавление и редактирование Компьютеров

Для входа в оснастку, необходимо в главном меню нажать ЛКМ по пиктограмме оснастки работы с АРМ. (Рисунок 14.2)



Компьютеры


Рисунок 14.2 - Пиктограмма для входа в меню работы с АРМ под управлением ПЗИ НСД «ARMlock»

После входа в оснастку будут отображены данные о заведенных на Сервере «ARMlock» АРМ под управлением ПЗИ НСД «ARMlock».


Для добавления нового АРМ необходимо нажать ЛКМ на кнопке .

В появившейся форме ввести имя добавляемого компьютера и нажать кнопку .

В следующей форме ввести параметры добавляемого компьютера и нажать кнопку

 Сохранить

Для редактирования АРМ необходимо нажать ЛКМ по его имени и в появившейся форме отредактировать параметры.

В меню редактирования компьютера также доступна кнопка , которая позволяет удалённо выключить или перезагрузить компьютер (рисунок 14.3)

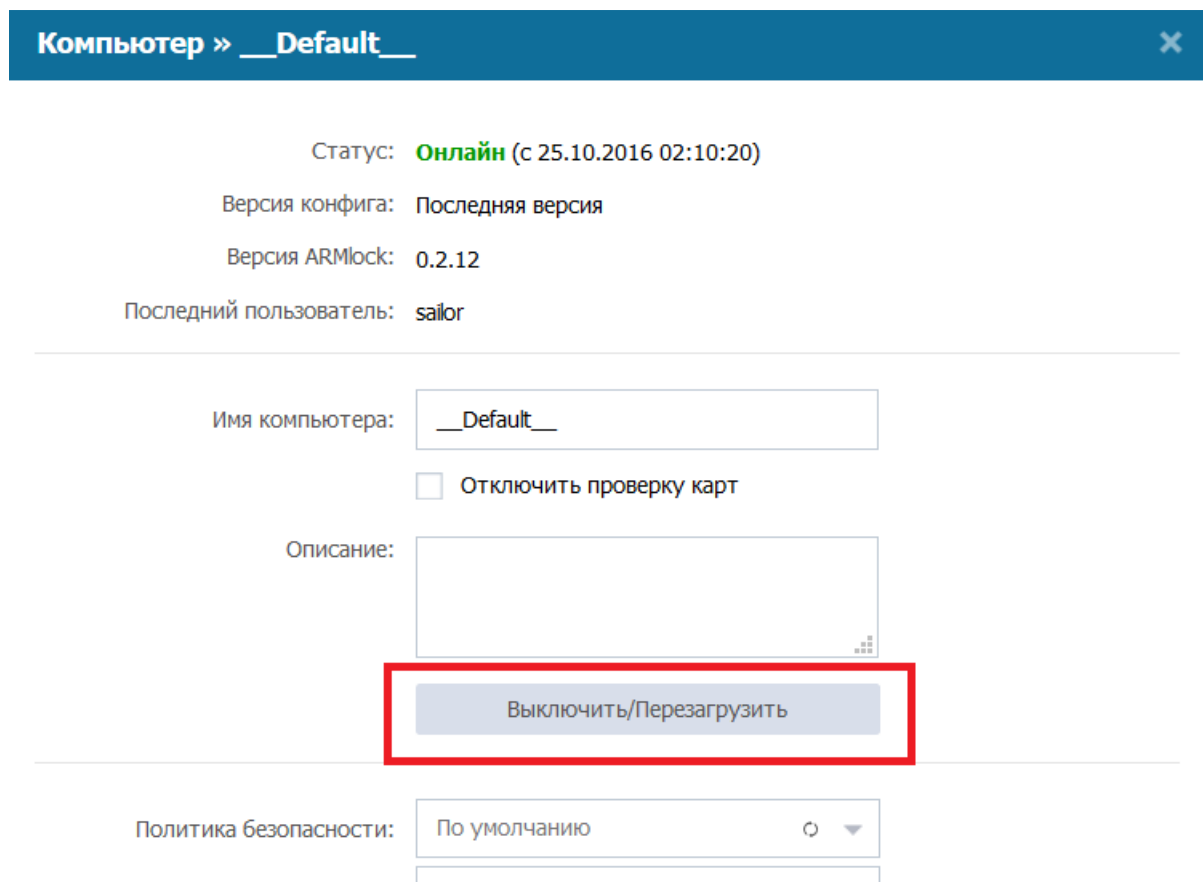


Рисунок 14.3 – Кнопка выключения и перезагрузки рабочей станции

15 Группы пользователей и компьютеров

15.1 Назначение групп пользователей и компьютеров

Группы пользователей и компьютеров предназначены для удобства распространения однотипных политик и настроек для типовых объектов управления и субъектов доступа.

Пользователи и компьютеры могут входить в группы. Например, Вы можете создать отдельную группу компьютеров, обрабатывающих персональные данные, и применить для них политику запрета подключения любых внешних устройств. Или создать группу пользователей финансово-экономической службы и присвоить им список объектов доступа с заданными правами.

Чтобы включить того или иного пользователя (или компьютер) в группу, необходимо зайти в меню настройки пользователя (или компьютера) и в нижней части меню нажать на «Добавить» (Рисунок 15.1 и 15.2)

Компьютер >> __Default__

Статус: **Онлайн** (с 25.10.2016 02:10:20)

Версия конфига: Последняя версия

Версия ARMlock: 0.2.12

Последний пользователь: sailor

Имя компьютера:

Отключить проверку карт

Описание:

Политика безопасности:

Параметры журналирования:

Параметры клиента:

Списки объектов:

Контроль целостности:

Группы: Компьютер не состоит в группах. **Добавить?**

Рисунок 15.1 – Добавление компьютера в группу

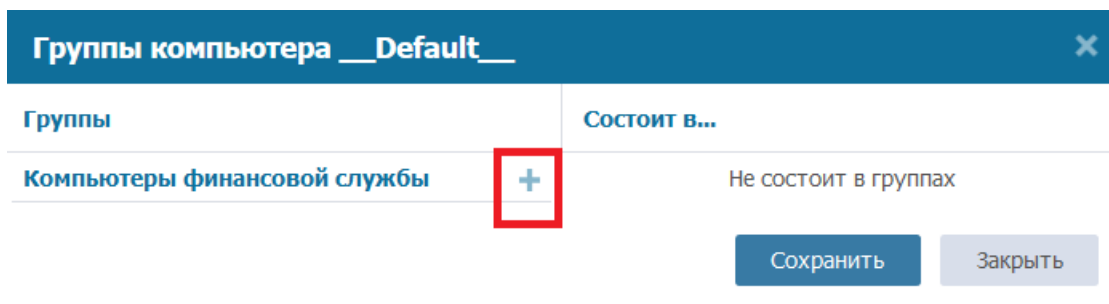


Рисунок 15.2 – Добавление компьютера в группу

15.2 Управление группами пользователей и компьютеров

Созданным группам пользователей и компьютеров можно присваивать специальные настройки, политики и списки (Рисунок 15.3)

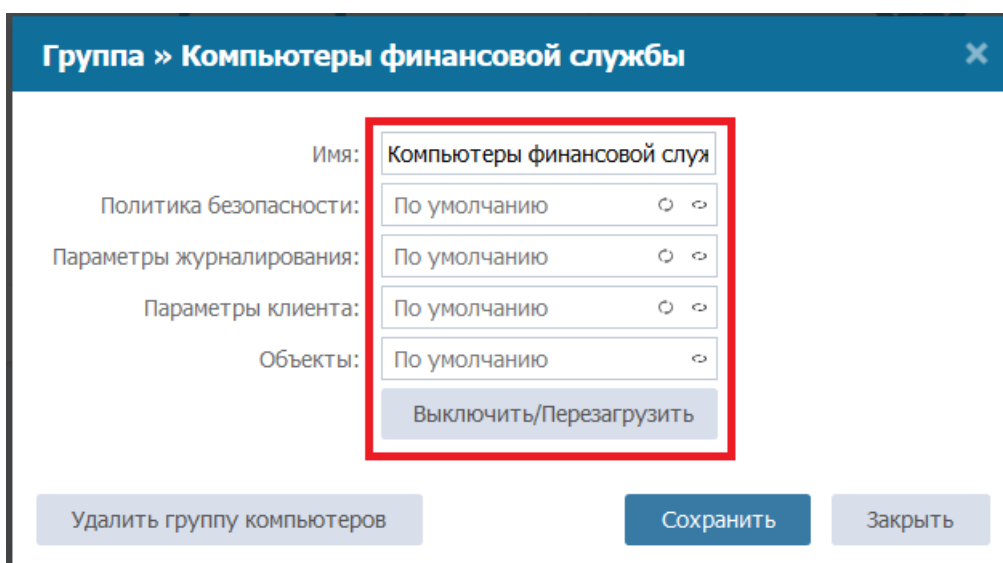


Рисунок 15.3 – Управление группой

При генерировании профиля безопасности для конкретного АРМ, обращающегося на Сервер «ARMlock» с запросом конфигурации, ему будет выдан профиль безопасности, сгенерированный в результате пересечения всех профилей безопасности пользователя, компьютера, групп пользователей и групп компьютеров, в которые входит обратившийся за конфигурацией АРМ и пользователь, работающий на данном АРМ.

Кроме того, интерфейс управления группой компьютеров позволяет осуществлять централизованное отключение или перезагрузку всех компьютеров, входящих в группу.

16 Термины и определения

Термины «компьютер» и «АРМ» считаются равнозначными.

Термин	Формулировка
• АРМ	Автоматизированное рабочее место
• ЛКМ	Левая кнопка мыши
• ПКМ	Правая кнопка мыши
• ПЭВМ	Персональная электронно-вычислительная машина
• Мышь	Ручной манипулятор, преобразующий механические движения в движение курсора на экране
• ОС	Операционная система
• ПЗИ НСД	Система защиты информации от несанкционированного доступа

