ПРОГРАММА ЗАЩИТЫ ИНФОРМАЦИИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
ARMLock

Руководство администратора

RU.60945681.501410-01 34

ARMlock

Листов 62

Содержание

Введение

Данное руководство предназначено для администраторов и пользователей АРМ, на которых установлена Программа защиты информации от несанкционированного доступа ARMlock (далее по тексту – система защиты, СЗИ НСД ARMlock).

В руководстве содержатся сведения, необходимые пользователям для работы на АРМ и администраторам для установки, настройки и администрирования СЗИ от НСД.

Руководство подразумевает наличие у администратора навыков работы в ОС Windows.

В руководстве представлены элементы графических интерфейсов СЗИ НСД ARMlock и операционной системы, которые соответствуют работе СЗИ НСД ARMlock в ОС Windows 7.

1 ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ

1.1 Назначение системы защиты

СЗИ НСД ARMlock представляет собой программное средство защиты информации в ОС семейства Windows.

Система защиты устанавливается на АРМ (как автономные, так и в составе локально-вычислительной сети) для защиты локальных ресурсов этих АРМ.

СЗИ НСД ARMlock предназначена для защиты персонального компьютера:

- от доступа к информации в нарушение установленных прав доступа к информации;
- от доступа к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения;
- от подключения незарегистрированных в системе защиты носителей информации;
- от доступа к информации в объеме, превышающем необходимый для выполнения служебных обязанностей.

В соответствии с требованиями безопасности организации, работниками, ответственными за установку и эксплуатацию системы защиты, настраиваются соответствующие параметры и политики безопасности, реализованные в СЗИ НСД ARMlock.

Лицом, ответственным за управление системой защиты, считается администратор безопасности. Эту функцию могут выполнять и несколько сотрудников подразделения по защите информации организации.

Оператором СЗИ НСД ARMlock является пользователь защищенного СЗИ НСД ARMlock АРМ, осуществляющий вход в систему, ввод и обработку информации любыми программными средствами.

1.2 Условия работы

1.2.1 Данные для учетной записи

Чтобы получить доступ к АРМ, на которое установлена СЗИ НСД ARMlock, необходимо иметь зарегистрированную в системе защиты учетную запись. Внесение в базу СЗИ учетных записей и их атрибутов доступа осуществляется администратором безопасности.

Учетная запись пользователя, зарегистрированного в СЗИ НСД ARMlock, имеет набор атрибутов, которые необходимы непосредственно для входа на защищенный компьютер. (Таблица 1.1)

Таблица 1.1 - Список атрибутов доступа, используемых в СЗИ 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)
Персональный идентификатор	Необязательный атрибут, представляющий из себя устройство в виде NFC-карты, прикладываемой к считывателю. Пользователю могут быть выданы один или несколько таких идентификаторов.

Авторизация пользователя осуществляется при каждом входе. Имена и пароли должны отвечать требованиям, приведенным в Таблица 1.1Таблица 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! Пользователю необходимо уточнить у администратора безопасности все атрибуты доступа для входа на защищенный компьютер.

Запомнить свое имя в системе защиты и пароль.

Не допускается сообщать пароль и передавать персональный аппаратный идентификатор другим лицам. В случае компрометации любого из атрибутов доступа необходимо немедленно сообщить об этом администратору безопасности.

1.2.2 Права учетной записи

Перед началом работы пользователю необходимо выяснить у администратора безопасности, какими именно правами и привилегиями обладает пользователь, к каким ресурсам может иметь доступ и с какими программами и приложениями работать.

Во всех сложных ситуациях, связанных с работой системы защиты, которые пользователь не в состоянии разрешить самостоятельно, необходимо обращаться к администратору. Так, в частности, если имеющихся прав доступа к ресурсам недостаточно для эффективного выполнения должностных обязанностей (запрещающие сообщения), необходимо обратиться к администратору безопасности или другому должностному лицу, отвечающему за распределение прав доступа к ресурсам компьютера и сети.

2 УСТАНОВКА И УДАЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ

2.1 Подготовка компьютера к установке СЗИ НСД ARMlock

2.1.1 Требования к аппаратному и программному обеспечению

СЗИ НСД ARMlock может быть установлена на АРМ, портативные ПК (ноутбуки), и виртуальные машины (например, в системе виртуализации VMware), работающие как в автономном режиме, так и в составе локально-вычислительной сети.

СЗИ НСД ARMlock может работать на любом компьютере, работающем под управлением следующих ОС:

- Microsoft Windows XP;
- Microsoft Windows Server 2003 R2 (SP2);
- Microsoft Windows Server 2008 (SP2);
- Microsoft Windows Server 2008 R2 (SP1);
- Microsoft Windows 7 (SP1);
- Microsoft Windows 8;
- Microsoft Windows 8.1 Update;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 (R2);
- Microsoft Windows 10.

Требования к производительности аппаратного обеспечения зависят от версии операционной системы Windows, на которую установлена СЗИ НСД ARMlock.

Для размещения файлов системы и ее работы требуется не менее 30 Мбайт пространства на системном разделе жесткого диска. В случае использования СЗИ НСД ARMlock на АРМ в составе ЛВС необходимо установить сетевой протокол TCP/IP и сконфигурировать интерфейс подключения к ЛВС.

При необходимости подключения считывателя аппаратных идентификаторов (NFC-карт в режиме двухфакторной аутентификации) требуется наличие свободного USB-порта в аппаратной части АРМ.

2.1.2 Ограничения

СЗИ НСД ARMlock имеет следующие ограничения при установке:

1. Корректная работа СЗИ в режиме двухфакторной аутентификации гарантируется только со считывателем марки ACS модели ACR-1251U-M2.

2.1.3 Предварительная подготовка

Перед установкой СЗИ НСД ARMlock необходимо выполнить следующие действия:

1. СЗИ НСД ARMlock является сложным многокомпонентным программно-техническим изделием. Поэтому при его установке и использовании могут возникнуть ошибки, в т.ч. приводящие к потере данных. Перед началом установки СЗИ НСД ARMlock скопируйте все документы, файлы, программы и иные данные представляющие действительную или потенциальную ценность для пользователя и/или организации на внешний энергонезависимый отчуждаемый носитель и убедитесь в их целостности. Регулярно осуществляйте резервное копирование таких данных в процессе эксплуатации СЗИ НСД.
2. Если на компьютере уже установлена какая-либо система защиты от НСД, ее необходимо удалить.
3. Необходимо убедиться, что на жестком диске имеется необходимое свободное пространство для установки системы защиты.
4. Рекомендуется проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты.
5. Рекомендуется произвести дефрагментацию диска.
6. Проверить АРМ на наличие вирусов САВЗ.
7. Закрыть все запущенные программы, так как установка системы потребует принудительной перезагрузки.

8. Перед установкой СЗИ НСД ARMlock рекомендуется создать точку восстановления системы (Мой компьютер (правая кнопка мыши) --> Свойства --> Защита системы --> Создать точку восстановления. В случае ошибки установки вы сможете восстановиться из резервной копии (для этого вам может понадобиться установочный диск Windows).

9. Если планируется использовать СЗИ НСД ARMlock в режиме двухфакторной аутентификации необходимо подключить к USB-порту АРМ считыватель NFC-карт.

2.1.4 Особенности установки

Внимание

Устанавливать систему защиты на АРМ может только пользователь, обладающий правами администратора ОС Windows на этом компьютере. Это может быть как локальный так и доменный пользователь.

Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Корректность запуска установки от имени другого пользователя («Run as») не гарантируется.

Внимание

При использовании сетевой версии СЗИ НСД ARMlock совместно с Межсетевым Экраном необходимо добавить разрешающие правила для TCP-портов, используемых сервером СЗИ НСД ARMlock. (Порядок настройки подключения к серверам СЗИ НСД ARMlock см. в Разделе 11.4)

Рекомендуется перед установкой Армлок перевести межсетевой экран в «режим обучения».

2.2 Установка системы защиты

Для установки СЗИ НСД ARMlock необходимо запустить приложение SetupClient.v.x.x.x.msi (где x.x.x – номер версии СЗИ НСД ARMlock), которое находится в корневой директории дистрибутива.

Если ARMlock устанавливается на ПК, не оснащенный приводом компакт дисков, а дистрибутив поставляется на CD или DVD-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-установщика. 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*»**.**

После запуска файла дистрибутива «SetupClient.v.x.x.x.msi» появится окно приветствия программы установки. (Рисунок 2.1).

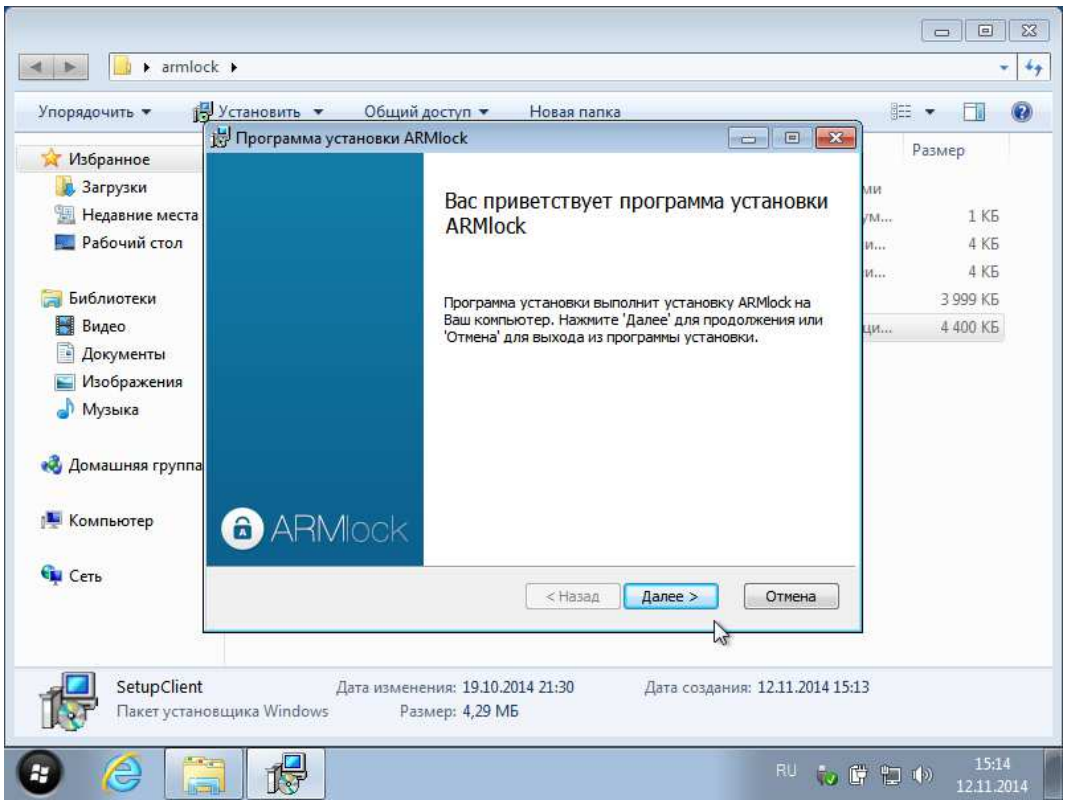

Рисунок 2.1 - Окно начала установки системы защиты

После нажатия кнопки «*Далее*» программа установки выведет окно, содержащее лицензионное соглашение и пункт о его принятии. (Рисунок 2.2) Следует поставить галочку в пункте «Я принимаю условия данного лицензионного соглашения» и нажать кнопку «*Далее*».

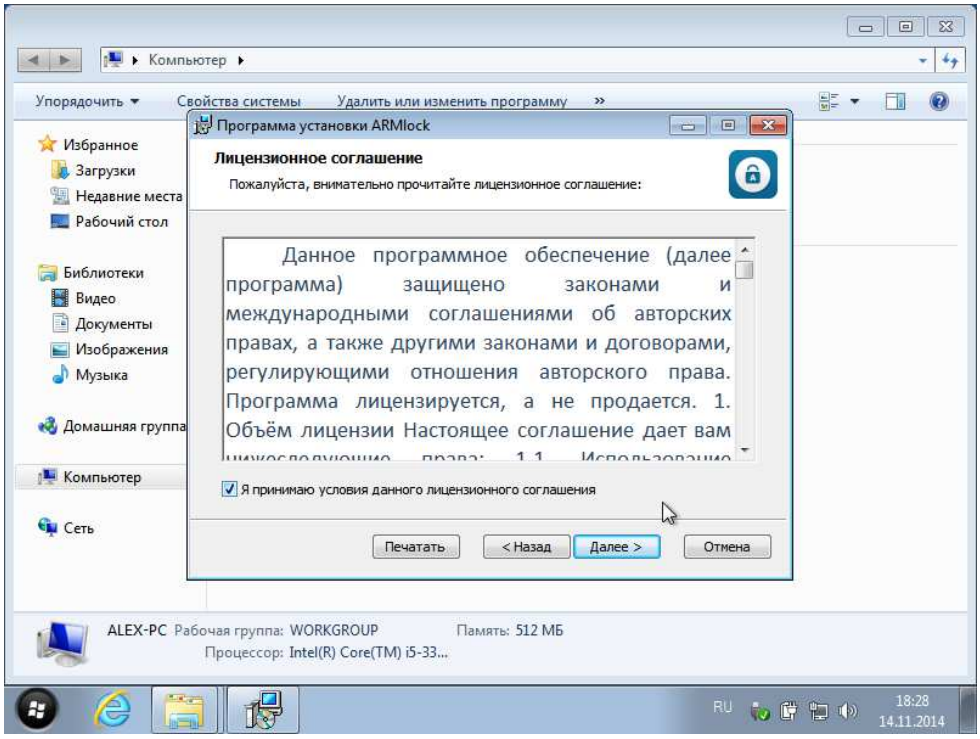

Рисунок 2.2 - Лицензионное соглашение

На текущем окне (Рисунок 2.3) для защиты от нелегального использования продукта необходимо указать программе установки путь к файлу лицензии с расширением **.p12*, содержащий серийный номер СЗИ НСД ARMlock. После ввода пути к файлу лицензии следует нажать кнопку «Далее».

Внимание. В случае если был указан неверный путь к файлу лицензии или сам файл поврежден, программа установки в дальнейшем выдаст сообщение об ошибке (Рисунок 2.5) и процесс установки будет прерван.

Примечание. Файлы лицензий с расширением **.p12* предоставляются заказчику на отдельном носителе. Их следует получить у администратора безопасности.

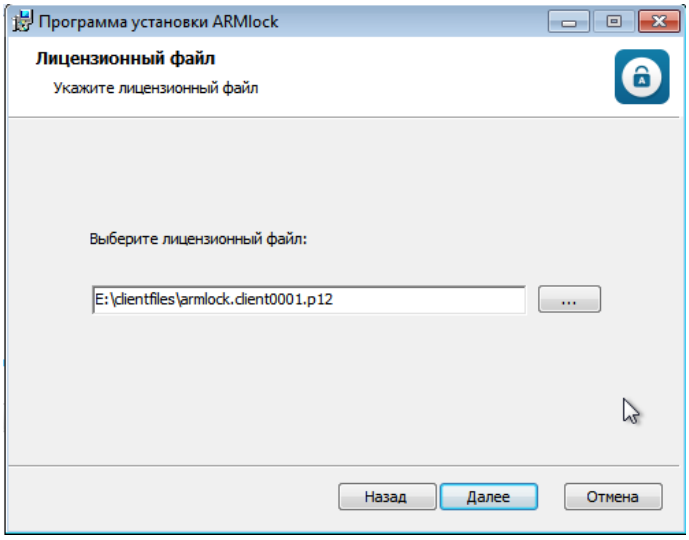

Рисунок 2.3 - Ввод пути к файлу лицензии

В следующем окне установщика будет предложено выбрать режим установки. Доступно 2 режима:

«Режим с аутентификацией по имени и паролю» - выберите режим, если планируется использовать СЗИ НСД ARMlock без применения персональных идентификаторов (NFC-карт) в качестве дополнительного фактора аутентификации.

«Режим с двухфакторной аутентификацией (имя, пароль, идентификатор карты)» - выберите режим, если планируется использовать СЗИ НСД ARMlock с персональными идентификаторами.

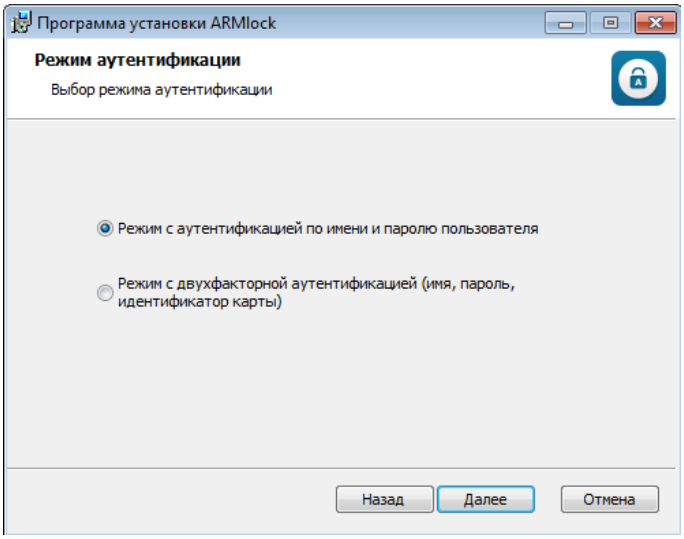

Рисунок 2.4 - Выбор режима аутентификации

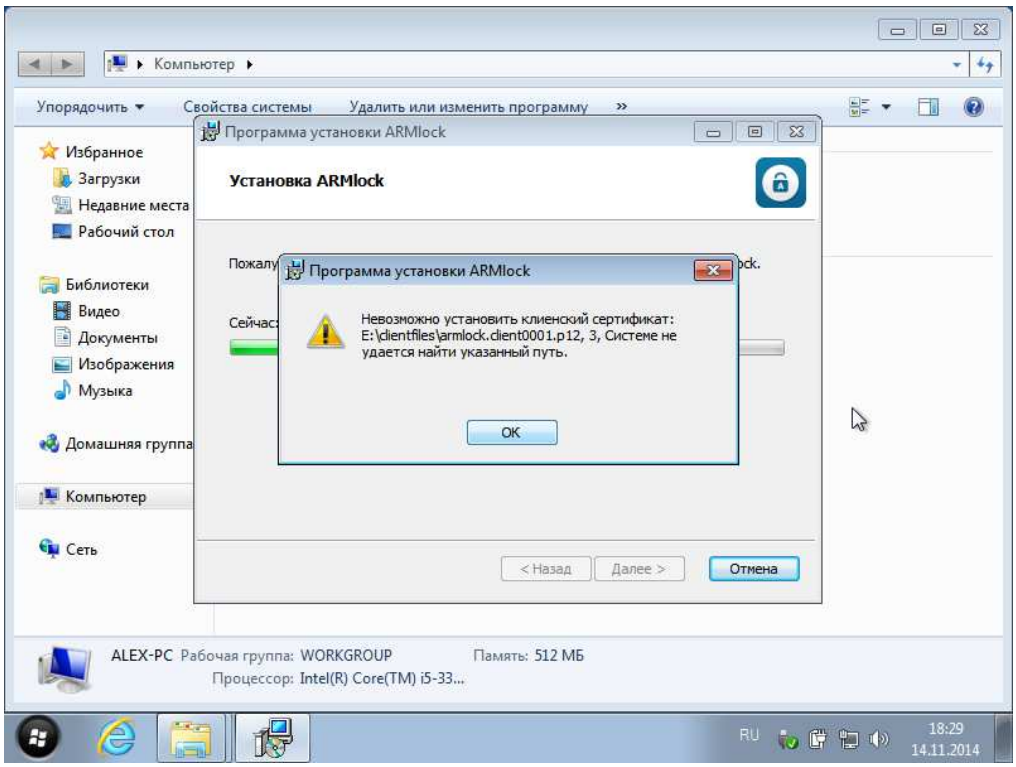

Рисунок 2.5 - Сообщение об ошибке при проверке файла лицензии

На текущем этапе программа установки попросит осуществить ввод параметров установки. (**Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.**).

Требуется выбрать локальную либо клиент-серверную версию для установки.

Если выбрана локальная установка, то пользователю предлагается дополнительно ввести пароль защиты локальных файлов конфигурации. В случае, если этот пароль будет задан при установке, то пользователи, являющиеся локальными администраторами СЗИ НСД ARMlock, впоследствии должны будут вводить данный пароль при входе в локальную консоль администратора. Пароль защиты локальных файлов можно оставить пустым. Для редактирования пароля рекомендуем использовать кнопку «TAB» на клавиатуре. Кнопка «Далее» будет доступна только если оба введённых пароля совпадают.

Если выбрана сетевая версия необходимо также указать адрес и порт подключения к серверу конфигурации СЗИ НСД ARMlock в формате *SEVER1:PORT,* где *«SERVER1»* доменное имя сервера конфигурации (или его IP-адрес), *PORT* - номер TCP-порта, через который осуществляется подключение. После ввода параметров необходимо нажать кнопу «*Далее*».

При выборе клиент-серверного варианта у Администратора безопасности появляется возможность централизованного управления политиками и правилами безопасности с помощью серверной консоли СЗИ НСД ARMlock.

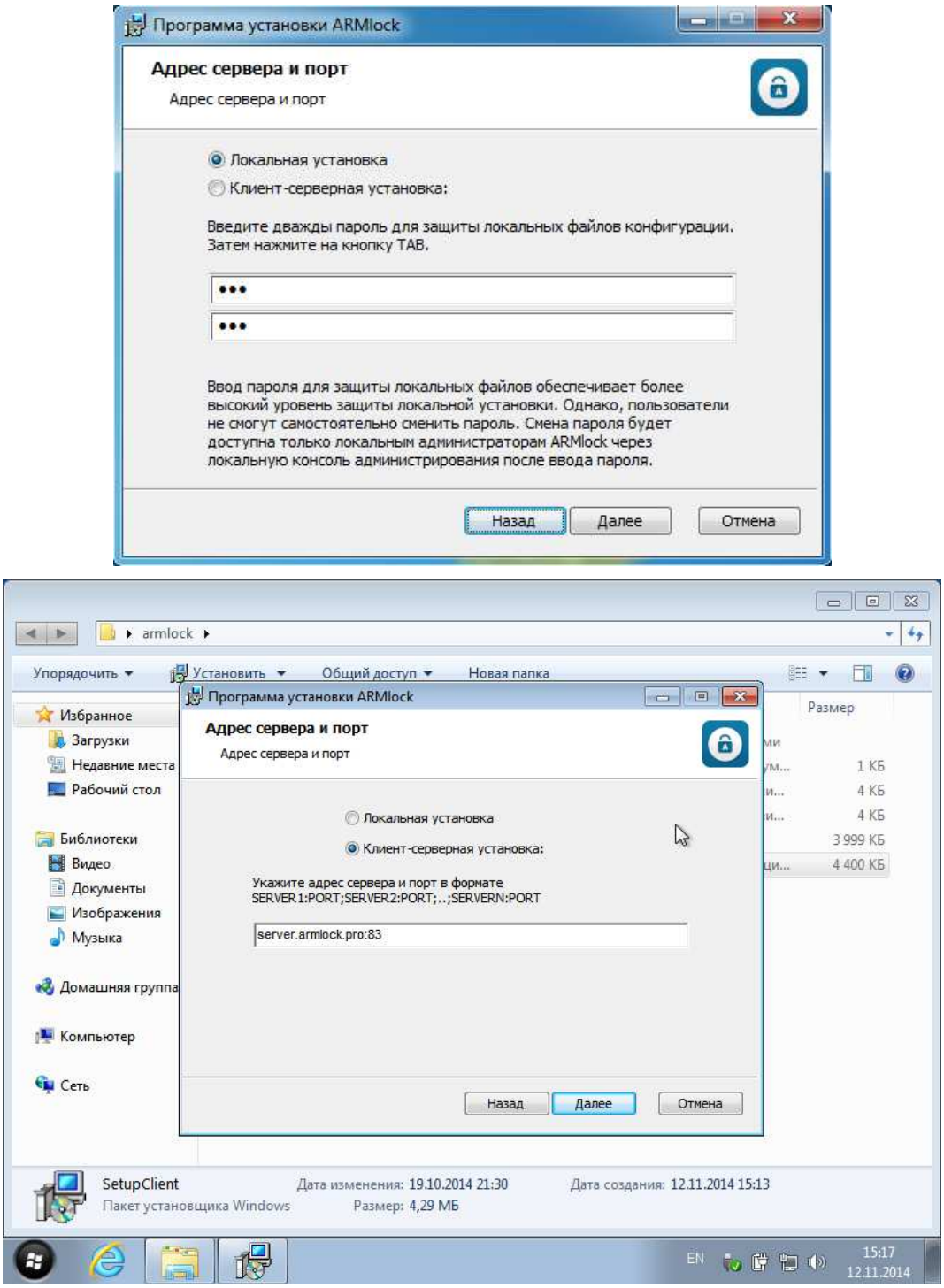

Рисунок 2.6 - Ввод параметров установки

Примечание. Параметры подключения к серверу конфигурации зависят от конкретной ЛВС, их требуется уточнить администратора безопасности.

В следующем окне в случае необходимости можно вручную указать путь установки, если требуется установить СЗИ НСД ARMlock в расположение, отличающееся от расположения указанного по умолчанию. При этом по умолчанию установщик сгенерирует случайное имя папки для усложнения задачи поиска дистрибутива СЗИ потенциальным нарушителем.

Для подтверждения пути установки требуется нажать кнопку «*Далее*». (Рисунок 2.7)

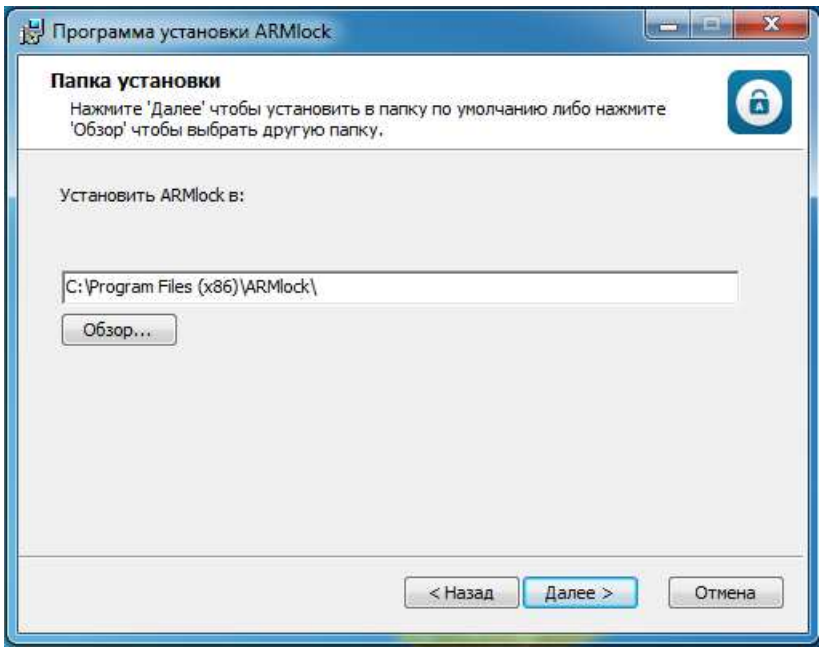

Рисунок 2.7 - Выбор пути установки

На следующем окне программа установки предложит подтвердить введенные в ходе установки параметры либо вернуться в предыдущие меню и изменить их. В случае необходимости изменения данных нужно нажать кнопку «*Назад*». В случае если введенные данные корректны следует нажать кнопку «*Начать*». (Рисунок 2.8 - Подтверждение параметров установкиРисунок 2.8)

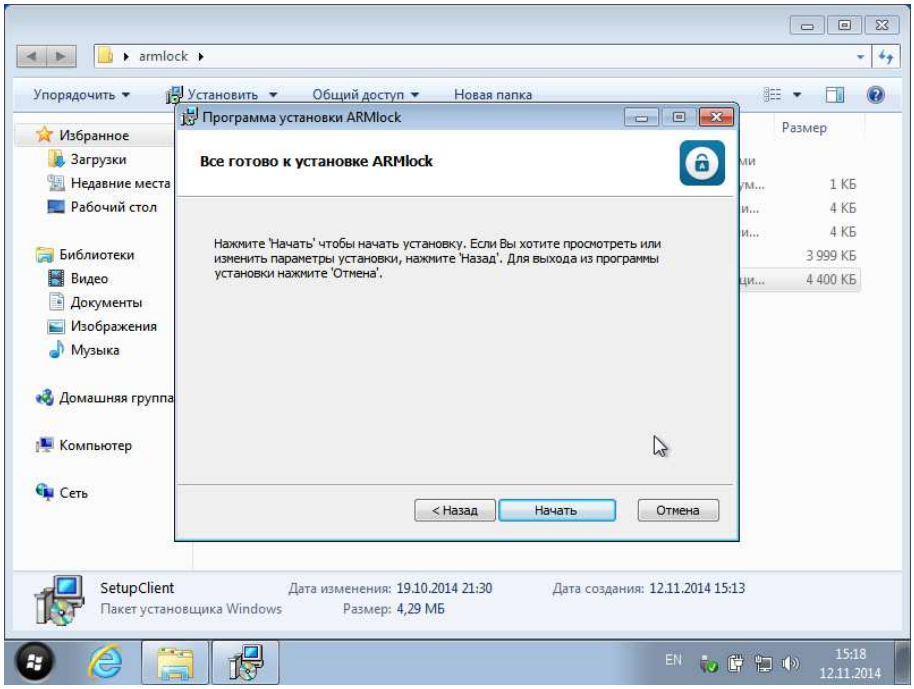

Рисунок 2.8 - Подтверждение параметров установки

После нажатия кнопки «Начать» запустится процесс установки СЗИ НСД ARMlock, ход которого отображается строкой состояния в том же окне. (Рисунок 2.9)

Внимание. Для установки и работы СЗИ НСД ARMlock в двухфакторном режиме требуется наличие подключенного к АРМ считывателя. В противном случае вход ни под одной из учетных записей, зарегистрированных в системе, будет невозможен.

В процессе копирования файлов будет выведено сообщение с просьбой проверки подключения считывателя аппаратных идентификаторов. Требуется проверить подключение считывателя к usb-порту АРМ и нажать кнопку «ОК».

В ходе копирования файлов возможно появление всплывающего окна консоли Windows с черным фоном, содержащее сообщения об установке необходимых служб и драйверов. При их появлении дополнительных действий со стороны пользователя не требуется.

В случае, если пользователем выбрана установка в режиме двухфакторной аутентификации, однако программа установки не обнаружила подключенный считыватель – произойдёт откат установки.

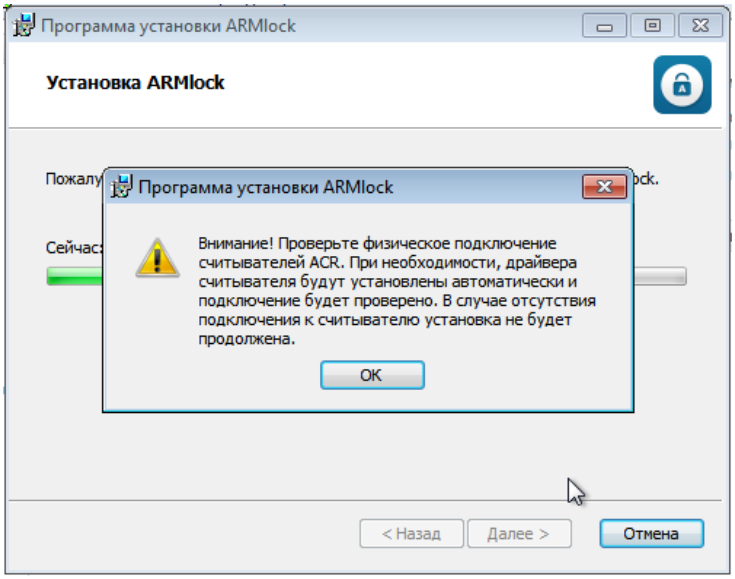

Рисунок 2.9 - Копирование файлов

В случае, если система запросит разрешение на установку программного обеспечения на данном компьютере – убедитесь, что установщик подписан проверенным издателем «ООО Вэлл-Сервис» и нажмите «Да» (Рисунок 2.10)

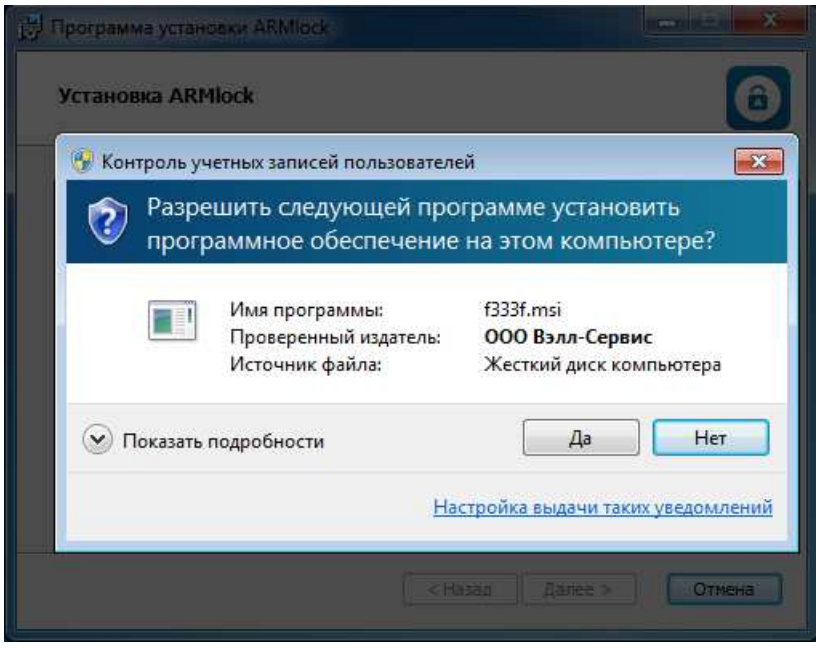

Рисунок 2.10 - Запрос разрешения на установку

После завершения копирования необходимых файлов появится окно, информирующее об успешном окончании установки. Для завершения установки СЗИ от НСД нажмите кнопку «*Готово*». (Рисунок 2.)

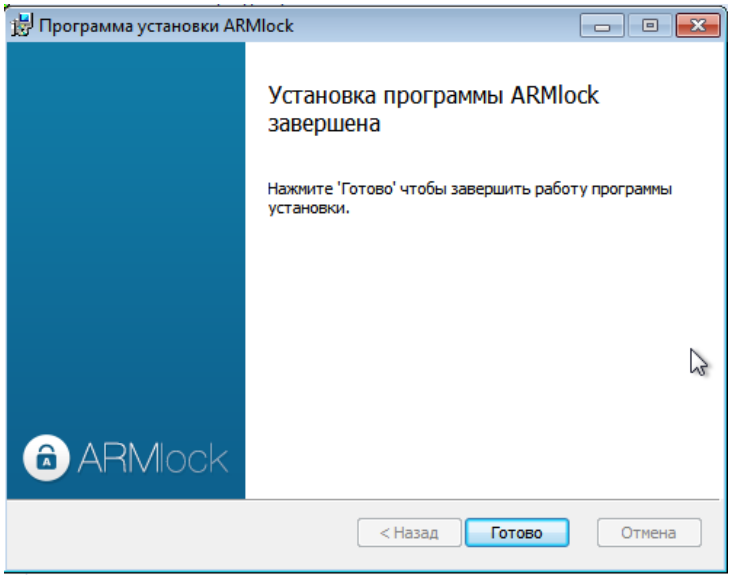

Рисунок 2.11 - Завершение установки программы

Для завершения установки потребуется перезагрузка ОС. После нажатия кнопки «*Готово*» в окне завершения установки программы (Рисунок 2.12) ОС предложит выполнить перезагрузку. Нажмите кнопку «*Да*» если хотите выполнить перезагрузку немедленно. Если хотите выполнить Перезагрузку вручную позже нажмите «*Нет*». (Рисунок 2.11)

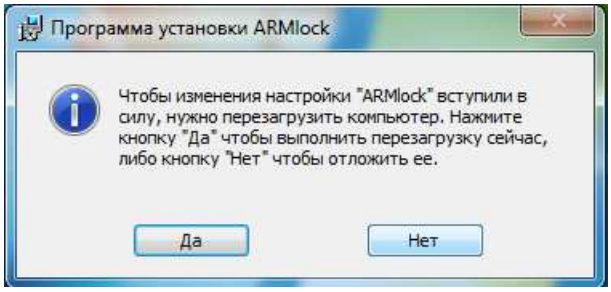

Рисунок 2.11 - Диалог перезагрузки

После перезагрузки первый вход на защищенный компьютер сможет осуществить локальный пользователь, под учётной записью, под которой была произведена установка СЗИ НСД ARMlock, либо это возможно с помощью специально созданной при установке учетной записи с именем пользователя «*armlock*» и паролем «*ARMl0ck!*». В случае сетевой установки, вход может осуществить либо доменный пользователь, если АРМ является клиентом контроллера домена и администратор добавил данные об необходимых атрибутах доступа пользователя (включая аппаратный идентификатор) в базу данных AD, либо пользователь, заведённый на сервере СЗИ НСД ARMlock (в зависимости от настроек, произведённых на сервере СЗИ НСД ARMlock. Для получения более подробной информации обратитесь к руководству по серверу СЗИ НСД ARMlock).

После установки системы защиты и перезагрузки компьютера в окне входа в систему появится логотип СЗИ НСД ARMlock.

2.3 Удаление системы защиты

Перед удалением системы защиты рекомендуется завершить работу всех приложений и сохранить результаты, так как удаление СЗИ НСД ARMlock потребует принудительной перезагрузки компьютера.

Удаление производится с помощью файла-дистрибутива «SetupClient.v.x.x.x.msi» (где x.x.x – номер версии). Дистрибутив более новой версии СЗИ НСД ARMlock способен в том числе корректно удалить более старые версии.

Внимание. Для удаления СЗИ НСД ARMlock требуется наличие прав администратора для учетной записи, под которой выполняться удаление, а также прав «локального администратора» в СЗИ НСД ARMlock.

Необходимо открыть в программе «Проводник» папку с дистрибутивом СЗИ НСД ARMlock и запустить файл «*SetupClient.v.x.x.x.msi*. (Рисунок 2.123)

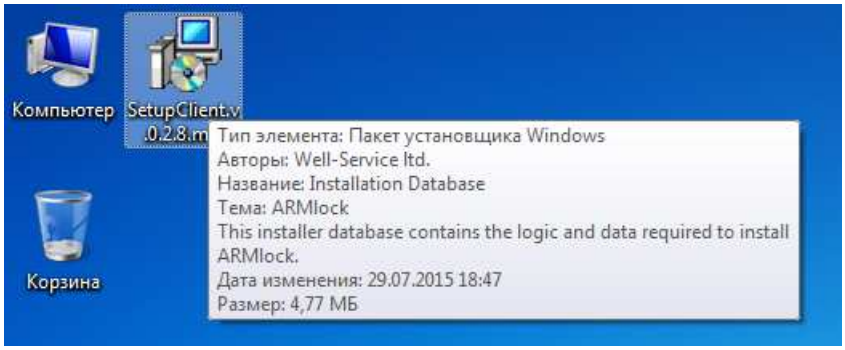

Рисунок 2.123 - Запуск процесса удаления СЗИ НСД ARMlock

После этого запустится программа деинсталляции. Для продолжения процесса удаления нажмите в появившемся окне кнопку «*Удалить*». (Рисунок 2.134)

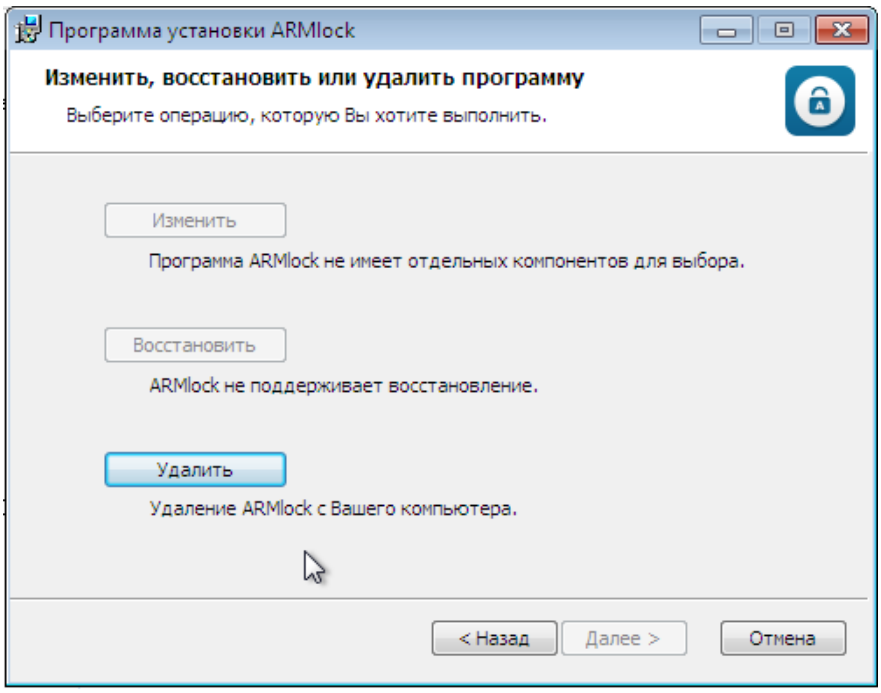

Рисунок 2.134 - Запуск процесса удаления СЗИ НСД ARMlock

В появившемся диалоговом окне можно отметить опцию «Удалить локальных пользователей, созданных ARMlock...». В случае выбора этой опции, учетные записи пользователей ОС Windows, созданные в процессе работы СЗИ НСД ARMlock, будут удалены. (Рисунок 2.145)

Внимание. Перед тем как выбрать пункт «Удалить локальных пользователей, созданных ARMlock...» убедитесь, что в системе зарегистрированы учетные записи, под которым будет возможно осуществить вход в ОС после удаления СЗИ НСД ARMlock.

Для продолжения удаления нажмите кнопку «Далее».

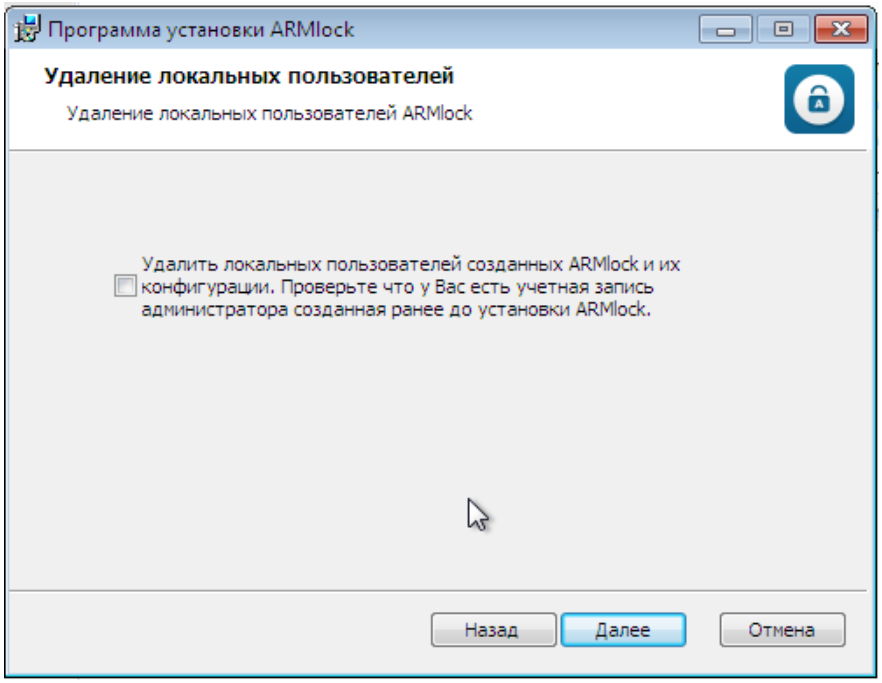

Рисунок 2.145 - Выбор опций удаления

В появившемся окне для продолжения удаления нажмите кнопку «*Удалить*». (Рисунок 2.156)

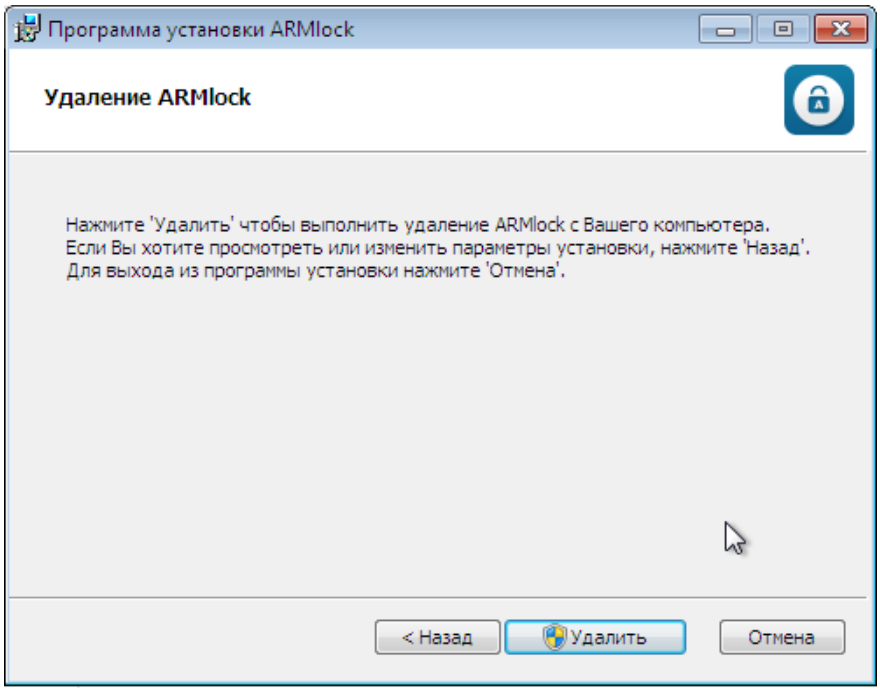

Рисунок 2.156 - Запуск процесса удаления

Появится окно со строкой статуса удаления СЗИ НСД ARMlock. По завершении процесса удаления появится окно. (Рисунок 2.167).

Для завершения процесса удаления нажмите кнопку «Готово».

Внимание. В процессе удаления возможно появление окна консоли Windows с черным фоном. Дополнительных действий со стороны пользователя при этом не требуется.

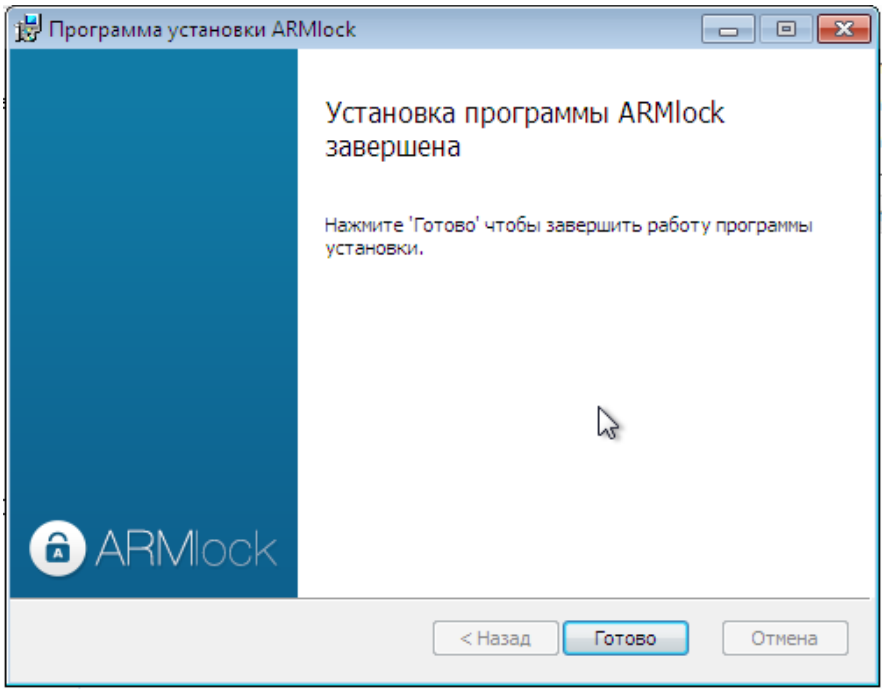

Рисунок 2.167 - Завершение процесса удаления

Окно программы удаления СЗИ НСД ARMlock закроется, пользователю будет предложено выполнить перезагрузку АРМ. Для того чтобы перезагрузить АРМ немедленно нажмите кнопку «Да», если вы хотите выполнить перезагрузку вручную позже нажмите кнопку «Нет».

3 ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР

3.1 Порядок действий пользователя при входе

При загрузке компьютера, защищенного СЗИ НСД ARMlock появляется экран приветствия (Рис. 3.1) с предложением приложить идентификатор к считывателю (в случае двухфакторной аутентификации). Если идентификатор уже приложен или используется режим аутентификации по имени и паролю - сразу появляется экран приглашения на вход в ОС. Рисунок 3.1.

Рисунок 3.1 - Экран приветствия в ОС Windows 7

Рисунок 3.2 - Экран приветствия в ОС Windows 7

Для входа на защищенный СЗИ НСД ARMlock АРМ каждому пользователю предлагается выполнить следующие шаги:

1. Приложить к считывателю аппаратный идентификатор, соответствующий учетной записи пользователя, под которой необходимо выполнить вход. (для случая с двухфакторной аутентификацией)
2. Заполнить поле «Имя пользователя», в соответствии именем пользователя, под которым он зарегистрирован в системе.

Примечание. В этом поле может быть автоматически указано имя пользователя, выполнившего вход последним. В случае использования двухфакторной аутентификации – будет указано имя пользователя, выполнившего вход последним с приложенной картой.

3. Ввести пароль. При вводе пароля, поле для ввода 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.
4. Нажать кнопку «Enter».

После нажатия кнопки «Enter» осуществляется проверка наличия в системе защиты зарегистрированного пользователя с указанным именем. Затем проверяется правильность указанного пользователем пароля. В случае успеха проверки введенных атрибутов доступа пользователю разрешается вход и начинается загрузка рабочего стола пользователя.

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.

Внимание! При отключении аппаратного идентификатора от считывателя в режиме двухфакторной аутентификации, АРМ будет заблокировано. Пользователю будет предложено подключить к АРМ считыватель или связаться со службой технической поддержки.

3.2 Возможные ошибки при входе

Попытка входа пользователя на защищенный компьютер может быть неудачной, к чему приводит ряд событий. При этом на экран могут выводиться сообщения о характере события, или соответствующие сообщения предупреждающего характера.

Если введен неверный пароль, то на экране появится сообщение об ошибке, после чего система предоставит возможность повторно ввести имя и пароль (Рисунок 3.3)

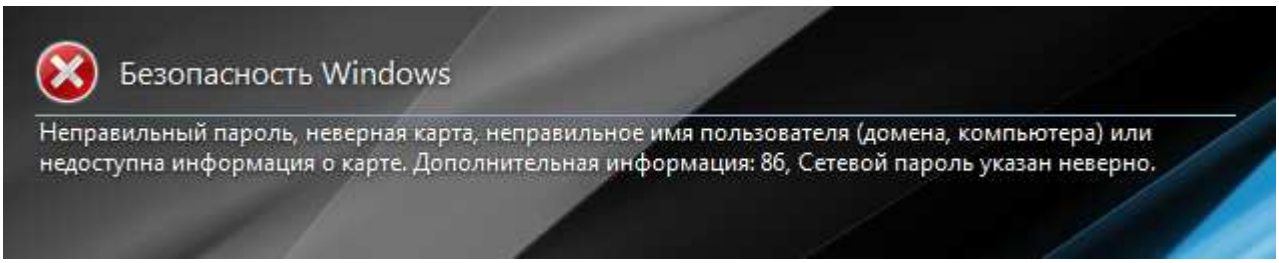

Рисунок 3.3 - Сообщение при вводе неверного пароля

Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он также должен обратиться к администратору, который имеет право назначить пользователю новый

пароль. Так же при ошибочном вводе данных в поле имени или домена могут возникнуть соответствующие сообщения (Рисунок 3.4)

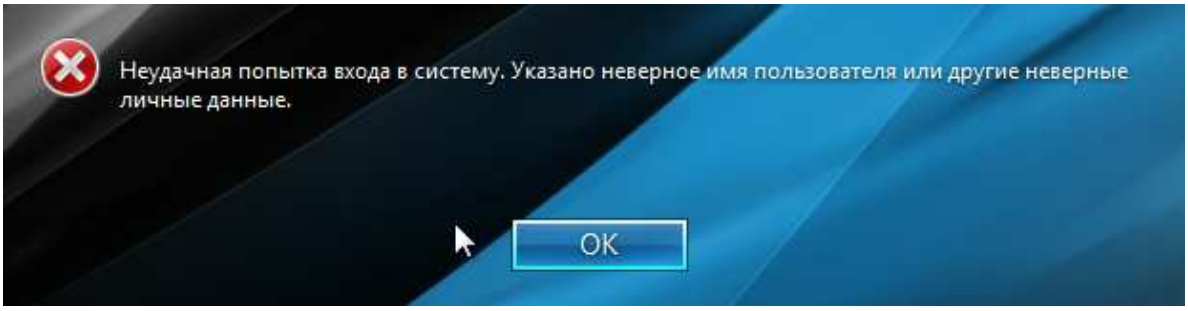

Рисунок 3.4 - Ошибка авторизации

Администратор может отключить учетную запись, в этом случае система выведет при авторизации соответствующее предупреждение (Рисунок 3.5).

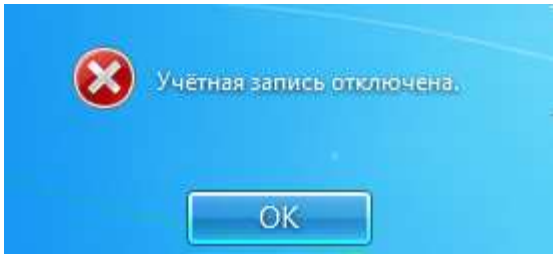

Рисунок 3.5 - Сообщение при попытке входа под отключенной учетной записи

В такой ситуации необходимо обратиться к администратору системы защиты. При проблеме подключения по локальной сети или других может возникнуть ошибка авторизации доменных пользователей (Рисунок 3.6).

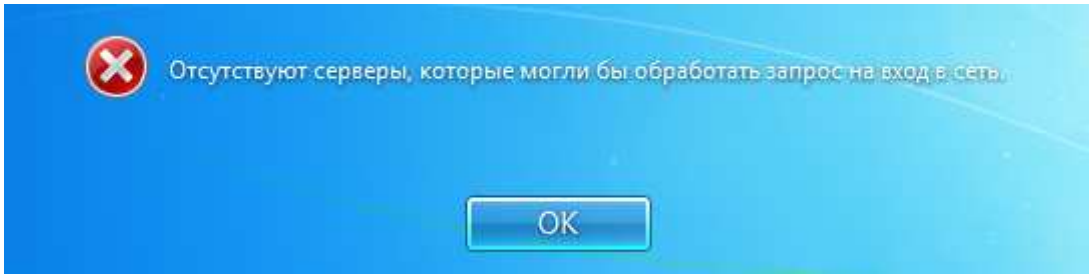

Рисунок 3.6 - Ошибка при вводе имени домена

В этом случае необходимо обратиться к администратору безопасности.

4 ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ

4.1 Завершение работы

При завершении сеанса работы пользователя на компьютере, например в конце рабочего дня, необходимо выполнить **стандартное выключение компьютера**. Для этого нужно:

Сохранить все данные и завершить работу всех приложений, так как выключение не сохраняет результатов работы.

В меню «Пуск» в нижнем правом углу нажать кнопку «Завершение работы».

После нажатия кнопки «Завершение работы» компьютер закрывает все открытые программы, вместе с самой ОС Windows, а затем полностью выключает компьютер и монитор.

4.2 Смена пользователя

Возможно, что завершение сеанса пользователя необходимо для смены пользователя компьютера, то есть для входа на данный компьютер под другой учетной записью.

Для завершения сеанса и смены пользователя, в зависимости от версии операционной системы, необходимо сделать следующее:

В меню «Пуск» в нижнем правом углу нажать вызов меню возле кнопки «Завершение работы» и выбрать пункт «Сменить пользователя» (Рисунок 4.1**Ошибка! Источник ссылки не найден.**).

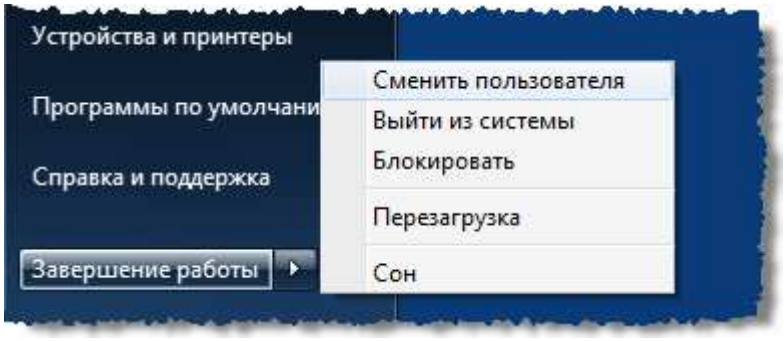

Рисунок 4.1 - Смена пользователя в ОС Windows 7

Сеанс текущего пользователя будет завершен, а на экране появится диалог для повторной авторизации в системе защиты. Перед сменой пользователя рекомендуется сохранить все необходимые данные и закончить работу приложений.

5 СМЕНА ПАРОЛЯ

Пользователь может самостоятельно сменить свой пароль для авторизации.

Для этого, после входа в операционную систему, необходимо нажать комбинацию клавиш «Ctr-Alt-Del» и выбрать операцию «Сменить пароль» (Рисунок 5.1).

Рисунок 5.1 - Меню действий

На экране появится диалоговое окно, предлагающее ввести данные для смены пароля (Рисунок 5.2 - Экран смены пароля в Windows 7).

Рисунок 5.2 - Экран смены пароля в Windows 7

На появившемся экране необходимо ввести в соответствующие поля имя пользователя, старый пароль, новый пароль и подтверждение нового пароля.

	Примечание. Для смены присвоенного пользователю аппаратного идентификатора необходимо воспользоваться консолью администратора СЗИ НСД ARMlock.

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

	Примечание. В соответствии с политиками безопасности могут быть включены настройки сложности паролей. Сложные пароли при их регулярной смене снижают вероятность успешной атаки на пароль. Поэтому при смене пароля пользователю необходимо выяснить у администратора безопасности дополнительные требования для установления паролей. К таким требованиям относятся: – максимальный/минимальный срок действия пароля; – напоминать о смене пароля за определенный срок; – минимальная длина пароля (количество символов); – необходимое наличие цифр; – необходимое наличие спецсимволов (*, #, @, %, ^, & и пр.); – необходимое наличие строчных и прописных букв; – необходимое отсутствие цифры в первом и последнем символе; – необходимое изменение пароля не меньше чем на определенное количество символов, в отличие от предыдущего пароля.

Если все требования соблюдены, то пароль пользователя будет успешно сменен, и появится соответствующее сообщение (Рисунок 5.3 - Успешная смена пароля).

Рисунок 5.3 - Успешная смена пароля

Далее вход пользователя на АРМ будет осуществляться с новым паролем.

6 БЛОКИРОВКА КОМПЬЮТЕРА

В некоторых случаях, возникает необходимость временно заблокировать АРМ, без завершения сеанса работы пользователя. Заблокировать защищенный системой защиты компьютер можно 3-мя способами:

1 Снять со считывателя аппаратный идентификатор. (В случае если СЗИ НСД ARMlock используется со считывателем.)

2 Нажать комбинацию клавиш «Win» + «L».

3 Нажать комбинацию клавиш «Ctr+Alt+Del» и на появившемся экране выбрать кнопку «Блокировать компьютер» (Рисунок 6.1 - Меню блокировки экрана).

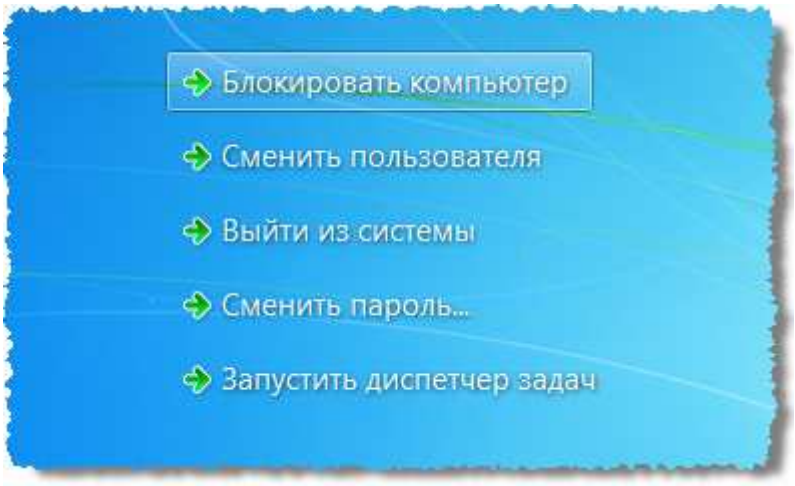

Рисунок 6.1 - Меню блокировки экрана

Кроме того, компьютер может заблокироваться автоматически по истечении заданного периода неактивности пользователя. Период неактивности, после которого компьютер будет автоматически заблокирован, задается стандартными средствами операционной системы (Рисунок 6.2).

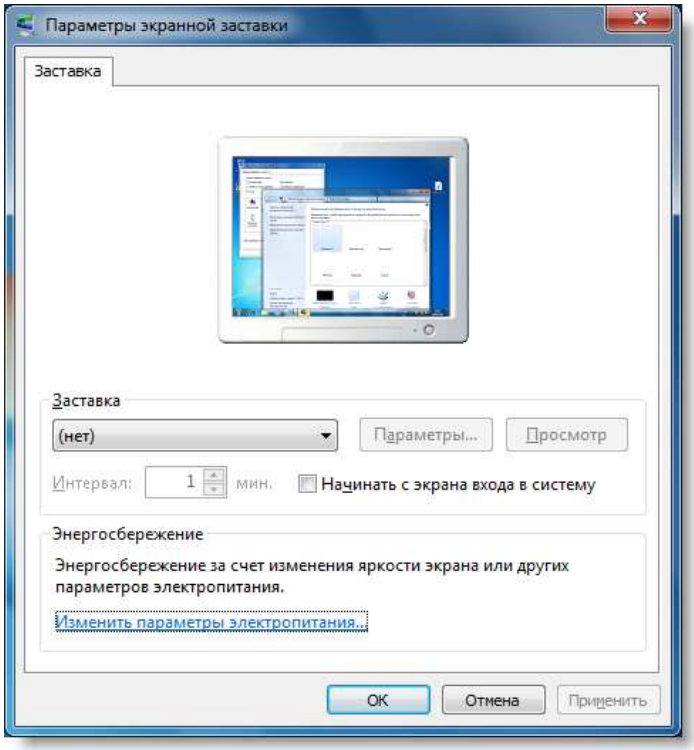

Рисунок 6.2 - Параметры автоматической блокировки экрана

Для разблокировки компьютера, нужно, как и при авторизации (обычном входе на компьютер), ввести имя пользователя, домен (для доменного пользователя), пароль и приложить к считывателю аппаратный идентификатор, если он назначен.

7 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

В СЗИ НСД ARMlock реализовано несколько дополнительных возможностей, позволяющих пользователю увеличить уровень защищенности информации путем нейтрализации угрозы восстановления исходных данных из остаточной информации в оперативной памяти и накопителей АРМ.

7.1 Механизм очистки остаточной информации

Для быстродействия ОС Windows при удалении файла не удаляет содержимое файла непосредственно, а всего лишь удаляют запись с его именем и расположением из таблицы размещения файлов.

До того момента, пока пространство, помеченное в таблице размещения файлов как пустое, не будет несколько раз перезаписано другими данными, содержимое файла остается на накопителе и его можно при помощи специальных утилит просмотреть и восстановить.

В СЗИ НСД ARMlock реализована функция очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Если пользователю необходимо удалить какие-либо файлы без возможности их восстановления (выполнить гарантированное удаление) нужно выполнить следующие действия:

1 В контекстном меню объекта файловой системы, который необходимо удалить, выбрать пункт «Удалить с обнулением» или «Удалить по алгоритму Шнейера». (Рисунок 7.1)

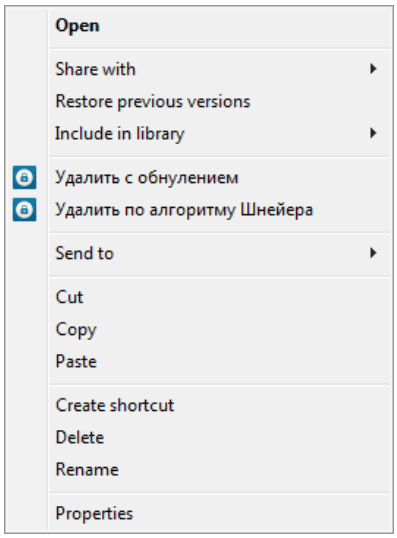

Рисунок 7.1 - Контекстное меню

2 Нажать «*Да*» в появившемся окне подтверждения операции (Рисунок 7.2 - Окно подтверждения операции).

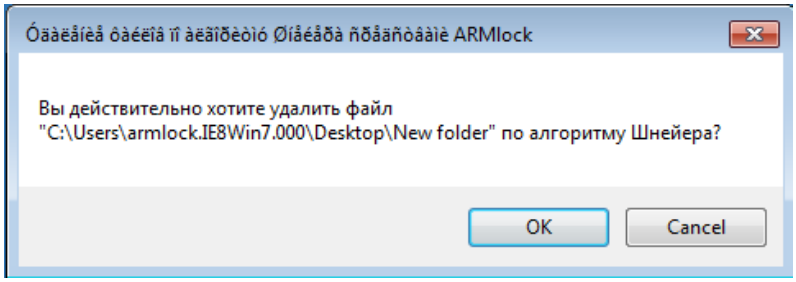

Рисунок 7.2 - Окно подтверждения операции

При активации удаления происходит зачистка данного объекта по выбранному алгоритму (Шнейера или заполнения нулями). После определенного количества циклов перезаписи по одному из алгоритмов восстановить даже фрагмент файла без применения специальных аппаратных средств восстановления становится практически невозможно.

Примечание. При нескольких одновременно выделенных объектах происходит удаление и зачистка всех выделенных объектов как группы.

Для гарантированного удаления требуется чтобы пользователь имел необходимые права доступа к удаляемым файлам. В случае отсутствия необходимых прав будет выведено сообщение об ошибке при удалении (Рисунок 7.3 - Ошибка удаления - отсутствуют права доступа). Для удаления такого файла необходимо выполнить настройку прав доступа пользователя.

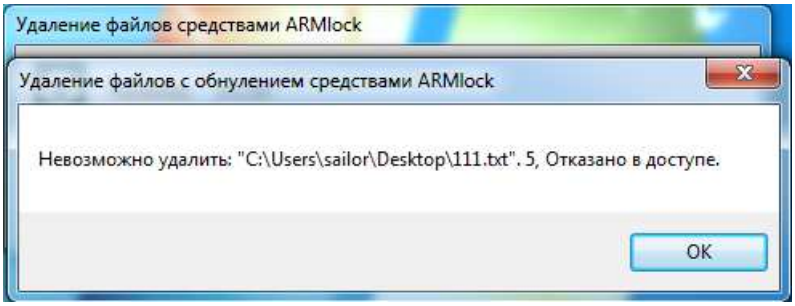

Рисунок 7.3 - Ошибка удаления - отсутствуют права доступа

7.2 Механизм очистки оперативной памяти

Данный механизм позволяет очищать содержимое памяти после завершения процесса. Это позволяет исключить несанкционированный доступ к процессам одного пользователя к информации, содержащейся в оперативной памяти АРМ если осуществляется вход под другой учетной записью пользователя без выключения компьютера.

Для включения механизма очистки оперативной памяти необходимо запустить консоль администрирования СЗИ НСД ARMlock двойным нажатием ЛКМ на файле «*console.exe*». Далее открыть в панели параметров группу «*Настройки*» и выбрать параметр *«Очистка памяти»*. (Рисунок 7.4)

Настройки	
Проверка карты	Локальная проверка карты
Проверка пароля	Локальная проверка пароля. Только пользователи, заведенные в ARMlock
Время повторной попытки связи	60
Сообщение о неподключенном считывателе	Считыватель не подключен. Телефон для связи: 444-44-44
Телефон для связи	Телефон для связи: 888-88-88
Время для отображения сообщения	4000
Логирование процессов	Отключено
Проверка цифровой подписи	Отключено
Очистка памяти	Отключено

Рисунок 7.4 - Включение механизма очистки оперативной памяти

Если вы хотите использовать механизм очистки оперативной памяти, необходимо в выпадающем списке выбрать для параметра «*Очистка памяти*» значение «*Включено*». Для отключения механизма требуется выбрать значение «*Отключено*».

8 Описание структуры и средств администрирования СЗИ НСД ARMlock

8.1 Описание структуры СЗИ НСД ARMlock

Структура СЗИ НСД ARMlock состоит из набора отдельных модулей, приведенных в таблице ниже.

Таблица 8.1 - Основные элементы СЗИ НСД ARMlock

Наименование	Описание
Локальная консоль администрирования	Программное средство администрирования, необходимое для изменения файлов конфигурации СЗИ НСД ARMlock
Локальный сервис СЗИ НСД ARMlock	Процесс на АРМ, реализующий необходимый функционал СЗИ НСД ARMlock
Credential Provider	Модуль, реализующий ввод и проверку учетных данных в среде Windows 7, Windows 8, Windows 8.1 и Windows 10, а также соответствующих серверных версиях Windows (Windows 2008, Windows 2012)
Gina	Модуль, реализующий ввод и проверку учётных данных в среде Windows XP и Windows 2003 Server
Модуль контроля доступа к объектам	Надстройка к ядру ОС. Обеспечивает контроль доступа к файлам, папкам и устройствам, а также скрытие рабочей папки СЗИ НСД ARMlock
Драйвер считывателя карт	Драйвер, необходимый для работы со считывателем аппаратных идентификаторов. Поставляется сторонним производителем.

8.2 Средства администрирования

Локальная настройка и управление СЗИ НСД ARMlock осуществляются с помощью консоли, поставляемой вместе с дистрибутивом. Для открытия консоли скопируйте на жесткий диск и запустите файл «*Console.v.x.x.x.exe*» (где x.x.x – номер версии локальной консоли администратора).

Для запуска локальной консоли администратора пользователь должен иметь права локального администратора. После установки локальной версии СЗИ НСД ARMlock такими правами обладают два пользователя: пользователь, под которым выполнялась установка СЗИ НСД ARMlock, а также специально созданный пользователь «armlock».

При запуске локальной консоли администратора может потребоваться ввести пароль защиты локальных файлов, который был задан при установке СЗИ.

Основные элементы интерфейса консоли администратора приведены на Рисунок 8.1 - Интерфейс консоли управления

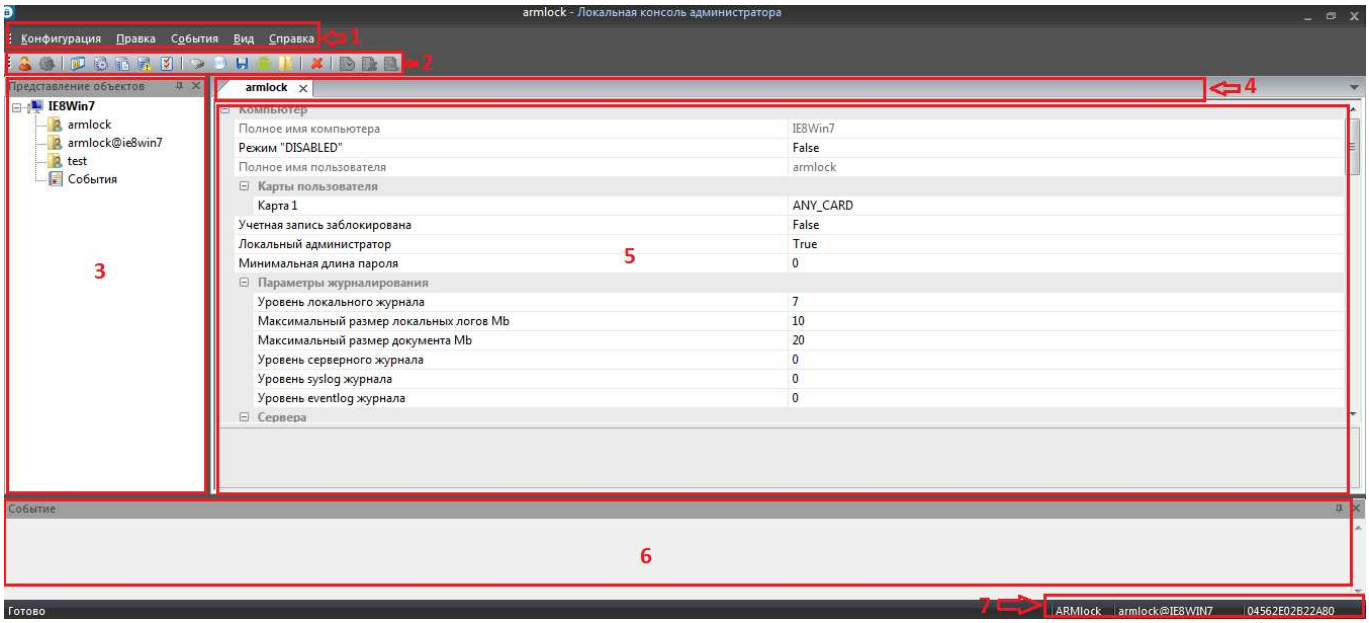

Рисунок 8.1 - Интерфейс консоли управления

Функциональное назначение элементов интерфейса консоли администрирования описано в ТаблицеТаблица 8.2. (Нумерация в таблице приведена в соответствии с нумерацией на Рисунок 8.1)

Таблица 8.2 - Описание элементов консоли администратора

№	Наименование	Описание
1	Системное меню	Набор основных инструментов для настройки и управления СЗИ НСД ARMlock
2	Панель инструментов	Панель инструментов для вызова основных функций СЗИ НСД ARMlock (добавление носителей, присвоение аппаратных идентификаторов и т. д.)
3	Представление объектов	Перечень АРМ и пользователей АРМ, доступных для редактирования. Журнал событий в объекте «*События*»
4	Вкладки открытых редактируемых объектов	Открытые для редактирования АРМ и пользователи
5	Параметры редактируемых объектов	Полный перечень настроек и параметров редактируемых объектов
6	События	Детализация данных об открытой записи при просмотре журнала событий
7	Информация о текущем пользователе	Имя учетной записи текущего пользователя и код его аппаратного идентификатора

Примечание. Объектами для редактирования настроек являются отдельные пользователи и АРМ. В случае редактирования настроек АРМ измененные параметры будут актуальны для АРМ до момента входа на него пользователя, после выхода пользователя из системы, а также для тех пользователей ОС, для которых не создано отдельных файлов конфигурации пользователей в СЗИ НСД ARMlock. Если же редактируются настройки отдельного пользователя, введенные настройки будут

	действовать только для данного отдельного пользователя.

9 Управление доступом

9.1 Управление учетными записями

9.1.1 Создание и удаление локальных пользователей

Внимание! Запуск консоли администрирования СЗИ НСД ARMlock возможен только из под учетной записи локального администратора СЗИ НСД ARMlock.

Для создания учетной записи нажмите на иконку «Создать нового пользователя» в панели инструментов. (Рисунок 9.1)

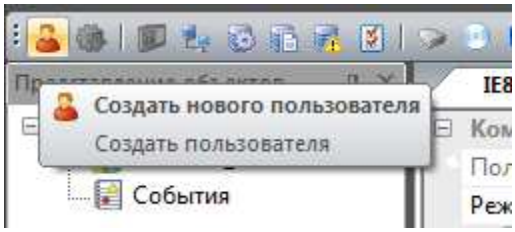

Рисунок 9.1 - Создание новой учетной записи

Появится окно создания нового пользователя с полями ввода атрибутов доступа создаваемого пользователя. (Рисунок 9.2)

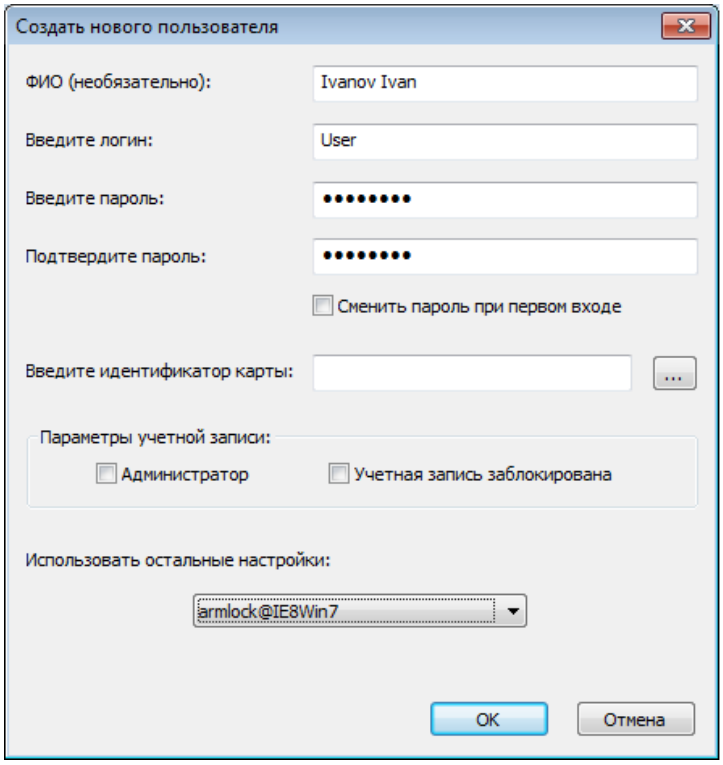

Рисунок 9.2 - Ввод атрибутов доступа учетной записи

В появившемся окне необходимо ввести или выбрать следующие соответствующие учетной записи атрибуты доступа. Описание атрибутов доступа приведено в Таблица9.1.

Таблица9.1

Наименование поля/параметра	Описание
ФИО	ФИО пользователя, вводятся для удобства управления учетными записями
Логин	Имя под котором идентифицируется пользователь
Пароль	Комбинация символов по которой аутентификация пользователя
Подтвердить пароль	Поле повторного ввода пароля, необходимо для проверки соответствия задуманной и реально введенной парольной комбинации символов
Сменить пароль при первом входе	В случае если пользователь сам выбирает себе пароль - необходимо отметить данный пункт. При первом входе под созданной учетной записью пользователю будет предложено ввести новый пароль.
Введите идентификатор карты	В данном поле требуется ввести ключ аппаратного идентификатора, соответствующего пользователю. В случае использования режима аутентификации только по имени и паролю - оставьте поле незаполненным. (Подробнее см. раздел 9.2.2)
Параметры учетной записи	В данном разделе необходимо выбрать права доступа пользователей. Если учетной записи необходимо предоставить права локального администратора СЗИ НСД ARMlock - отметьте поле «Администратор»
Использовать остальные настройки	В выпадающем списке вам будет предложено выбрать источник-шаблон для загрузки остальных настроек учетной записи. Можно выбрать глобальные настройки для всего АРМ, либо можно скопировать настройки другого пользователя СЗИ НСД ARMlock.

После ввода аутентификационных данных необходимо нажать кнопку *«ОК»*. Учетная запись пользователя добавится в панель объектов настроек консоли администрирования (список пользователей и АРМ).

9.1.2 Блокирование/разблокирование локальных пользователей

Для блокирования учетной записи необходимо щелкнуть левой кнопкой мыши на имени блокируемой учетной записи в дереве редактируемых объектов консоли администрирования. В панели параметров откроются параметры учетной записи.

В параметрах учетной записи необходимо выставить значение поля *«Учетная запись заблокирована»* в выпадающем списке значение *«Заблокирована»*.(Рисунок 9.3)

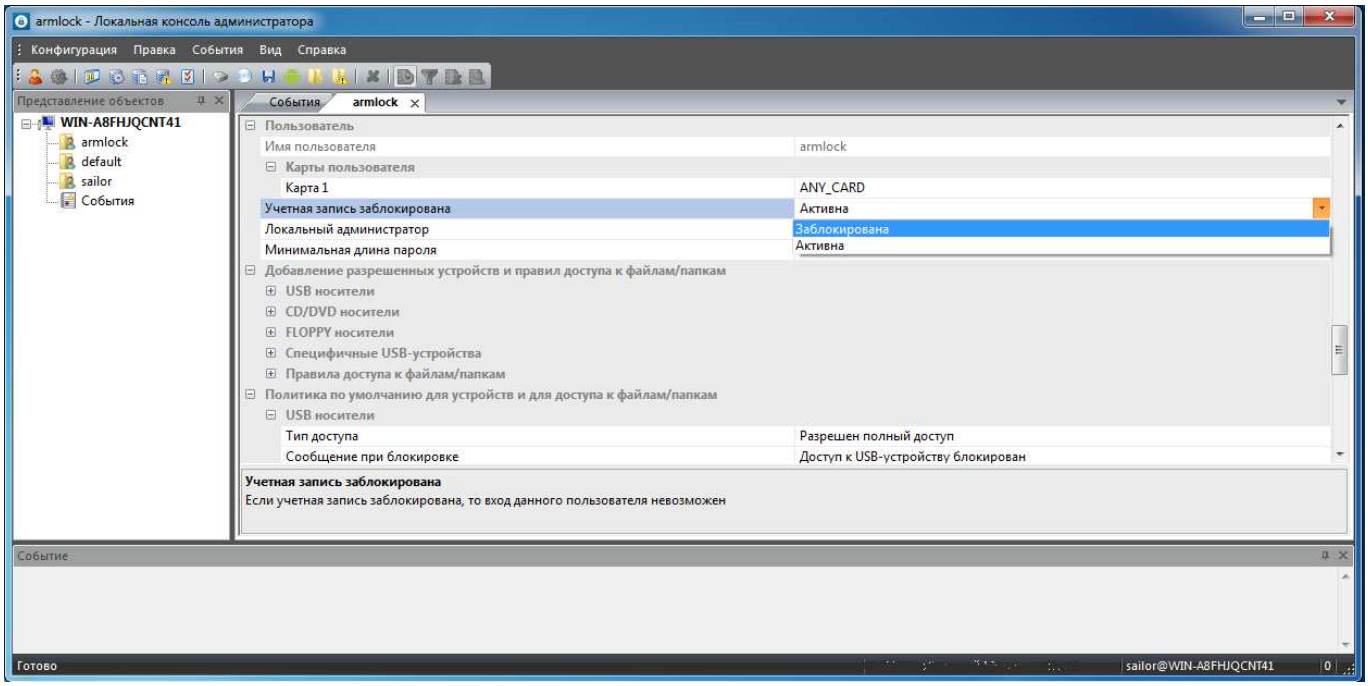

Рисунок 9.3 - Параметр блокировки учетной записи

После выставления параметра необходимо нажать на кнопку «*Сохранить настройки*» в панели инструментов администрирования СЗИ НСД ARMlock. (Рисунок 9.6).

Для разблокирования учетных записей необходимо выполнить все вышеуказанные действия, но выставив значение параметра «*Учетная запись заблокирована*» как *«Активна».*

9.2 Аппаратная идентификация пользователя

Двухфакторная аутентификация является наиболее надежным способом аутентификации, обеспечивающим наибольшую защиту от НСД. В зависимости от выбранных параметров при установке СЗИ НСД ARMlock может применяться как со считывателем аппаратных идентификаторов (режим двухфакторной аутентификации), так и без считывателя, с аутентификацией только по имени и паролю пользователя.

9.2.1 Включение/выключение аппаратной идентификации

9.2.2 Присвоение аппаратного идентификатора пользователю

Для присвоения учетной записи аппаратного идентификатора откройте в дереве объектов настройки консоли учетную запись, которой необходимо присвоить аппаратный идентификатор. Затем нажмите на иконку «*Добавить карту для пользователя*» в панели инструментов консоли администратора. (Рисунок 9.4)

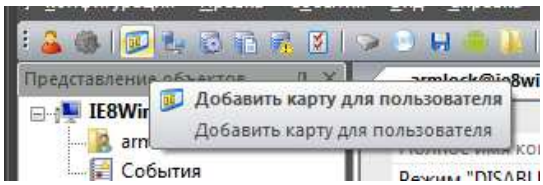

Рисунок 9.4 - Добавление аппаратного идентификатора

Откроется меню выбора аппаратного идентификатора. (Рисунок 9.5)

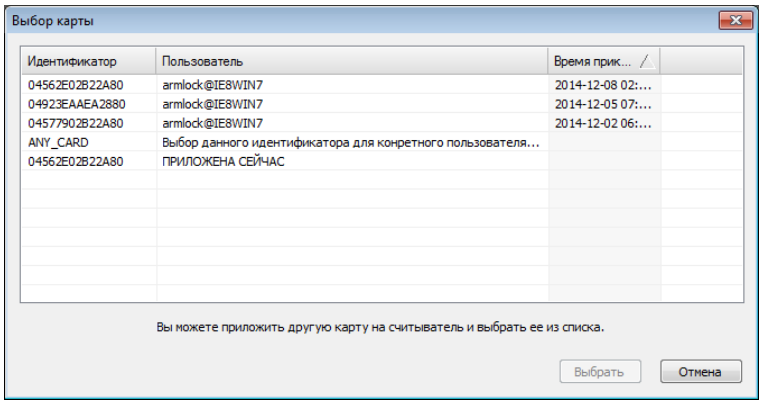

Рисунок 9.5 - Назначение аппаратного идентификатора учетной записи

В данном меню представлен таблица со списком аппаратных идентификаторов. Таблица состоит из 3 столбцов:

1. *«Идентификатор»* - в этом столбце указан код идентификатора присвоенный пользователю и считываемой при аутентификации;
2. *«Пользователь»* - имя учетной записи, которой присвоен идентификатор;
3. *«Время прикладывания»* - время и дата последней аутентификации с данным аппаратным идентификатором.

Аппаратные идентификаторы в списке можно условно разделить на 3 группы:

1. Запись со значение столбца «идентификатор» *«ANY_CARD»* - если выбрать данную запись пользователю для входа подойдет аппаратный идентификатор с любым записанным кодом. Т.е. для аутентификации достаточно будет приложить к считывателю любую карту.
2. Запись со значение столбца «идентификатор» в вид числа в шестнадцатеричном формате и записью в формате *«Имя_пользователя@АРМ»* в столбце «Пользователь». В данной группе представлены аппаратные идентификаторы назначенные какой-либо из учетных записей на АРМ. Таким образом можно не имея самого идентификатора назначить новому пользователю ранее использовавшийся на АРМ аппаратный идентификатор;
3. Запись со значением *«ПРИЛОЖЕНА СЕЙЧАС»* в столбце «Пользователи» - выберите эту запись чтобы назначить пользователю аппаратный идентификатор, приложенный к считывателю.

Выбрав в списке требуемый идентификатор необходимо нажать кнопку «Выбрать», после чего в панели инструментов консоли администратора нажать на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6)

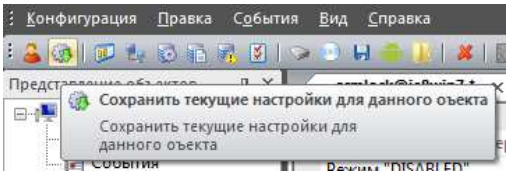

Рисунок 9.6 - Сохранение настроек в консоли администратора

После выполнения всех вышеуказанных действий учетной записи пользователя будет назначен аппаратный идентификатор.

9.3 Параметры входа в систему

Для АРМ можно указать параметры аутентификации и идентификации пользователя при входе. Для задания параметров доступа необходимо запустить консоль администрирования *«console.exe»*.

9.3.1 Параметры входа по карте

Откройте в панели параметров консоли группу «*Настройки*». (**Ошибка! Источник ссылки не найден.**)

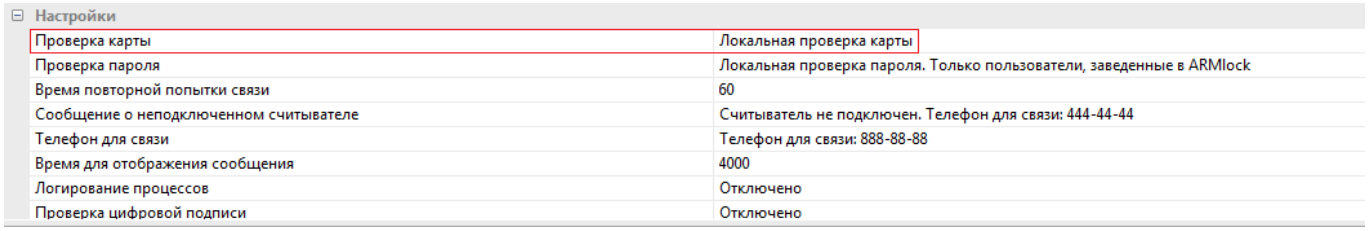

Рисунок 9.7 - Настройки параметров входа по карте

В выпадающем списке параметра «*Проверка карты*» можно выбрать одно из нескольких доступных значений. Возможны следующие значения параметра проверки карты:

Таблица 9.2 - Параметр проверки карты пользователя

Наименование параметра	Описание параметра
Любая карта	Вход пользователя возможен при предъявлении любого аппаратного идентификатора. При отсутствии подключенного считывателя вход в систему будет невозможен и будет выведено сообщение с просьбой подключить считыватель.
Проверка карты на сервере ARMlock	Приложенный аппаратный идентификатор сверяется данными об идентификаторе пользователя, хранимыми на сервере СЗИ НСД ARMlock. Если сервер не доступен, аппаратный идентификатор сверяется со значением, хранимым в локальном файле конфигурации СЗИ от НСД (т.е. последнем файле, успешно полученном от сервера)
Проверка карты в домене AD	Приложенный аппаратный идентификатор сверяется данными об идентификаторе пользователя в AD (поле EmployeeNumber в формате «ID1;ID2;…;IDn»). Если контроллер AD недоступен, аппаратный идентификатор сверяется со значением, хранимым в локальном файле конфигурации СЗИ от НСД
Локальная проверка каты	Приложенный аппаратный идентификатор сверяется данными об идентификаторе, хранимыми в локальном файле конфигурации СЗИ от НСД на АРМ
Проверка на сервере СЗИ НСД ARMlock. Отказ при недоступности сервера	Приложенный аппаратный идентификатор сверяется данными об идентификаторе пользователя, хранимыми на сервере СЗИ НСД ARMlock. Если сервер недоступен, пользователю будет запрещен вход и выведено сообщение о невозможности подключиться к серверу
Проверка карты в домене AD. Отказ при недоступности контроллера	Приложенный аппаратный идентификатор сверяется данными об идентификаторе пользователя в AD. Если контроллер домена недоступен, пользователю будет запрещен вход и выведено сообщение о невозможности подключиться к контроллеру домена
Не проверять карту	Осуществляется аутентификация пользователя только по имени и паролю, без использования идентификаторов карты. Аппаратный идентификатор и наличие считывателя при входе не проверяются.

Выбрав в выпадающем списке требуемый параметр проверки карты в панели инструментов консоли администратора нажать на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6)

9.3.2 Параметры входа по паролю

Откройте в панели параметров консоли «*Настройки*». (**Ошибка! Источник ссылки не найден.**)

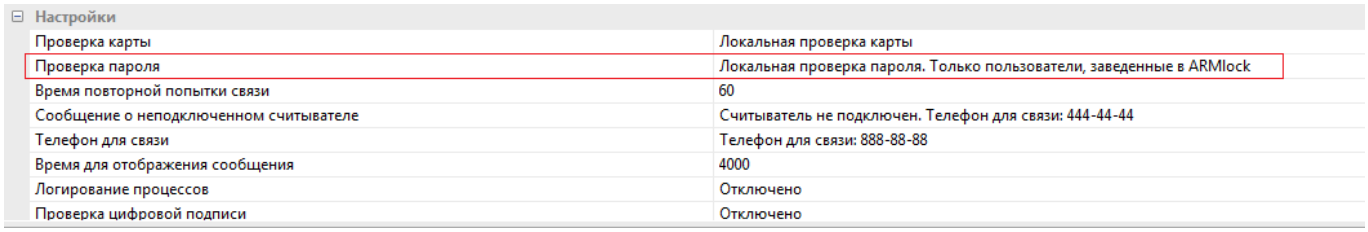

Рисунок 9.8 - Настройка параметров входа по карте

В выпадающем списке параметра «*Проверка пароля*» можно выбрать одно из нескольких доступных значений. Возможны следующие значения параметра проверки пароля:

Наименование параметра	Описание параметра
Локальная проверка пароля	Проверка пароля осуществляется сначала в файлах конфигурации СЗИ НСД ARMlock. Если данные об учетной записи пользователя/пароле в файлах конфигурации отсутсвуют, допускается проверка пароля в SAM-базе локальной ОС. При этом, в случае отсутствия файла конфигурации пользователя в СЗИ НСД ARMlock, но наличия его в системе Windows, ему присваиваются настройки безопасности АРМ.
Локальная проверка пароля. Только пользователи, заведенные в ARMlock	Пароль и логин пользователя сверяются с данными, хранимым в файлах конфигурации СЗИ НСД ARMlock. Если пользователь зарегистрирован в ОС, но не зарегистрирован в СЗИ НСД ARMlock, вход будет запрещен.
Проверка пароля на сервере ARMlock	Пароль и логин пользователя сверяются с данными, хранимым на сервере ARMlock. Если сервер недоступен (или адрес сервера не указан в параметрах пользователя) Пароль сверяется со значениями в файлах конфигурации СЗИ НСД ARMlock. Если пользователь заведён в ОС, но не зарегистрирован в СЗИ НСД ARMlock, вход будет запрещен.
Проверка пароля на сервере ARMlock. Отказ при недоступности сервера	Пароль и логин пользователя сверяются с данными, хранимым на сервере ARMlock. Если сервер недоступен (или адрес сервера не указан в параметрах пользователя) пользователю будет отказано во входе в систему
Проверка пароля стандартными средствами Windows (либо домена AD).	Проверка пароля осуществляется стандартными средствами локальной ОС или на контроллере домена (AD), в зависимости от настроек ОС

Выбрав в выпадающем списке требуемый параметр проверки пароля в панели инструментов консоли администратора нажать на иконку «*Сохранить текущие настройки для данного объекта*». (Рисунок 9.6)

9.3.3 Настройка уведомлений

Функционал СЗИ НСД ARMlock позволяет настроить уведомления пользователя в случае возникновения определенных ситуаций. В частности отредактировать текст сообщений, появляющихся при определенных событиях.

Для редактирования необходимо запустить консоль администрирования и открыть группу «*Настройки*». (Рисунок 9.9).

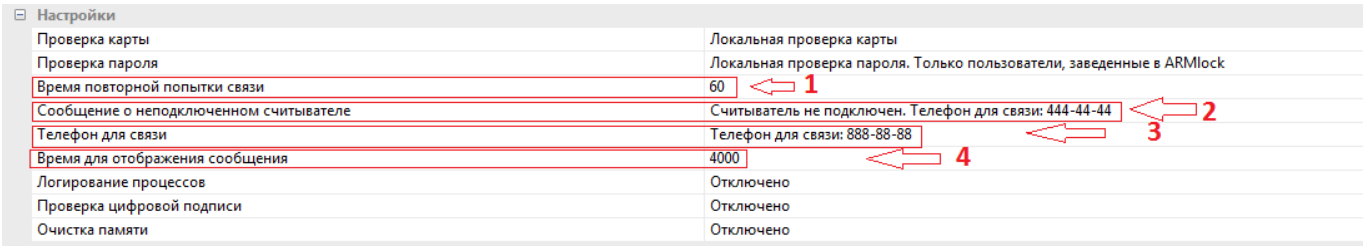

Рисунок 9.9 - Параметры отображения уведомлений

Можно задать следующие параметры содержания и отображения сообщений (Нумерация приведена в соответствии с нумерацией на Рисунок 9.9):

1. «*Время повторной попытки связи*» - этим параметром задается в секундах период попыток подключения клиентской части СЗИ НСД ARMlock к серверу после предыдущей неудачной попытки.
2. «*Сообщение о неподключенном считывателе*» - текст сообщения в случае отсутствия подключенного к АРМ считывателя;
3. *«Телефон для связи» - сообщение, которое отобразиться пользователю в случае отсутствия подключенного считывателя или иной проблемы, которая может потребовать технической поддержки;*
4. *«Время для отображения сообщения» - время в миллисекундах, в течение которого пользователю будут отображаться информационные сообщения.*

После ввода настройки параметров требуется сохранить сделанные изменения. Для этого в панели инструментов консоли администратора нажмите на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6).

10 Разграничение доступа к объектам

10.1 Политика доступа по умолчанию

Для каждого из субъектов доступа (учетной записи пользователя или АРМ) должна быть определена политика доступа к объектам безопасности. В СЗИ НСД ARMlock под этой политикой понимаются правила, применяемые по умолчанию к различным видам объектов безопасности (usbflash-дисков, CD/DVD-дисков, floppy, файлов на диске и тд).

После первой установки СЗИ НСД ARMlock для носителей, файлов и папок, печати, всем субъектам доступа по умолчанию разрешен полный доступ, При такой политике доступ к конкретному объекту может быть заблокирован только в случае, если будет создано специальное запрещающее правило, указывающее на конкретный объект, подлежащий запрету.

Внимание! Если ранее на АРМ уже использовалось СЗИ НСД ARMlock, то в случае если не были удалены старые параметры, после установки они будут загружены для пользователей и АРМ

Если субъекту доступа (пользователю или всем пользователям АРМ) необходимо разрешить доступ только к ограниченному набору объектов доступа, необходимо в значении группы «*Политика по умолчанию для устройств и для доступа к файлам и папкам*» выбрать в выпадающем списке параметра «*тип доступа*» значение блокировать. Далее требуется сохранить настройки, для чего в панели инструментов консоли администратора нажать на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6)

Не рекомендуется использовать запрещающую политику для доступа к файлам и папкам, т.к. при неправильной настройке это может привести к невозможности входа в систему или невозможности нормальной работы в системе.

10.2 Разграничение доступа к съемным носителям

10.2.1 Разграничение доступа к USB носителям

Для создания правил доступа необходимо запустить консоль администрирования *«console.exe»*.

Дважды щелкните на объекте (учетной записи или АРМ) для которого вы хотите добавить правило для USB носителя, чтобы открылась вкладка редактируемого объекта (пользователя или АРМ) в панели параметров.

Внимание! Настроенные политики по умолчанию и правила для USB-накопителей не распространяются на такие специфичные USB-устройства как смартфоны, плееры, мультимедиа-проигрыватели. Для регламентации доступа к специфичным USB-устройствам см. Раздел 10.4 «Разграничение доступа к специфичным USB-устройствам (мультимедиа-устройствам)

Далее для разграничения доступа к USB-носителям нажмите на иконку «*Добавить USB носитель»*. (Рисунок 10.1)

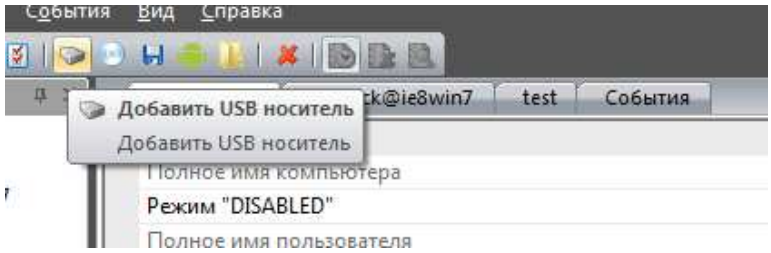

Рисунок 10.1 - Добавление USB носителя

Появится окно с уведомлением о создании правила. Нажмите кнопку «*ОК*». (Рисунок 10.2)

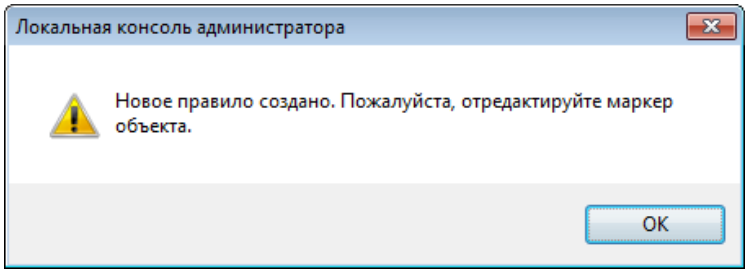

Рисунок 10.2 - Окно с сообщением о создании нового правила

Далее необходимо отредактировать в дереве панели параметров объекта (*Компьютер \ добавление разрешенных устройств ...\USB носители \ Носитель X*, где X - порядковый номер добавляемого носителя) шаблон созданного правила. (Рисунок 10.3)

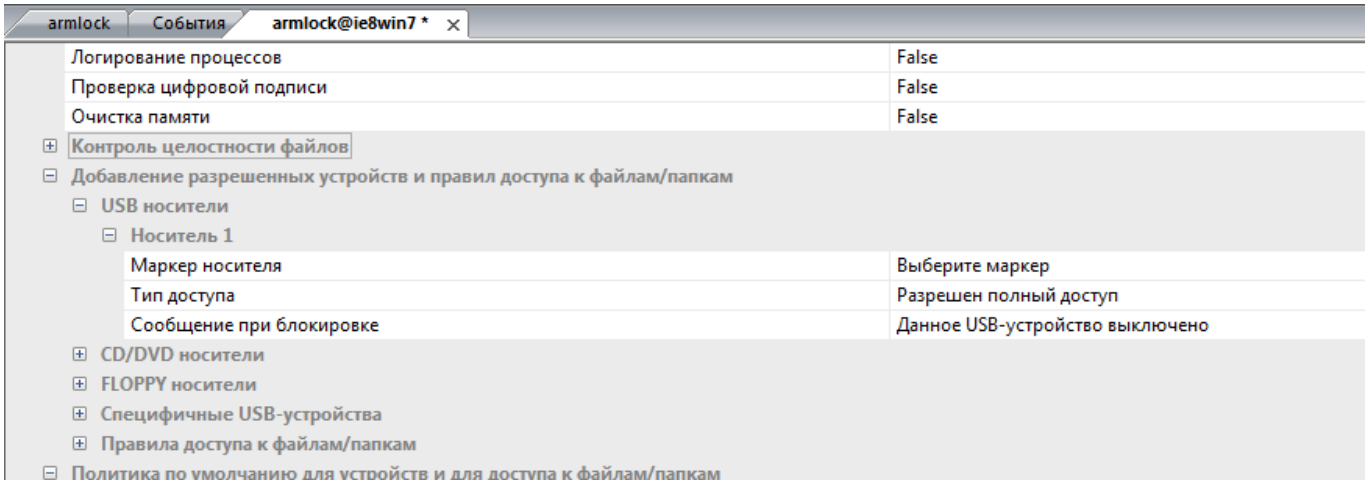

Рисунок 10.3 - Правило для USB носителя

Всего требуется указать три параметра:

1. *Маркер носителя* - по двойному нажатию ЛКМ мыши откроется окно добавления носителя, в котором можно выбрать носитель, для которого создается правило. (Рисунок 100.4)

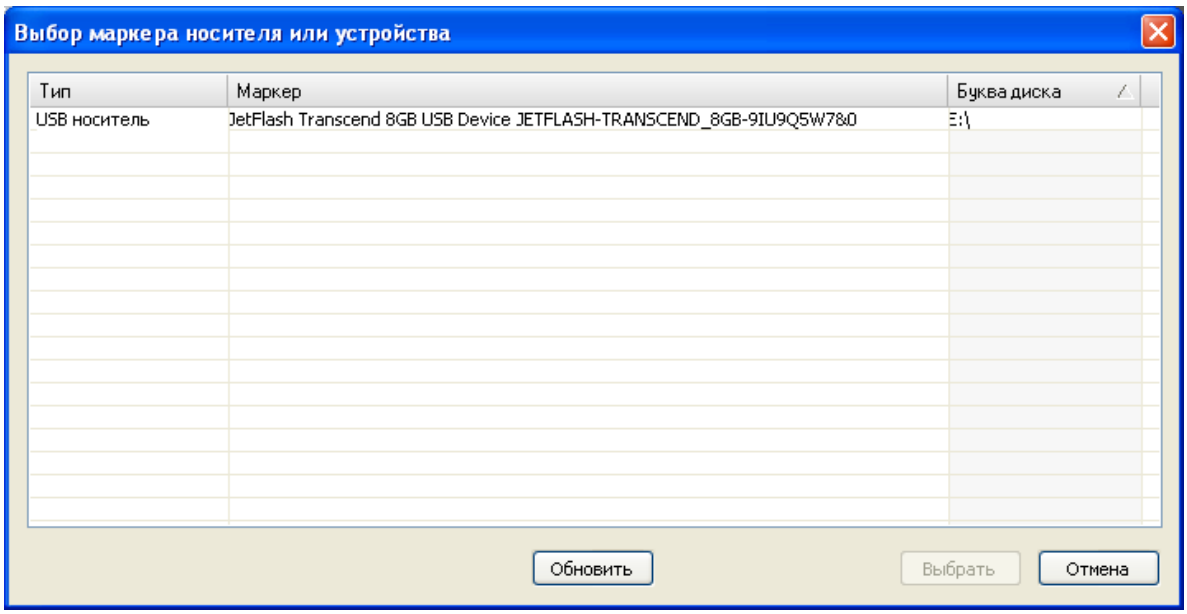

Рисунок 100.4 - Выбор носителя для создания правила

Для добавления в систему нового носителя подключите его к АРМ, выберите в списке и нажмите кнопку «*Выбрать*». (Если носитель не отображается - проверьте его подключение к USB-порту и нажмите кнопку «*Обновить*».)

2. *Тип доступа* - права доступа к добавленному носителю, в выпадающем списке можно выбрать один из трех режимов:
   – «*Разрешен полный доступ*» - полный доступ к носителю (чтение и запись);
   – «*Блокировать*» - доступ к носителю полностью запрещен;
   – «*Только чтение*» - разрешается только копирование с носителя, запись запрещена.
3. *Сообщение при блокировке* - сообщение, выводимое пользователю в случае блокировки носителя.

Далее необходимо сохранить сделанные изменения. Для этого в панели инструментов консоли администратора нажать на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6)

10.2.2 Разграничение доступа к floppy-дискам

Для создания правил доступа необходимо запустить консоль администрирования *«console.exe»*.

Дважды щелкните на объекте (учетной записи или АРМ) для которого вы хотите добавить правило для floppy диска, чтобы открылась вкладка редактируемого объекта (пользователя или АРМ) в панели параметров консоли.

Далее для разграничения доступа к floppy дискам нажмите на иконку «*Добавить floppy-носитель*». (Рисунок 10.5)

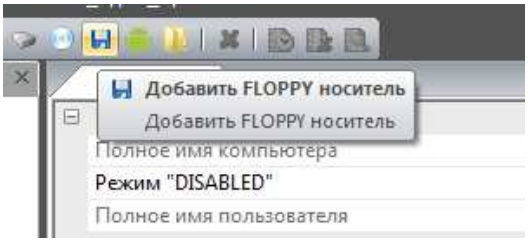

Рисунок 10.5 - Добавление floppy носителя

Появится окно с уведомлением о создании правила. Нажмите кнопку «*ОК*». (Рисунок 10.6)

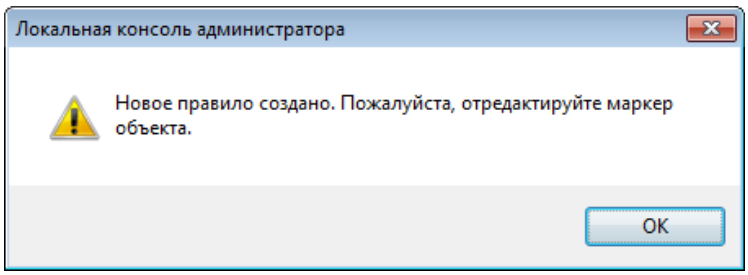

Рисунок 10.6 - Окно с сообщением о создании нового правила

Автоматически будет создан и отображен в дереве панели параметров объекта (*Компьютер \ добавление разрешенных устройств ...\floppy носители \Носитель X*, где X - порядковый номер добавляемого носителя) шаблон правила. (Рисунок 10.7)

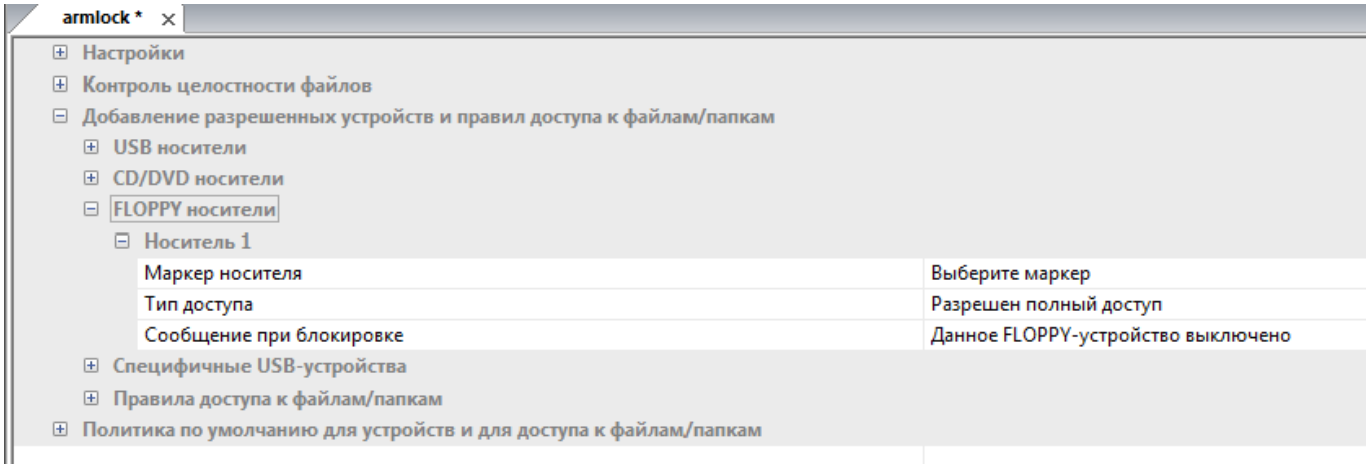

Рисунок 10.7 - Правило для floppy носителя

Далее требуется отредактировать созданный шаблон правила. Всего требуется указать 3 параметра:

1. *Маркер носителя* - по двойному нажатию ЛКМ мыши на параметре откроется окно добавления носителя, в котором можно выбрать носитель, для которого создается правило. (Рисунок 10.8)

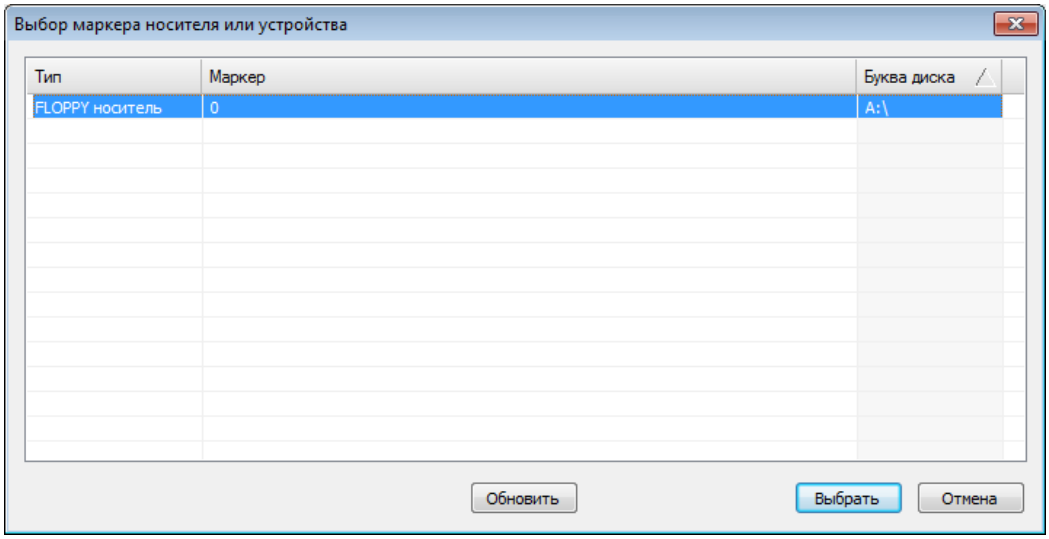

Рисунок 10.8 - Выбор floppy для создания правила

Для добавления в систему нового носителя вставьте его в дисковод АРМ, выберите в списке и нажмите кнопку «Выбрать». (Если носитель не отображается - проверьте его наличие в считывателе и нажмите кнопку «Обновить»)

2. *Тип доступа* - права доступа к добавленному носителю, в выпадающем списке можно выбрать один из трех режимов:
   – «*Разрешен полный доступ*» - полный доступ к носителю (чтение и запись);
   – «*Блокировать*» - доступ к носителю полностью запрещен;
   – «*Только чтение*» - разрешается только копирование с носителя, запись запрещена.
3. *Сообщение при блокировке* - сообщение, выводимое пользователю в случае блокировки носителя.

Далее необходимо сохранить сделанные изменения. Для этого в панели инструментов консоли администратора нажать на иконку «*Сохранить текущие настройки для данного объекта*». (Рисунок 9.6)

Внимание! Маркер носителя для FLOPPY и CD/DVD-дисков – это маркер файловой системы (в отличие от USB-дисков). Таким образом, после форматирования FLOPPY или перезаписи CD/DVD-диска они считаются новым объектом безопасности, т.к. содержат совершенно новую файловую систему и файлы на ней. У таких floppy и cd/dvd-дисков в момент форматирования/полной перезаписи генерируется новый маркер и доступ к таким объектам необходимо разграничивать заново, создавая новые правила в консоли СЗИ НСД ARMlock

10.2.3 Разграничение доступа к компакт-дискам (CD)

Для создания правил доступа необходимо запустить консоль администрирования *«console.exe»*.

Дважды щелкните на объекте (учетной записи или АРМ) для которого вы хотите добавить правило для CD-диска, чтобы открылась вкладка редактируемого объекта (пользователя или АРМ) в панели параметров консоли.

Далее для разграничения доступа к CD дискам нажмите на иконку «*Добавить CD-носитель*». (Рисунок 10.9)

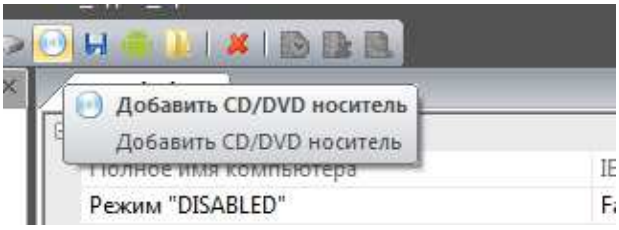

Рисунок 10.9 - Добавление CD носителя

Появится окно с уведомлением о создании правила. Нажмите кнопку «ОК». (Рисунок 10.10)

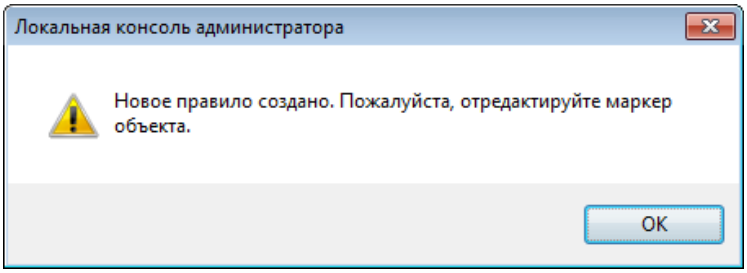

Рисунок 10.10 - Окно с сообщением о создании нового правила

Автоматически будет создан и отображен в дереве панели параметров объекта (*Компьютер \ добавление разрешенных устройств ...\CD носители \Носитель X*, где X - порядковый номер добавляемого носителя) шаблон правила. (Рисунок 10.11)

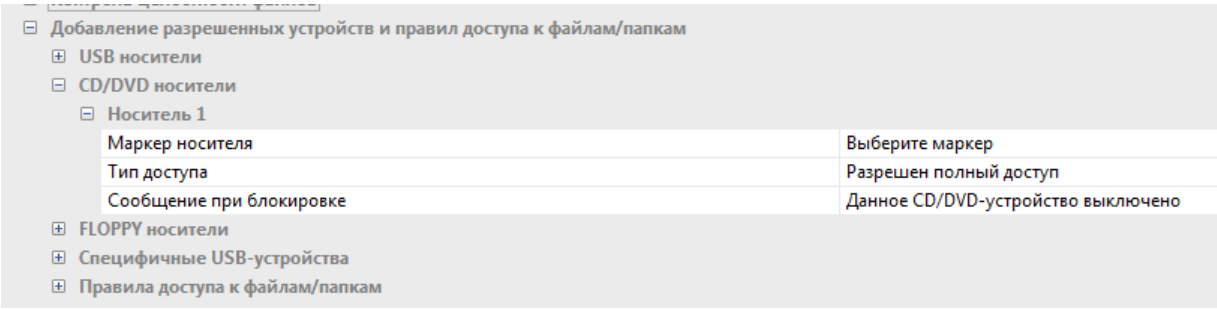

Рисунок 10.11 - Правило для CD-носителя

Далее требуется отредактировать созданный шаблон правила. Всего требуется указать три параметра:

1. *Маркер носителя* - по двойному нажатию ЛКМ мыши на параметре откроется окно добавления носителя, в котором можно выбрать носитель, для которого создается правило. (Рисунок 10.12)

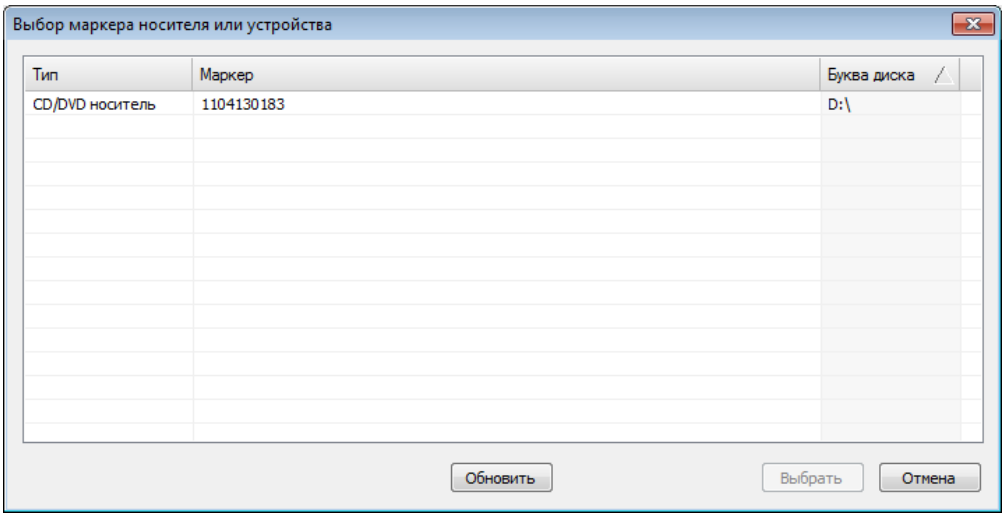

Рисунок 10.12 - Выбор CD носителя для создания правила

Для добавления в систему нового носителя вставьте его в дисковод АРМ, выберите в списке и нажмите кнопку «Выбрать». (Если носитель не отображается - проверьте его наличие в считывателе и нажмите кнопку «Обновить»)

2. *Тип доступа* - в выпадающем списке можно выбрать один из трех режимов:
   - «*Разрешен полный доступ*» - полный доступ к носителю (чтение и запись);
   - «*Блокировать*» - доступ к носителю полностью запрещен;
   - «*Только чтение*» - разрешается только копирование с носителя, запись запрещена.
3. *Сообщение при блокировке* - сообщение, выводимое пользователю в случае блокировки носителя.

Далее необходимо сохранить сделанные изменения. Для этого в панели инструментов консоли администратора нажать на иконку «*Сохранить текущие настройки для данного объекта*». (Рисунок 9.6)

Внимание! Маркер носителя для FLOPPY и CD/DVD-дисков – это маркер файловой системы (в отличие от USB-дисков). Таким образом, после форматирования FLOPPY или перезаписи CD/DVD-диска они считаются новым объектом безопасности, т.к. содержат совершенно новую файловую систему и файлы на ней. У таких floppy и cd/dvd-дисков в момент форматирования/полной перезаписи генерируется новый маркер и доступ к таким объектам необходимо разграничивать заново, создавая новые правила в консоли СЗИ НСД ARMlock

10.3 Разграничение доступа к системе печати

В текущей версии СЗИ НСД ARMlock создание отдельных правил доступа к системе печати не имеет смысла. Система печати блокируется либо полностью либо полностью доступна исходя из настроек политики. Добавление данных правил предусмотрено с целью реализации возможности добавления разрешающих правил печати на отдельных принтерах в будущих версиях СЗИ НСД ARMlock.

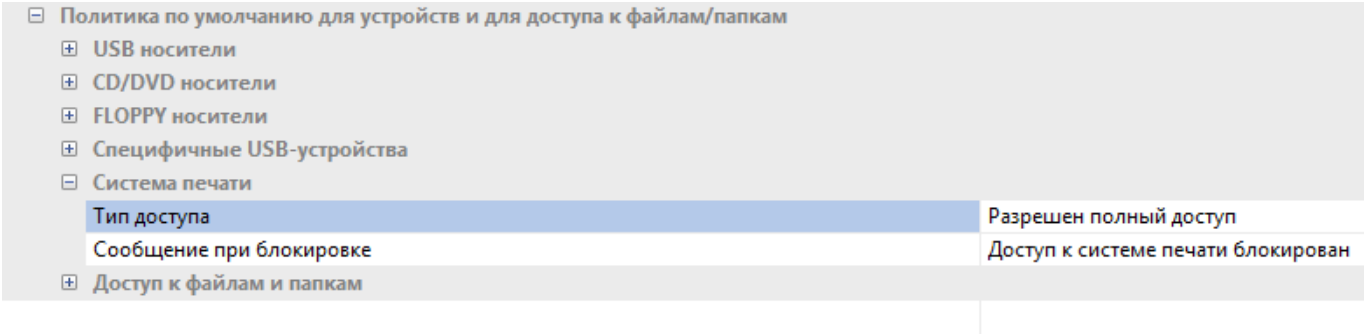

Рисунок 10.13 - Добавление правил доступа к системе печати

10.4 Разграничение доступа к специфичным USB-устройствам (мультимедиа-устройствам)

Администратору безопасности при настройке СЗИ НСД ARMlock следует учесть, что настроенные политики по умолчанию и правила для USB-накопителей не распространяются на такие специфичные USB-устройства как смартфоны, плееры, мультимедиа-проигрыватели. Эти устройства позволяют пользователю выполнять копирование информации на их встроенную память, что создает потенциальный канал для утечки информации. Функционал СЗИ НСД ARMlock позволяет управлять доступом к таким устройствам.

Прежде всего, рекомендуется запретить доступ к специфичным USB-устройств с помощью настроек политики.

При необходимости создания отдельных разрешающих правил (например, для отдельного телефона на базе ОС Android) это можно сделать с помощью меню локальной консоли.

Для создания правила доступа к специфичному USB-устройству необходимо запустить консоль администрирования *«console.exe»*.

Дважды щелкните на объекте (учетной записи или АРМ) для которого вы хотите добавить правило для мультимедиа-носителя, чтобы в панели параметров консоли открылась вкладка с параметрами редактируемого объекта (пользователя или АРМ).

Далее для разграничения доступа к CD дискам нажмите на иконку «*Добавить специфичное USB-устройство*». (Рисунок 10.14)

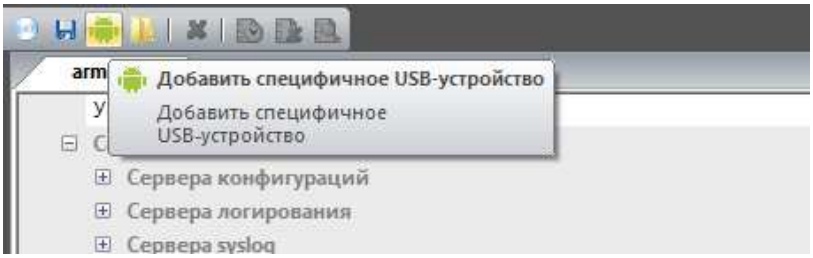

Рисунок 10.14 - Добавление мультимедиа-носителя

Автоматически будет создан и отображен в дереве панели параметров объекта (*Компьютер \ добавление разрешенных устройств ...\CD носители \Устройство X*, где X - порядковый номер добавляемого устройства) шаблон правила. (Рисунок 10.15)

Рисунок 10.15 - Правило для специфичного USB-устройства

Далее требуется отредактировать созданный шаблон правила. Всего требуется указать три параметра:

1. *«Маркер носителя»* - по двойному нажатию ЛКМ мыши на параметре откроется окно добавления носителя, в котором можно выбрать носитель, для которого задается правило доступа. (Рисунок 10.16)

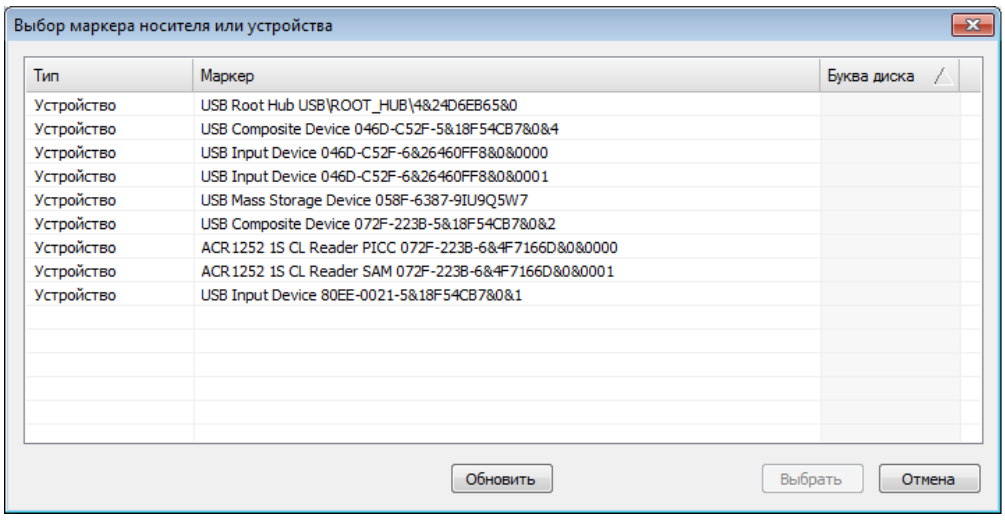

Рисунок 10.16 - Выбор мультимедиа-носителя для создания правила

Выберите в списке необходимое устройство и нажмите кнопку «*Выбрать*». (Если носитель не отображается - нажмите кнопку «*Обновить*»)

2. *«Состояние»* - в выпадающем списке можно выбрать один из двух параметров:
   - «*Выключено*» - доступ к носителю запрещен;
   - «*Включено*» - доступ к носителю разрешен.
3. *«Сообщение при блокировке»* - сообщение, выводимое пользователю в случае блокировки носителя.

Далее необходимо сохранить сделанные изменения. Для этого в панели инструментов консоли администратора нажать на иконку «Сохранить текущие настройки для данного объекта». (Рисунок 9.6)

10.5 Разграничение доступа к файлам и папкам

Для создания правил доступа к файлам и папкам необходимо запустить консоль администрирования *«console.exe»*.

Дважды щелкните на объекте (учетной записи или АРМ) для которого вы хотите добавить правило для мультимедиа-носителя, чтобы в панели параметров консоли открылась вкладка с параметрами редактируемого объекта (пользователя или АРМ).

Далее для разграничения доступа к файлам и папкам нажмите на иконку «*Добавить специфичное USB-устройство*». (Рисунок 10.17 - Добавление правила доступа к файлу/папкеРисунок 10.14)

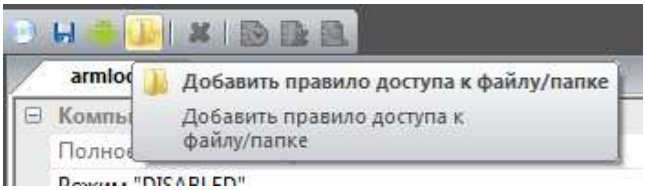

Рисунок 10.17 - Добавление правила доступа к файлу/папке

Автоматически будет создан шаблон правила, о чем будет выдано сообщение. (Рисунок 10.18)

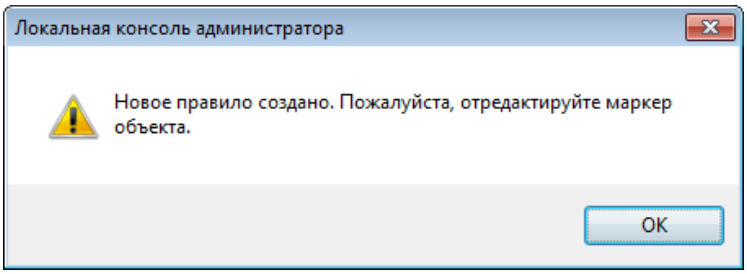

Рисунок 10.18 - Сообщение о добавлении правила

Далее требуется в панели параметров отредактировать созданный шаблон правила. Всего требуется указать пять параметров. (**Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.**)

Рисунок 10.199

Таблица 1.1 содержит описание параметров, указываемых для правила доступа к файлам и папкам.

Таблица 10.1 - Параметры правил доступа к файлам/папкам

Наименование параметра	Описание	Возможное значение
Поисковая строчка	расположение файла/папки, к которому настраивается доступ	*Путь к объекту контроля-(*файлу/папке. Например *C:\Folder_1|... и т.п.)*
Чтение	право редактируемого пользователя на чтение файла/папки	*Разрешить/Блокировать*
Запись	право редактируемого пользователя на запись файла/папки	*Разрешить/Блокировать*
Исполнение	право редактируемого пользователя на запуск	*Разрешить/Блокировать*
Сообщение при блокировке	сообщение, выводимое пользователю при блокировании доступа к файлу/папке	Текст сообщения, выводимого при блокировании доступа

Примечание. При создании правила СЗИ НСД ARMlock можно воспользоваться инструментом «символьной маски». Т.е. вместо имени файла указать символ «*». Такое правило будет распространяться на файлы с любым именем/расширением, расположенные в указанной папке.

Например: правило с указанием пути C:\Folder_1*.txt распространяется на все файлы с расширением «txt» в папке Folder_1, но не в её подпапках.

Правило с указанием пути C:\Folder_1\armlock.* распространяется на все файлы с именем «armlock» в папке «Folder_1», но не в её подпапках.

Правило вида *«C:\Folder_1*»* будет распространяться на все файлы в папке «Folder_1».

Также функционал СЗИ НСД ARMlock позволяет использовать маску вида «**». При использовании этой маски под действие правила попадают все вложенные подпапки и файлы в них.

Например: правило с параметром пути *«C:\Folder_1**»* будет распространяться на все содержимое папки *Folder_1*, включая подпапки.

Внимание! СЗИ НСД ARMlock использует контроль доступа к объектам безопасности файловой системы не с помощью системных механизмов ОС Windows, таких как ACL, а по маске полного пути, что влечет за собой ряд особенностей. Так, при добавлении файла/папки на контроль с помощью правила с детальным указанием полного пути, у злоумышленника остаётся возможность получить несанкционированный доступ к файлу с помощью изменения имен папок уровнем выше, что приведет к изменению полного пути файла таким образом, что созданные правила безопасности перестанут действовать. Исключить такую возможность злоумышленнику можно с помощью блокирования изменений имен папок в полном пути к файлу с помощью отдельных правил, либо использованием блокировки доступа к объектам без указания полного пути: например шаблон «**confedential.data.xls» распространится на все соответствующие файлы в любых подпапках. Ещё одним способом защиты от подобных действий злоумышленника является использование специальных системных переменных %WINDIR%, %USERPROFILE%, %PATH% и других, а также специальной переменной %ARMLOCK%, определяющей путь установки СЗИ НСД ARMlock. Вместо указания буквы диска рекомендуется использовать переменную вида %ABCD-EF01%, где ABCD-EF01 – номер тома (volume number), который можно посмотреть с помощью командной строки, набрав команду «dir».

Не рекомендуется использовать запрещающую политику для доступа к файлам и папкам, т.к. при неправильной настройке это может привести к невозможности входа в систему или невозможности нормальной работы в системе.

10.6 Разграничение доступа к консоли администрирования

Функционал СЗИ НСД ARMlock позволяет разграничить доступ к средствам администрирования самого СЗИ от НСД.

Для того чтобы разрешить учетной записи пользователя запуск средства администрирования - консоли, необходимо открыть вкладку пользователя в панели параметров

(двойное нажатие ЛКМ на имени учетной записи в дереве представления объектов) и в группе «Пользователь» выставить параметр «*Локальный администратор*» в значение «*Является локальным администратором*». (Рисунок 10.20)

Рисунок 10.20 - Права доступа к консоли администрирования

Для запрета доступа учетной записи к консоли администрирования следует выбрать параметр «*Не является локальным администратором*».

Удаление СЗИ НСД ARMlock с АРМ разрешено только локальным администраторам.

Для того, чтобы изменения, производимые в локальной консоли могли быть применены при входе в локальную консоль администратора может дополнительно запрашиваться пароль защиты локальных файлов, который был задан при установке СЗИ НСД ARMlock на АРМ.

10.7 Автовход и авторазблокировка

СЗИ НСД ARMlock предусматривает возможность включения авторазблокировки АРМ (в случае выполненного ранее пользователем входа) или автоматического входа в систему при прикладывании карты пользователя (в случае использования двухфакторной аутентификации).

Для включения одной из этих функций воспользуйтесь локальной консолью администратора (Рисунок 10.20).

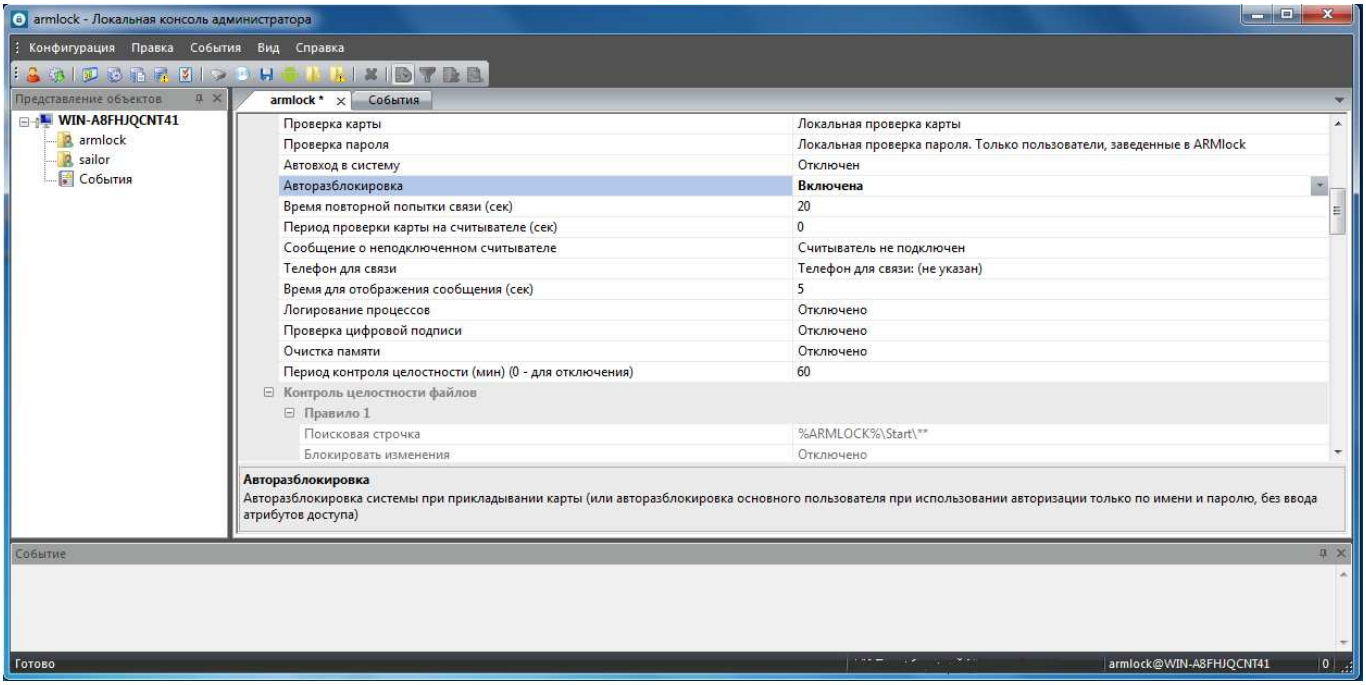

Рисунок 100.21 - Настройка авторазблокировки

10.8 Режим «DISABLED»

В случае, если СЗИ НСД ARMlock работает в режиме двухфакторной аутентификации, у сетевого администратора могут возникнуть сложности в процессе удалённого администрирования АРМ пользователя. Например, при попытке входа в систему по протоколу RDP.

Для подобных случаев в СЗИ НСД ARMlock специально создан режим «DISABLED», предназначенный для временного отключения считывателя карт и перевода СЗИ в режим аутентификации по имени и паролю.

При этом настройки пользователя и/или АРМ не теряются. Для восстановления нормального функционирования администратор должен просто выключить режим «DISABLED», вернув тем самым СЗИ НСД ARMlock в нормальный режим функционирования.

Перевод в режим «DISABLED» и обратно может быть выполнен как на сервере СЗИ НСД ARMlock, так и с помощью локальной консоли администратора (Рисунок 10.21)

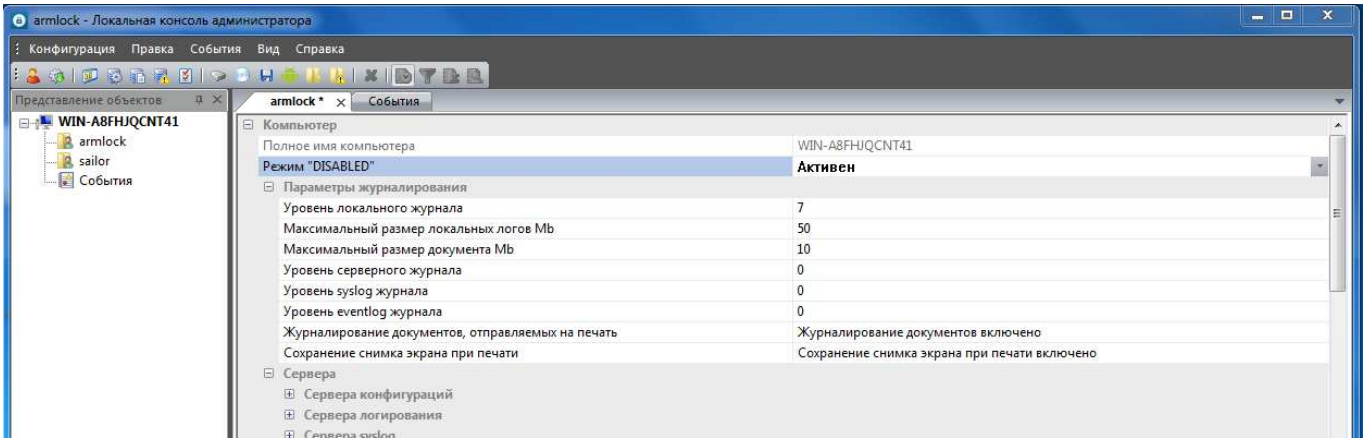

Рисунок 100.22 - Включение режима «DISABLED»

11 Регистрация и учет

11.1 Настройка параметров журналирования

В зависимости от условий функционирования СЗИ НСД ARMlock можно указать параметры журналирования.

Для этого необходимо запустить консоль администрирования. Далее нажатием ЛКМ открыть в панели редактирования параметров АРМ или пользователя, для которого выполняется настройка журналирования. Затем в открывшейся вкладке с параметрами раскрыть группу «Параметры журналирования». (Рисунок 111.1).

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 СЗИ НСД ARMlock «0», то в локальный журнал событий не будет попадать ни одного события безопасности.

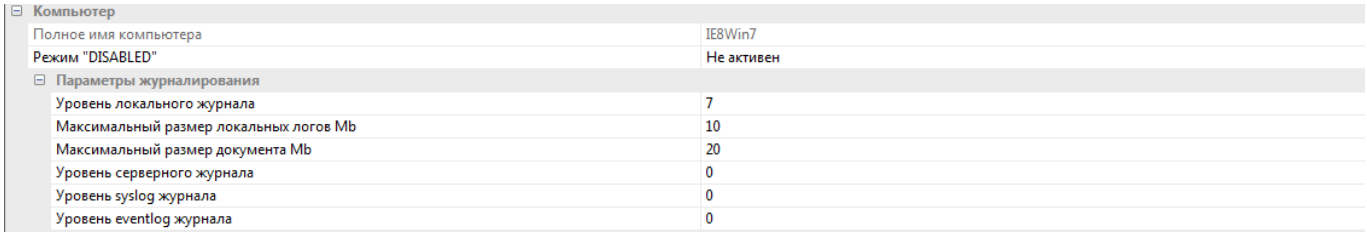

Рисунок 111.1 - Параметры журналирования

Описание назначения параметров журналирования приведено в Таблица 11.1

Таблица 11.1 - Описание параметров журналирования

Наименование параметра	Описание
Уровень локального журнала	События отправляются в локальный журнал, если его уровень меньше указанного в параметре.
Максимальный размер локальных логов	Ограничение максимального размера файла с журналом в мегабайтах.
Максимальный размер документа	Ограничение максимального размера теневой копии распечатываемых пользователем документов в мегабайтах.
Уровень серверного журнала	Если уровень важности события меньше данного значения событие отправляется для записи на сервер конфигураций.
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 на сервер логирования.

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

11.2 Работа с журналом событий

11.2.1 Просмотр журнала

Для просмотра записей о событиях в журнале необходимо в панели представления объектов открыть двойным нажатием ЛКМ мыши элемент «*События*» для АРМ, которого необходимо просмотреть журнал. (Рисунок 11.2)

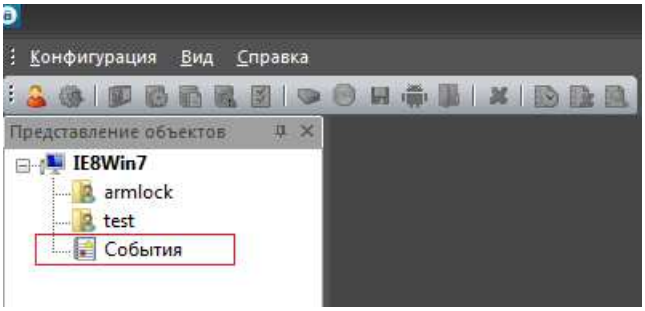

Рисунок 11.2 -Открытие журнала событий

В панели редактирования параметров откроется вкладка *«События»* с отображением записей журнала событий. (Рисунок 111.3)

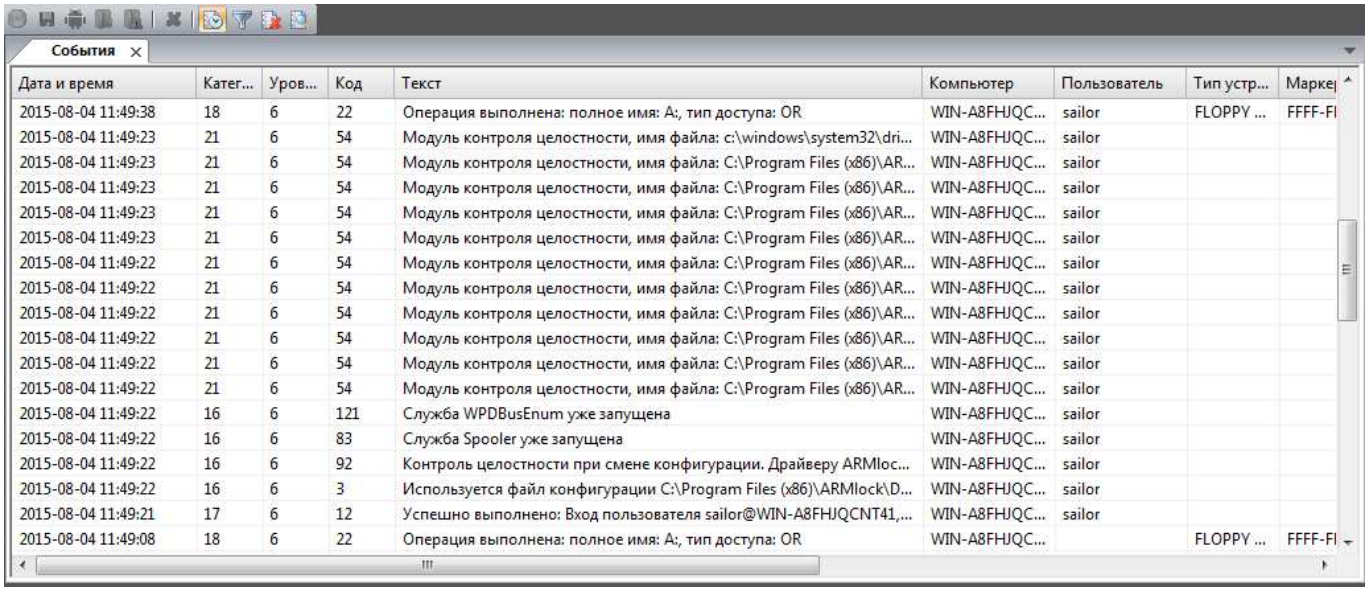

Рисунок 111.3 - Вкладка с отображением записей журнала событий

Журнал событий представляет собой таблицу из нескольких столбцов с данными о событиях.

Примечание. Одиночным шелком левой кнопки мыши по заголовку столбца журнала во вкладке панели редактирования параметров можно отсортировать записи по указанному заголовку в порядке убывания/возрастания.

Для более удобного отображения информации о событии можно его выделить нажатием ЛКМ и вывести данные о событии в панели отображения данных о событии консоли администрирования. (Рисунок 111.4)

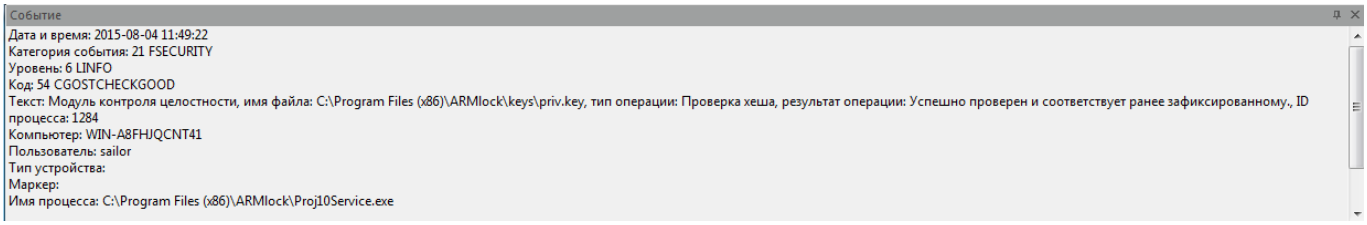

Рисунок 111.4 - Данные о выделенном событии в панели отображения событий

Состав и описание назначения столбцов журнала событий приведены в Таблица 11.2 - Описание столбцов журнала событий.

Таблица 11.2 - Описание столбцов журнала событий

Наименование столбца	Описание
Дата и время	Дата и время записи о событии в журнале
Категория	Тип события
Уровень	Уровень важности сообщения в соответствии с протоколом syslog.
Код	Код (уникальный номер) события
Текст	Текстовое описание события
Компьютер	Имя АРМ на котором произошло событие
Пользователь	Имя учетной записи пользователя под сеансом которого произошло событие
Тип устройства	Устройство с которым произошло событие
Маркер	Признак устройства, который его однозначно определяет
Имя процесса	Имя процесса связанного с событием
Документ	Копия распечатанного пользователем документа
Снимок	Снимок экрана, сделанный при событии

11.2.2 Настройка обновления журнала событий

Инструмент «*Автоматически загружать и отображать в таблице локальные события*» позволяет включить/выключить добавление новых событий, произошедших уже в ходе открытия и просмотра журнала событий. (Рисунок 11.55)

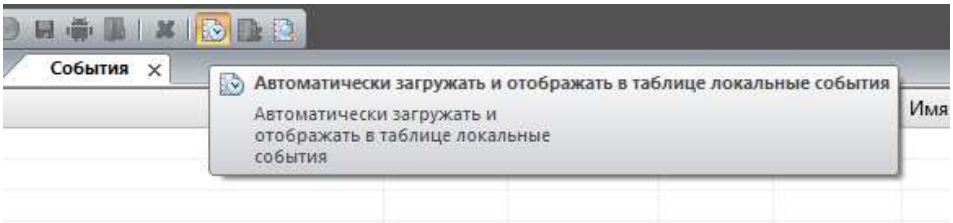

Рисунок 11.5 - Автодобавление новых записей в отображаемый журнал

Для включения автодобавления новых событий необходимо активировать щелчком ЛКМ мыши иконку «*Автоматически загружать и отображать в таблице локальные события*» в панели инструментов консоли администрирования. После этого новые записи о событиях будут добавляться во вкладку «*События*» по мере их появления.

11.2.3 Поиск записей журнала

Инструменты просмотра журнала событий в консоли администрирования СЗИ НСД ARMlock позволяют осуществлять поиск событий по заданным параметрам в событиях.

Для того чтобы воспользоваться поиском нажмите на иконку «*Поиск события по параметрам и тексту*» в панели инструментов консоли администрирования СЗИ НСД ARMlock. Также для этого можно воспользоваться сочетанием клавиш «Ctrl+F». (Рисунок 11.6)

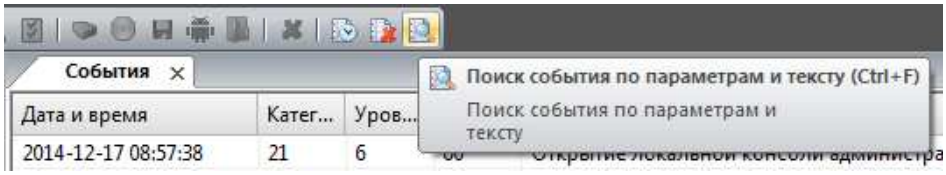

Рисунок 11.6 - Иконка «Поиск события...» в панели инструментов консоли

Появится окно с полем ввода искомого сочетания символов и флаговыми кнопками. (Рисунок 11.7)

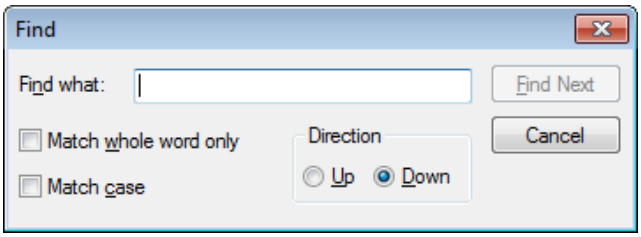

Рисунок 11.7 - Окно поиска

В поле ввода «*Find what*» («*Найти*») нужно ввести искомое сочетание символов. Флаговыми кнопками «*Match whole word only*» («Искать только целое слово») и «*Match case*» («*Учитывать регистр*») можно задать параметры поиска. Переключатель «*Direction*» («*Направление*») отвечает за то будет ли поиск осуществлять выше/ниже («Up»/«Down») текущего активного/выделенного события на вкладке журнала в консоли.

После ввода искомого сочетания и указания параметров поиска необходимо нажать на кнопку «*Find Next*» («*Найти далее*»). Будет осуществлен поиск события по строке указанной в поле *Find what*» («*Найти*»). Если событие с таким сочетанием символов будет найдено, оно автоматически выделится и станет активным, данные о нем будут отображены в панели «*Событие*». Для поиска других событий содержащих искомое сочетание символов необходимо нажать кнопку «*Find Next*» («*Найти далее*»).

11.3 Очистка журнала событий

Иногда для удобства просмотра журналов событий или в случае их переполнения возникает необходимость удалить информацию о старых, не актуальных событиях.

Для этого необходимо запустить консоль администрирования СЗИ НСД ARMlock путем двойного нажатия ЛКМ «*console.exe*».

Для того чтобы очистить журнал событий необходимо выделить АРМ в панели представления объектов консоли администрирования и щелкнуть ЛКМ на иконке «*Удалить все локальные события*» в панели инструментов консоли администрирования. (Рисунок 11.8)

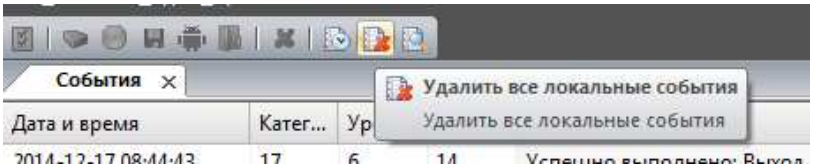

Рисунок 11.8 - Очистка журнала событий

Появится окно с просьбой подтверждения очистки журналов. (Рисунок 11.9). Для выполнения очистки нажмите кнопку «*OK*».

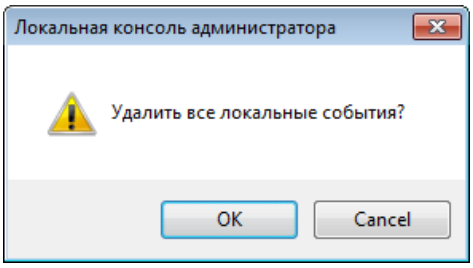

Рисунок 11.9 - Подтверждение очистки журнала

Примечание. После очистки журнала появится запись о событии «Очистка журнала» с указанием имени пользователя, под сеансом которого была выполнена очистка журнала.

11.4 Журналирование документов и снимков экрана при печати

СЗИ НСД ARMlock предусматривает возможность сохранения на сервере копий документов, отправляемых пользователями на печать, а также сриншота экрана в момент отправки документа на печать. Включить данную функцию возможно либо на сервере СЗИ НСД ARMlock, либо через локальную консоль администратора.

Скриншоты и документы сохраняются в рабочей директории СЗИ НСД ARMlock. Для удобного просмотра данных файлов необходимо воспользоваться функционалом сервера СЗИ НСД ARMlock.

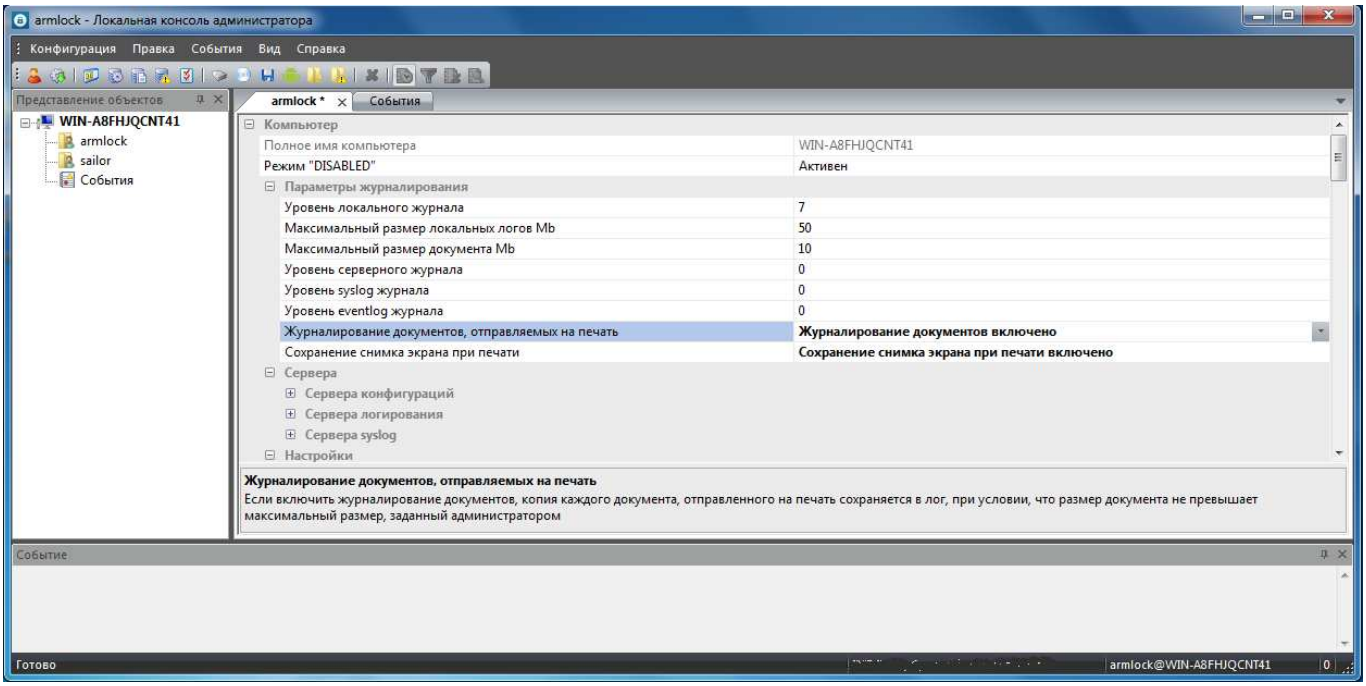

Рисунок 11.10 - Включение журналирования документов и сохранения снимков экрана

12 Взаимодействие с серверами СЗИ НСД ARMlock

12.1 Описание серверов взаимодействия

СЗИ НСД ARMlock для удобства хранения и работы с конфигурациями/журналами событий позволяет настроить взаимодействие с тремя серверами:

- Syslog-сервер;
- Сервер логирования;
- Сервер конфигураций.

Сервер конфигураций позволяет администратору осуществлять централизованное управление настройками АРМ и учетных записей пользователей.

Сервер логирования осуществляет сбор локальных журналов событий (в зависимости от настроек журналирования)

Сервер Syslog осуществляет сбор журналов АРМ, а также позволяет использовать собранные данные как переменные в администрировании.

12.2 Настройка взаимодействия с серверами

Если параметры подключения к серверам не были указаны при установке или была выбрана установка локальной версии СЗИ НСД ARMlock в случае необходимости можно настроить взаимодействие с ними посредством настройки параметров подключения.

12.2.1 Настройка подключения к серверу конфигураций

Для настройки подключения к серверу конфигураций необходимо запустить консоль администратора нажать ЛКМ на иконке «*Добавить сервер конфигураций*» в панели инструментов консоли администрирования. (Рисунок 12.1)

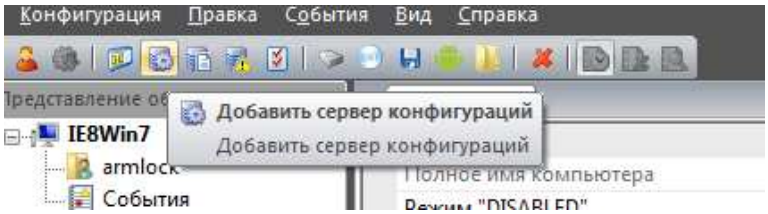

Рисунок 12.1 - Добавление сервера конфигураций

После этого появится окно с полями ввода параметров подключения к серверу. (Рисунок 12.2). В появившемся окне необходимо указать в поле «*Адрес*» адрес подключения к серверу. Допускается ввод как IP-адреса сервера, так и его доменного имени. (Например «CONFIGSERV.loc»)

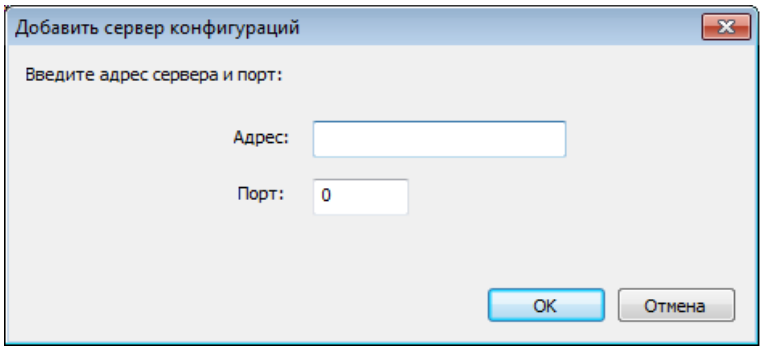

Рисунок 12.2 - Ввод параметров подключения к серверу конфигураций

После ввода параметров подключения необходимо нажать кнопку «*ОК*».

12.2.2 Настройка подключения к серверу логирования

Для настройки подключения к серверу логирования необходимо запустить консоль администратора, затем нажать ЛКМ на иконке «*Добавить сервер логирования*» в панели инструментов консоли администрирования. (Рисунок 12.3)

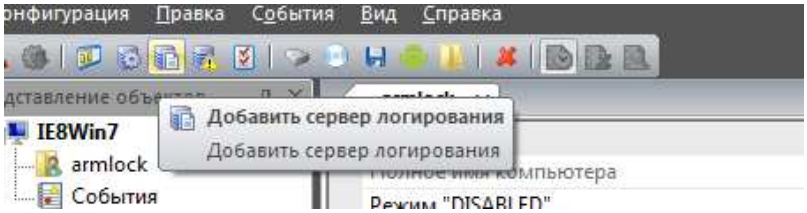

Рисунок 12.3 - Добавление сервера логирования

После этого появится окно с полями ввода параметров подключения к серверу. (Рисунок 12.4). В появившемся окне необходимо указать в поле «*Адрес*» адрес подключения к серверу. Допускается ввод как IP-адреса сервера, так и его доменного имени. (Например «SERVLOG.loc»)

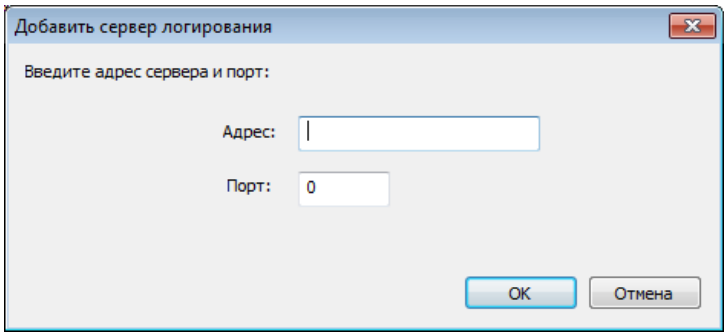

Рисунок 12.4 - Окно ввода параметров подключения к серверу логирования

После ввода параметров подключения необходимо нажать кнопку «*ОК*».

12.2.3 Настройка подключения к Syslog-серверу

Для настройки подключения к Syslog-серверу необходимо запустить консоль администратора, затем нажать ЛКМ на иконке «*Добавить syslog сервер*» в панели инструментов консоли администрирования. (Рисунок 122.5)

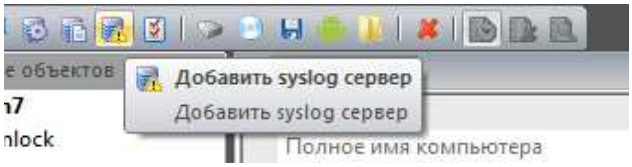

Рисунок 122.5 - Добавление Syslog-сервера

После этого появится окно с полями ввода параметров подключения к серверу. (Рисунок 12.6). В появившемся окне необходимо указать в поле «*Адрес*» адрес подключения к серверу. Допускается ввод как IP-адреса сервера, так и его доменного имени. (Например «SYSLOG»)

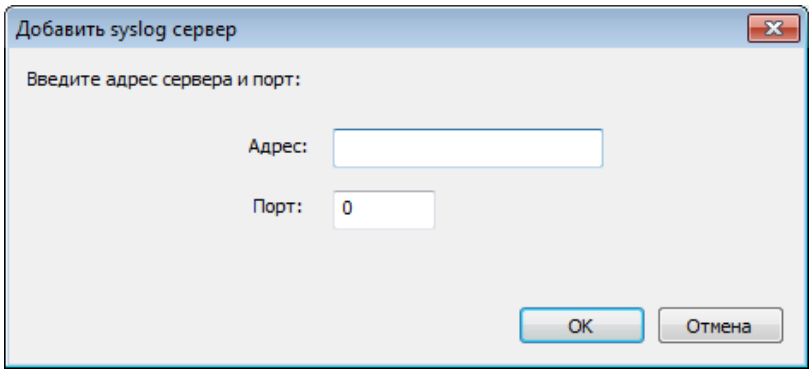

Рисунок 12.6 - Окно ввода параметров подключения к syslog-серверу

После ввода параметров подключения необходимо нажать кнопку «*ОК*».

13 Контроль целостности

СЗИ НСД ARMlock включает функционал контроля целостности файлов.

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

По умолчанию в системе уже создан ряд правил для контроля целостности рабочих файлов СЗИ «ARMlock». Эти правила нельзя удалить либо отредактировать, но пользователь может добавить собственные правила.

Для этого в локальной консоли администратора необходимо нажать на иконку «Добавить правило для контроля целостности файлов». При этом в конфигурации редактируемого пользователя (либо АРМ) будет создано новое правило, о чём локальная консоль информирует администратора.

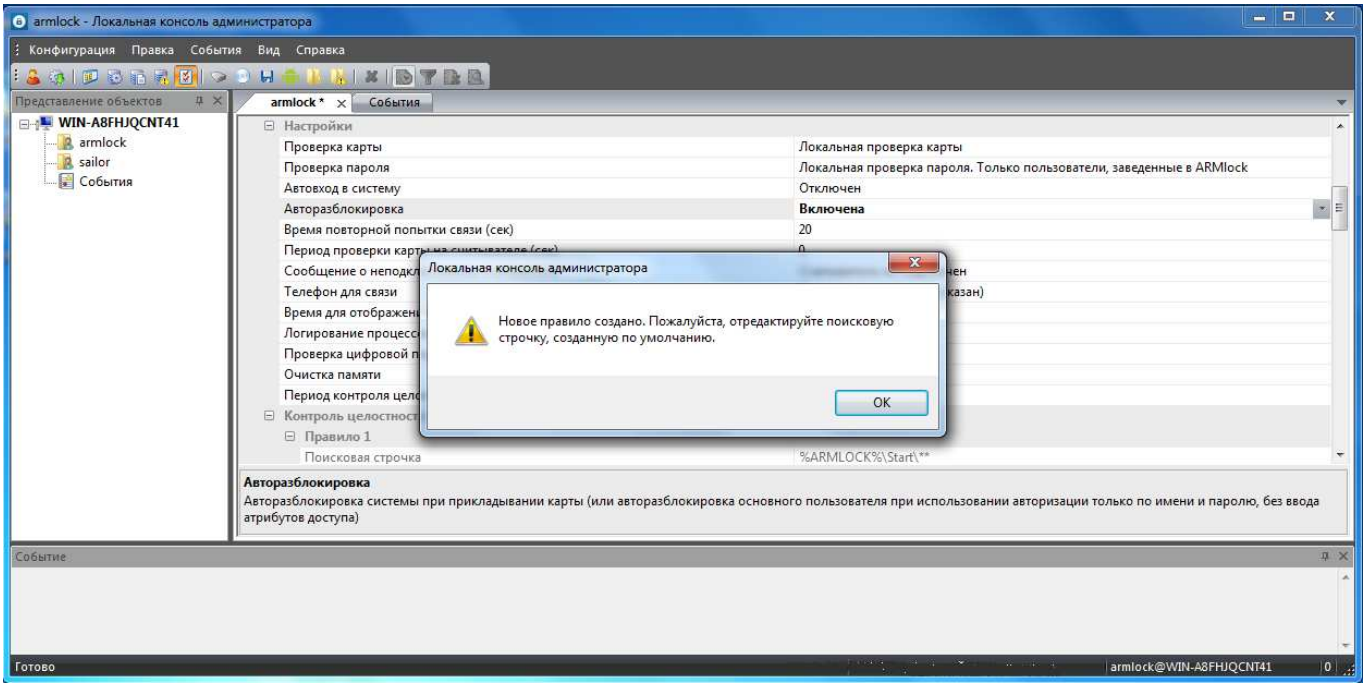

Рисунок 13.1 - Создание нового правила контроля целостности

Вновь созданное правило необходимо отредактировать, задав необходимую маску для файлов. Это можно сделать вручную, либо воспользовавшись диалогом, вызываемым кнопкой «..».

В случае задания маски с помощью диалогового окна 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 «*».

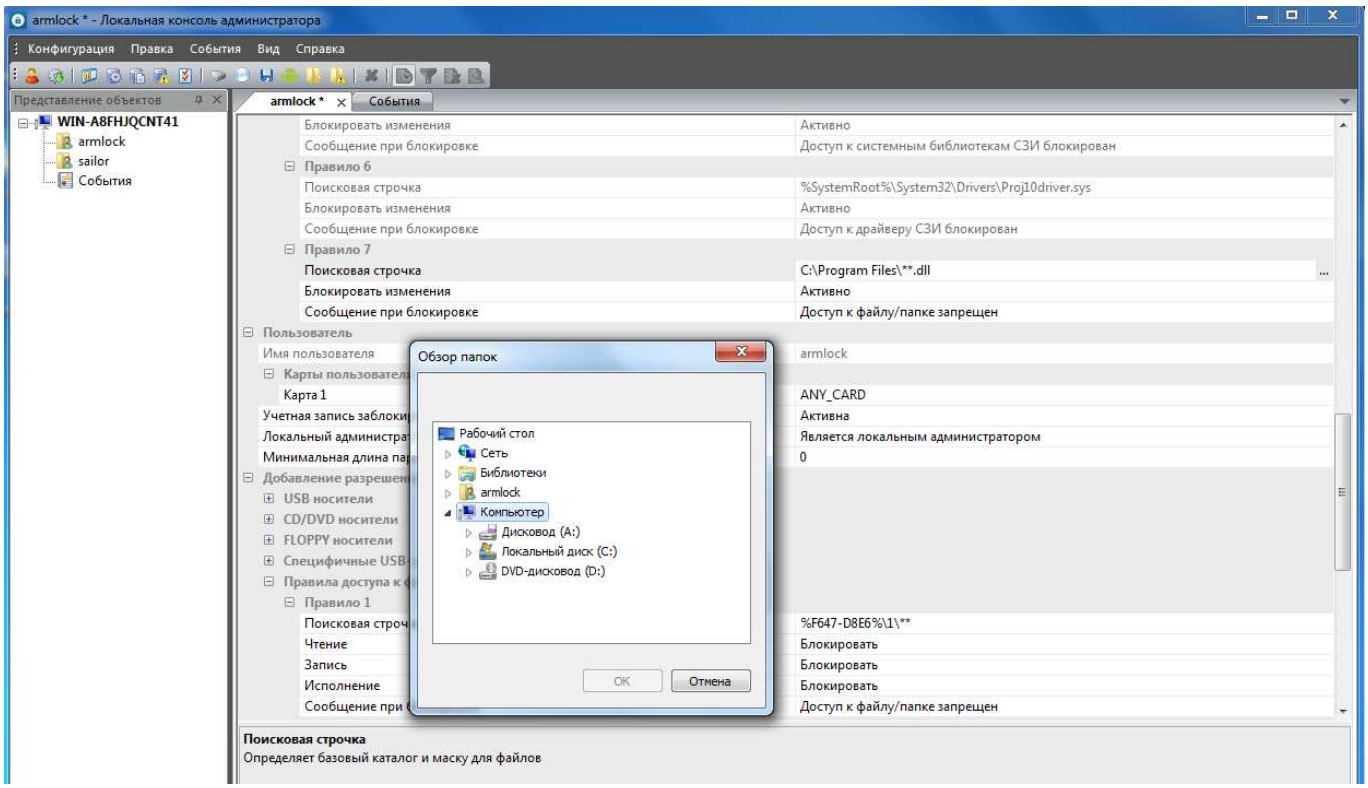

Рисунок 133.2 - Редактирование нового правила контроля целостности

В настройках правила также доступна опция «Блокировать изменения». Если данная опция выставлена в состояние «Активно», то система контроля целостности будет блокировать изменения файлов, удовлетворяющих данному правилу. Если же опция находится в состоянии «Отключено», то система будет только обнаруживать изменённые файлы и генерировать соответствующие события в журнал аудита.

Процедура проверки целостности файлов запускается при старте операционной системы, при смене активной конфигурации (т.е. при входе и выходе пользователя в/из Windows или при загрузке обновлённой конфигурации с сервера). Кроме того доступна опция периодического контроля целостности. Эта опция может быть настроена с помощью локальной консоли администратора (Рисунок 13.3)

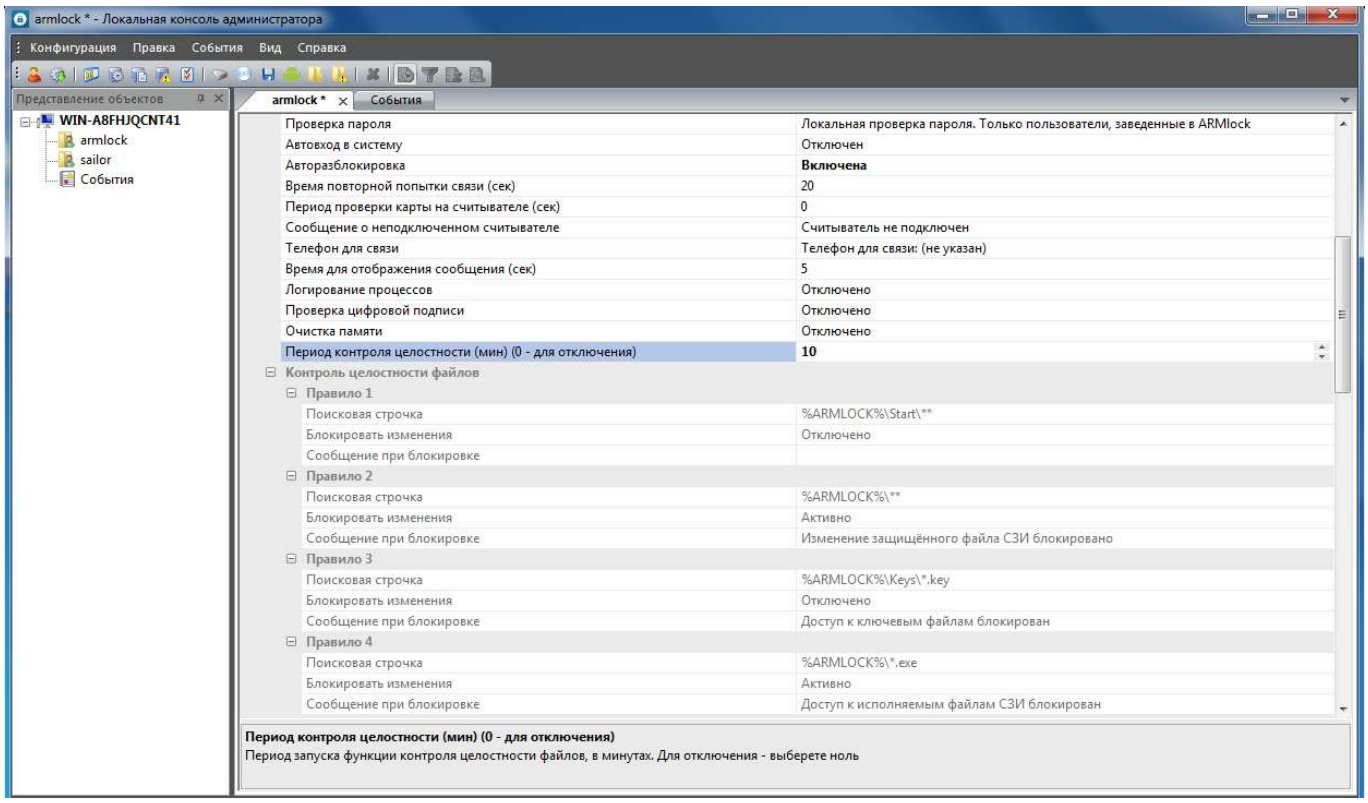

Рисунок 133.3 - Настройка периодического контроля целостности файлов

Данный параметр задаётся в минутах. Если выставить параметр в значение «0», то периодический контроль целостности будет отключен.

14 Термины и определения

Термины «компьютер» и «АРМ» считаются равнозначными.

Термин	Формулировка
• AD	Active Directory
• BIOS	Базовая система ввода-вывода, реализованная в виде микропрограмм, записанных в ПЗУ (постоянное запоминающее устройство) компьютера. Это – первая программа, которую компьютер использует сразу же после включения. Задача – опознать устройства (процессор, память, видео, диски и т. д.), проверить их исправность, инициализировать системные устройства
• АРМ	Автоматизированное рабочее место
• ЛКМ	Левая кнопка мыши
• НСД	Несанкционированный доступ
• ПКМ	Правая кнопка мыши
• Мышь	Ручной манипулятор, преобразующий механические движения в движение курсора на экране
• ОС	Операционная система
• САВЗ	Средство антивирусной защиты (Антивирус)
• СЗИ НСД	Система защиты информации от несанкционированного доступа

15 Изменения

В таблице приведены сведения о последних изменениях данного документа, включая версию, дату, автора и краткое описание изменений.

Версия	Дата	Автор	Изменения
01	16.12.2014	ООО «Вэлл-Сервис»	Создание документа
02	08.07.2015	ООО «Вэлл-Сервис»	Внесение исправлений и дополнений
03	23.07.2015	ООО «Вэлл-Сервис»	Внесение исправлений и дополнений