УТВЕРЖДЕНО
ПФНА.501410.001 34-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 4.68)

Руководство оператора (пользователя)

ПФНА.501410.001 34

Листов 23

Содержание

ВВЕДЕНИЕ

Система защиты информации в виртуальных инфраструктурах Dallas Lock включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах;
- агент управления доступом (далее по тексту — АУД);
- веб-сервер ЦУ СЗИ ВИ;
- агент DL ESXi для гипервизора ESXi;
- агент DL vCenter for Windows для сервера виртуализации vCenter (для ОС Windows);
- агент DL vCSA для сервера виртуализации vCSA;
- агент DL Hyper-V для гипервизора Hyper-V;
- агент DL Hyper-V Cluster для контроля кластера гипервизоров Hyper-V;
- агент DL VMM для ПО Microsoft System Center Virtual Machine Manager;
- агент DL KVM для гипервизора KVM;
- агент DL oVirt Engine для СВ oVirt;
- агент DL oVirt Host для гипервизора oVirt;
- агент DL zVirt Engine для СВ zVirt;
- агент DL zVirt Host для гипервизора zVirt;
- агент DL RedVirt Engine для СВ RedVirt;
- агент DL RedVirt Host для гипервизора RedVirt;
- агент DL HOSTVM Engine для СВ HOSTVM;
- агент DL HOSTVM Host для гипервизора HOSTVM.

Ядро СЗИ ВИ представляет собой компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий защиту серверов виртуализации посредством взаимодействия с АУД. Реализовано в виде службы.

В руководстве содержатся сведения, необходимые пользователю для работы на компьютерах с установленными компонентами защиты СЗИ ВИ.

Руководство подразумевает наличие у пользователя навыков работы в операционной среде Windows.

В руководстве представлены элементы графических интерфейсов СЗИ ВИ и операционной системы, которые соответствуют работе СЗИ ВИ в ОС Windows 7, Windows Server 2012 R2.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для СЗИ ВИ, другие используются для удобства, третьи выбраны из соображений краткости.

Термины *компьютер* и *ПК* считаются эквивалентными и используются в тексте руководства.

Принятые сокращения

Сокращение	Полная формулировка
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, инициировать
ESXi	гипервизор ESXi. Средство виртуализации VMware vSphere
HOSTVM Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации HOSTVM (СВ HOSTVM)
HOSTVM Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор HOSTVM
Hyper-V	гипервизор Hyper-V. Средство виртуализации Microsoft Hyper-V
KVM	Kernel-based Virtual Machine. Программное решение, обеспечивающее виртуализацию в среде Linux
Microsoft Hyper-V	платформа (среда) виртуализации серверов/рабочих станций 64х ОС Windows
oVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации oVirt (СВ oVirt)
oVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор oVirt
RedVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации RedVirt (СВ RedVirt)
RedVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор RedVirt
vCenter	VMware vCenter Server. Сервер централизованного управления средством виртуализации ESXi (vCenter for Windows)
vCSA	VMware vCenter Server Appliance. Сервер управления средством виртуализации ESXi (vCenter на виртуальной машине на базе ОС Photon)
zVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации zVirt (СВ zVirt)
zVirt Host	вычислительный узел (гипервизор), управляющий физическими хостами виртуализации, доменами данных, кластерами, виртуальными машинами и предоставляющая администратору интерфейс управления. Далее по тексту – гипервизор zVirt
VMware vSphere	платформа (среда) виртуализации серверов/рабочих станций с возможностями согласованного управления виртуальными центрами обработки данных

Агент DL ESXi	компонент защиты гипервизора ESXi
Агент DL HOSTVM Engine	компонент защиты сервера виртуализации HOSTVM
Агент DL HOSTVM Host	компонент защиты гипервизора HOSTVM
Агент DL Hyper-V	компонент защиты гипервизора Hyper-V
Агент DL Hyper-V Cluster	компонент защиты для контроля кластера гипервизоров Hyper-V
Агент DL KVM	компонент защиты гипервизора KVM
Агент DL oVirt Engine	компонент защиты сервера виртуализации oVirt
Агент DL oVirt Host	компонент защиты гипервизора oVirt
Агент DL RedVirt Engine	компонент защиты сервера виртуализации RedVirt
Агент DL RedVirt Host	компонент защиты гипервизора RedVirt
Агент DL vCenter for Windows	компонент защиты сервера vCenter
Агент DL vCSA	компонент защиты сервера vCSA
Агент DL VMM	компонент защиты для ПО Microsoft System Center Virtual Machine Manager
Агент DL zVirt Engine	компонент защиты сервера виртуализации zVirt
Агент DL zVirt Host	компонент защиты гипервизора zVirt
АУД	агент управления доступом. Компонент СЗИ ВИ Dallas Lock, устанавливаемый на объекты ВИ (сервер vCenter for Windows, гипервизор Hyper-V, SC VMM, кластеры Hyper-V) для обеспечения выполнения политик безопасности
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
ОС	операционная система
ПК	персональный компьютер
Центр управления СЗИ ВИ Dallas Lock	совокупность программных компонентов АУД и Ядра СЗИ ВИ, управляемая с помощью Консоли

1 ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ

1.1 Назначение системы защиты

СЗИ ВИ предназначена для защиты среды виртуализации на VMware vSphere (vCenter for Windows 5.5, 6.0, 6.5, 6.7 и vCSA 6.5, 6.7, 7.0 совместно с ESXi[1] аналогичной версии), Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019), KVM, использующей библиотеки libvirt (версии не ниже 4.5.0) в качестве инструмента управления гипервизором, oVirt (версия 4.4.x) и Виртуализация zVirt (версий 3.0, 3.1, 3.3, 4.0), РЕД Виртуализация 7.3 и HOSTVM от несанкционированного доступа при работе в многопользовательских автоматизированных системах, государственных информационных системах, в автоматизированных системах управления, информационных системах персональных данных и на объектах критической информационной инфраструктуры.

В соответствии с требованиями безопасности предприятия лицами, ответственными за установку и эксплуатацию СЗИ ВИ, настраиваются соответствующие параметры и политики безопасности, механизмы которых реализованы в СЗИ ВИ. Подробное описание настройки механизмов администрирования СЗИ ВИ содержится в документе ПФНА.501410.001 РЭ «Руководство по эксплуатации».

Оператором (пользователем) СЗИ ВИ является пользователь, осуществляющий ввод и обработку информации любыми программными средствами на персональном компьютере, на котором установлен один из компонентов СЗИ ВИ.

1.2 Условия работы

1.2.1 Данные учетной записи

Чтобы получить доступ к компьютеру, на который установлена СЗИ ВИ, необходимо иметь зарегистрированную в СЗИ ВИ учетную запись. Регистрация учетных записей осуществляется администратором безопасности.

Учетная запись пользователя, зарегистрированного в СЗИ ВИ, имеет следующие атрибуты, которые необходимы непосредственно для входа на защищенный компьютер (авторизации):

Основные	
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)
Имя домена	Необходимо для доменных пользователей
Персональный идентификатор	Пользователю может быть выдан один электронный идентификатор
Дополнительные	
PIN-код аппаратного идентификатора	Если пользователю назначен аппаратный идентификатор, то для авторизации дополнительно может быть использован PIN-код идентификатора

Внимание! Чтобы приступить к работе на компьютере, необходимо:

1. Уточнить у администратора безопасности все авторизационные данные для входа на защищенный компьютер.
2. Запомнить свое имя в системе защиты и пароль.
3. Никому не сообщать пароль и никому не передавать персональный аппаратный идентификатор.

[1] Для защиты среды виртуализации на базе гипервизора ESXi 5.5 необходимо применять сертифицированную версию изделия СЗИ ВИ Dallas Lock 376.3.

Авторизация пользователя осуществляется при каждом входе.

При вводе имени и пароля необходимо соблюдать следующие правила:

- **для имени:**
  a. максимальная длина имени — 20 символов;
  b. имя может содержать латинские символы, символы кириллицы, цифры и специальные символы;
  c. 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:**
  a. максимальная длина пароля — 32 символа;
  b. пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
  c. разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (Password и password являются разными паролями).

1.2.2 Права для работы под учетной записью

Также необходимо выяснить у администратора безопасности, какими именно правами и привилегиями обладает оператор (пользователь), к каким ресурсам может иметь доступ и с какими программами и приложениями работать.

Во всех сложных ситуациях, связанных с работой СЗИ ВИ, которые оператор (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 ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР

2.1 Вход в операционную систему

При загрузке компьютера, на который установлен один из компонентов СЗИ ВИ, в зависимости от ОС, появляется экран приветствия (приглашение на вход в операционную систему) (рис. 1, рис. 2).

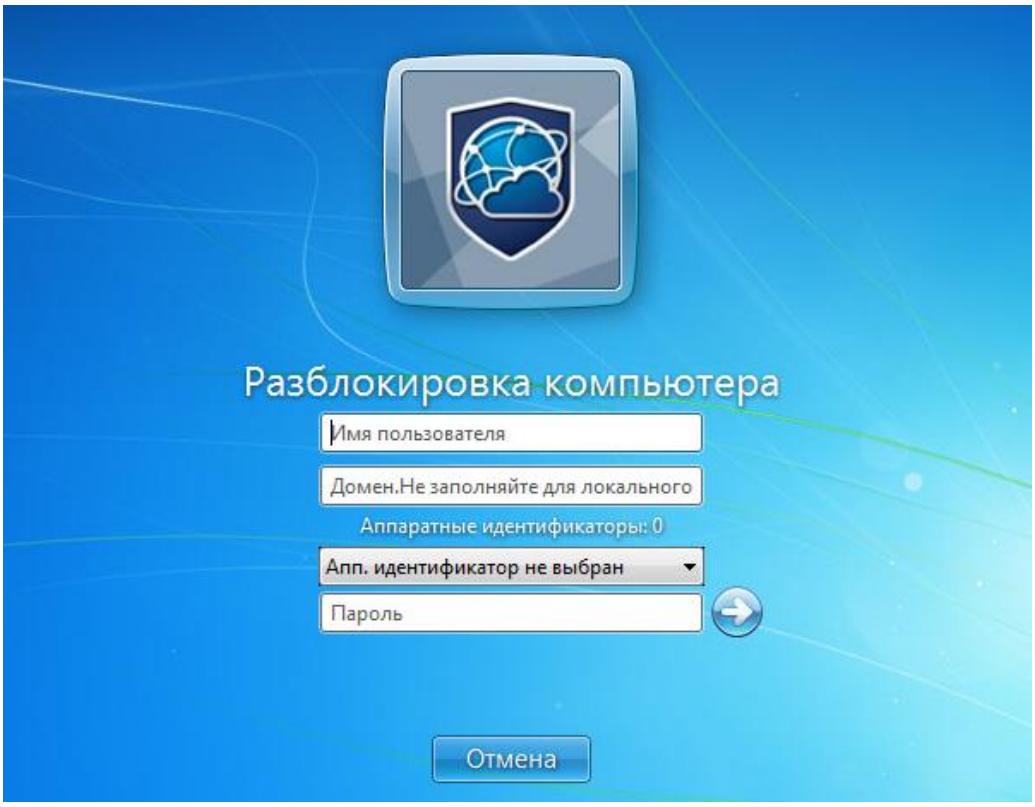

Рис. 1. Экран приветствия в ОС Windows 7

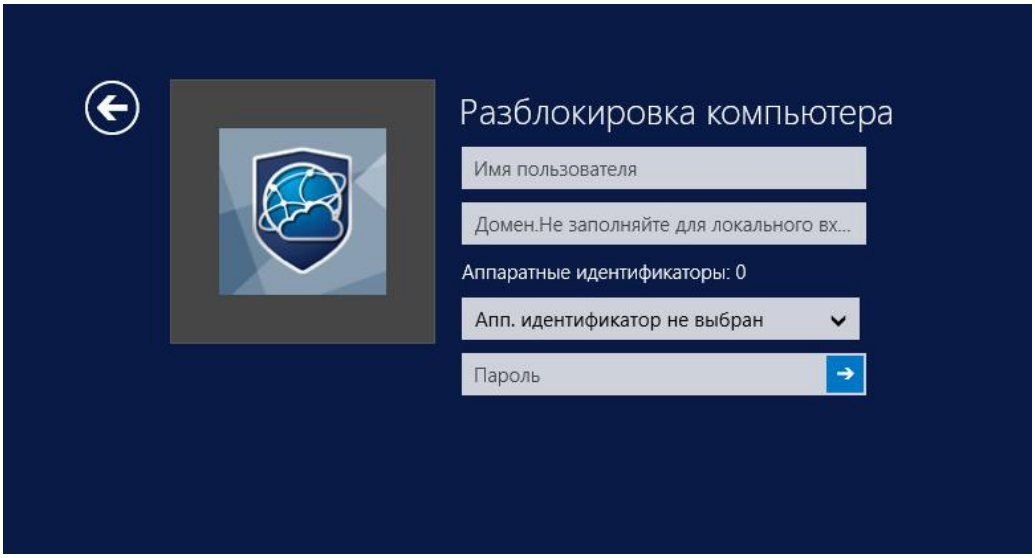

Рис. 2. Экран приветствия ОС Windows Server 2012 R2

Для входа на компьютер, на который установлен один из компонентов СЗИ ВИ, каждому оператору (пользователю) предлагается выполнить следующую последовательность шагов.

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе защиты. В зависимости от настроек в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.

3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить (подробное описание приводится ниже).
4. 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.
5. Нажать кнопку «Enter».

После нажатия кнопки «Enter» осуществляется проверка наличия в системе защиты зарегистрированного пользователя с указанным именем. После чего проверяется соответствие с именем пользователя номера аппаратного идентификатора, зарегистрированного в системе защиты, и правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход.

Если пользователю назначен аппаратный идентификатор, то необходимо выполнить следующие шаги:

1. В зависимости от типа устройства предъявить идентификатор можно, вставив его в USB-порт, или прикоснувшись к считывателю.
2. Необходимо выбрать наименование идентификатора из списка, который появится в выпадающем меню в поле «Аппаратные идентификаторы» (рис. 3).

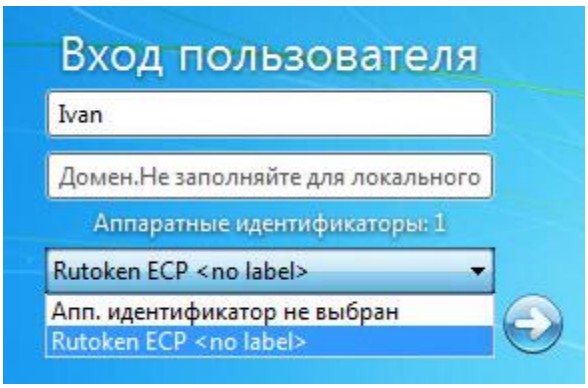

Рис. 3. Выбор аппаратного идентификатора при входе в ОС Windows

При подключении единственного идентификатора он будет выбран автоматически.

3. Далее, в зависимости от настроек, произведенных администратором безопасности применительно к учетной записи пользователя, возможны следующие способы авторизации:
   - Выбор аппаратного идентификатора и заполнение всех авторизационных полей формы (рис. 4).

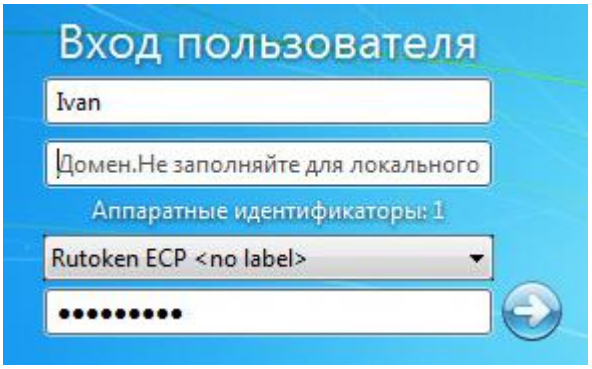

Рис. 4. Поля авторизации после предъявления идентификатора

   - Выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (рис. 5):

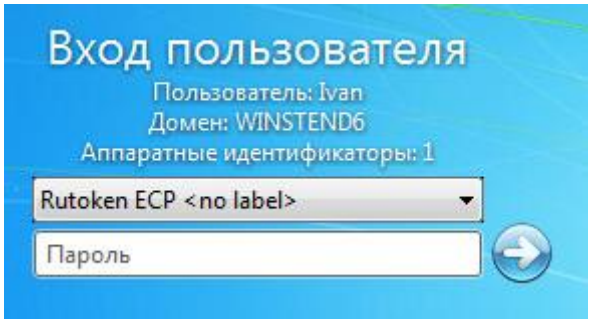

Рис. 5. Поля авторизации после предъявления идентификатора

- Выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 6):

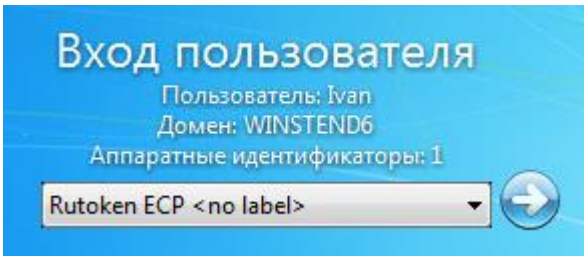

Рис. 6. Поля авторизации после предъявления идентификатора

- Выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 7):

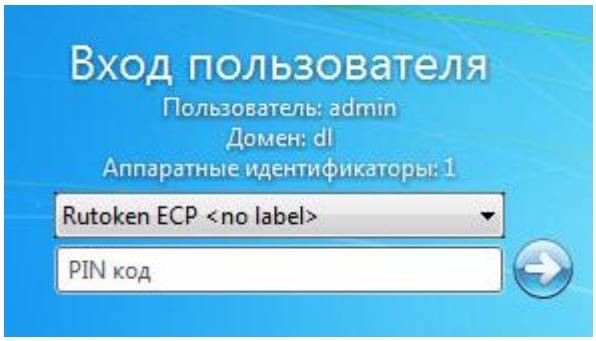

Рис. 7. Поля авторизации после предъявления идентификатора

Примечание. Изменение настроек параметров различных категорий возможно несколькими способами: двойным кликом выделенного параметра, с помощью кнопки «Свойства» на панели действий или с помощью контекстного меню параметра, вызываемого правой кнопкой мыши.

Внимание! При получении аппаратного идентификатора оператору (пользователю) следует выяснить, необходим ли идентификатор для работы на данном ПК. Администратором безопасности может быть настроено так, что использование аппаратного идентификатора обязательно для работы на защищенном компьютере, и при отключении идентификатора компьютер может быть заблокирован.

2.2 Ошибки, возникающие при входе

Попытка входа оператора (пользователя) на компьютер, на который установлен один из компонентов СЗИ ВИ, может быть неудачной, к чему приводит ряд событий. При этом на экран могут выводиться сообщения о характере события или соответствующие сообщения предупреждающего характера.

Если введенный пароль неверен, то на экране появится сообщение об ошибке, после чего система защиты предоставит возможность повторно ввести имя и пароль (рис. 8).

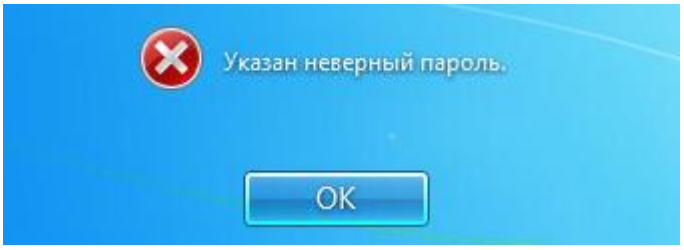

Рис. 8. Сообщение при вводе неправильного пароля

Подобное сообщение появится и при предъявлении неверного аппаратного идентификатора или в случае, когда зарегистрированный за оператором (пользователем) идентификатор не предъявлен вообще (рис. 9).

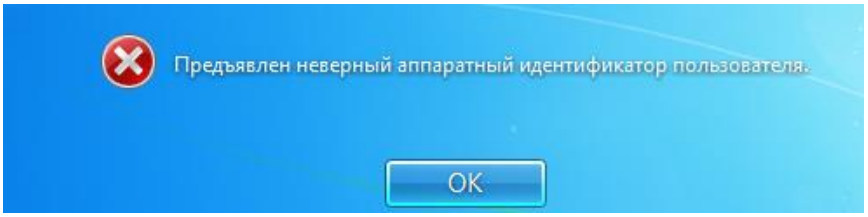

Рис. 9. Сообщение при неверном идентификаторе

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

Так же при ошибочном вводе данных в поле имени или домена могут возникнуть соответствующие сообщения (рис. 10).

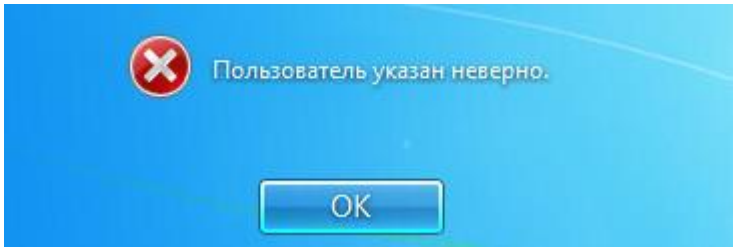

Рис. 10. Ошибка авторизации

Администратор может отключить учетную запись, тогда при авторизации система защиты выведет соответствующее предупреждение (рис. 11).

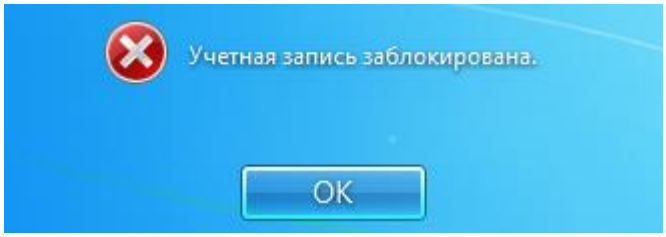

Рис. 11. Сообщение при отключенной учетной записи

В такой ситуации необходимо обратиться к администратору системы защиты.

При проблеме подключения по локальной сети может возникнуть ошибка авторизации доменных пользователей (рис. 12).

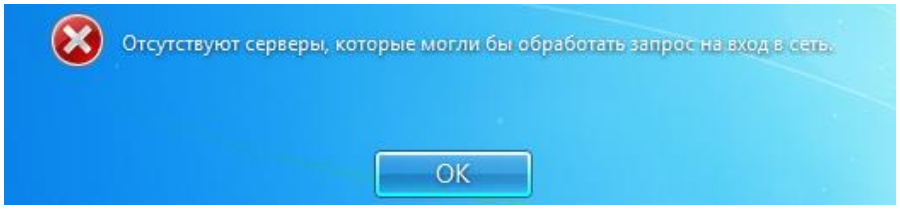

Рис. 12. Ошибка при вводе имени домена

В этом случае необходимо обратиться к администратору безопасности.

На этапе загрузки компьютера осуществляется контроль целостности аппаратно-программной среды BIOS, поэтому может быть выведено предупреждение о нарушении данных параметров.

После ввода имени и пароля на этапе загрузки компьютера на экране может появиться предупреждение о том, что нарушен контроль целостности, вход в операционную систему для пользователя будет запрещен (рис. 13).

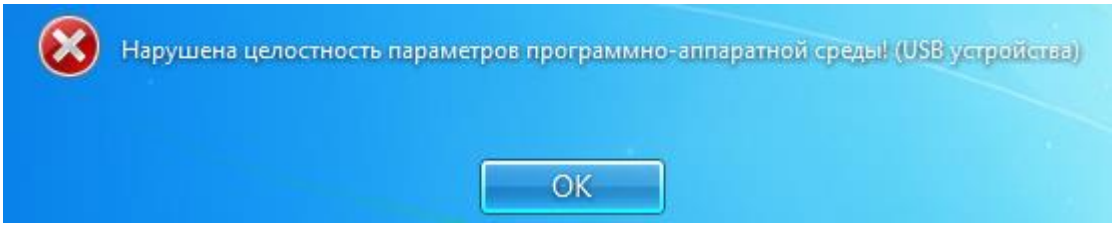

Рис. 13. Сообщение при входе

Также возможен случай, когда при нарушении целостности вход в ОС осуществляется, но на панели задач в области уведомлений появляется всплывающее предупреждение о нарушении целостности (рис. 14).

Рис. 14. Предупреждение о нарушенной целостности

Администратором безопасности может быть задан особый механизм контроля доступа к информационным ресурсам — «мягкий» режим контроля доступа. При включенном «мягком» режиме проверяются все права доступа оператора (пользователя) к ресурсам и программам, сообщения о запрете, при попытке осуществления запрещенной политиками безопасности операции, заносятся в журнал системы защиты, и в тоже время доступ к запрещенным объектам предоставляется, не смотря на запрет.

При включенном «мягком» режиме после загрузки операционной системы на панели задач в области уведомлений появляется всплывающее предупреждение.

Подобное сообщение после загрузки операционной системы можно увидеть, если администратор включил неактивный режим (рис. 15).

Рис. 15. Предупреждение о включенном неактивном режиме

При появлении таких предупреждений работа на данном компьютере для оператора (пользователя) разрешается, ошибки не возникает.

Внимание! При всех возникающих затруднительных ситуациях следует обращаться к администратору безопасности.

3 ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ

3.1 Завершение работы

Внимание! Компьютер, на котором установлен Центр управления СЗИ ВИ Dallas Lock, предназначен для режима беспрерывной работы. Выключение данного компьютера влечет за собой нештатную ситуацию в работе СЗИ ВИ.

При завершении сеанса работы оператора (пользователя) на компьютере, на котором установлен один из компонентов СЗИ ВИ, выполняется выход оператора (пользователя) из системы. Для этого нужно (при работе в ОС Windows 7):

1. Сохранить все данные и завершить работу всех приложений.
2. В меню «Пуск» в нижнем правом углу нажать вызов меню возле кнопки «Завершение работы» и выбрать пункт «Выйти из системы».
3. После нажатия кнопки «Выйти из системы» сеанс текущего оператора (пользователя) будет завершен, а на экране появится диалог для повторной авторизации в системе защиты.
4. При работе в ОС Windows Server 2012 R2 необходимо:
5. Сохранить все данные и завершить работу всех приложений.
6. Нажать кнопку «Пуск». В правом верхнем углу левой кнопкой мыши нажать на поле учетной записи оператора (пользователя).
7. Из выпадающего меню выбрать пункт «Выйти».
8. После нажатия кнопки «Выйти из системы» сеанс текущего оператора (пользователя) будет завершен, а на экране появится диалог для повторной авторизации в системе защиты.

3.2 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:

1. В ОС Windows 7 в меню «Пуск» в нижнем правом углу нажать вызов меню возле кнопки «Завершение работы» и выбрать пункт «Сменить пользователя» (рис. 16).

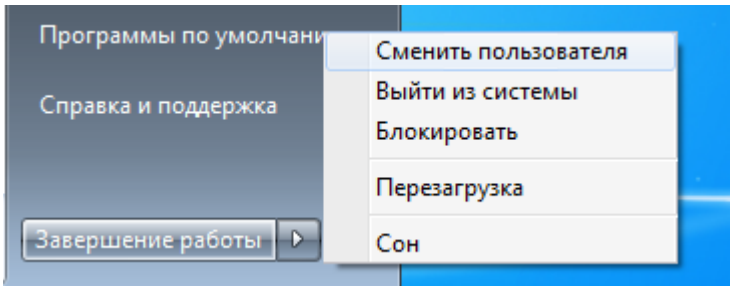

Рис. 16. Смена пользователя в ОС Windows 7

2. В ОС Windows 2012 R2 в меню «Пуск» в правом верхнем углу левой кнопкой мыши нажать на поле учетной записи оператора (пользователя). Из выпадающего меню выбрать пункт «Выйти» (рис. 17).

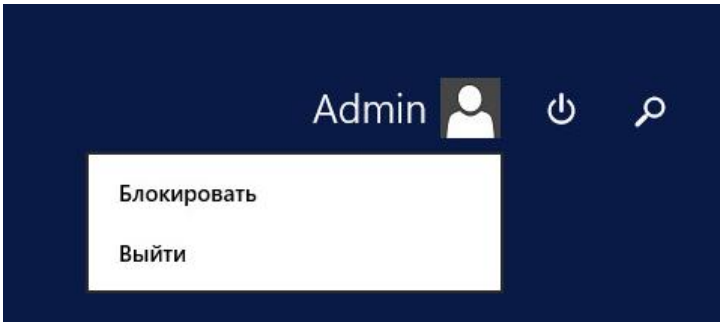

Рис. 17. Смена пользователя в ОС Windows Server 2012 R2

Сеанс текущего пользователя будет завершен, а на экране появится диалог для повторной авторизации в системе защиты.

Внимание! При смене сеанса пользователя, хотя выход пользователя и происходит, но на компьютере продолжают работать все запущенные им приложения, и в случае завершения работы компьютера одним из пользователей на экране появится соответствующее предупреждение.

Перед сменой пользователя рекомендуется сохранить все необходимые данные и закончить работу приложений, так как администратором безопасности в СЗИ ВИ может быть включен режим запрета смены пользователя без перезагрузки компьютера.

В этом случае, при смене пользователя, операционная система автоматически завершит работу и выполнит перезагрузку (рис. 18).

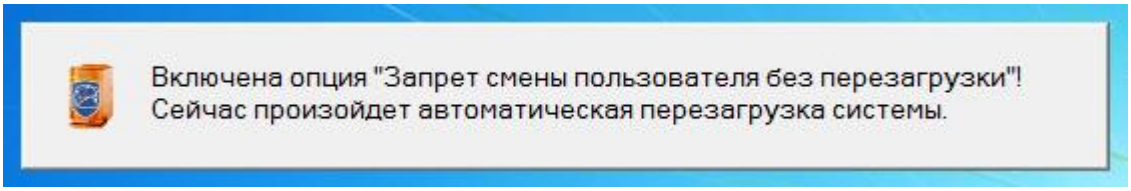

Рис. 18. Автоматическая перезагрузка при смене пользователя

Несохраненные другими пользователями результаты работы в этом случае не сохранятся.

4 СМЕНА ПАРОЛЯ

Оператор (пользователь) может самостоятельно сменить свой пароль для авторизации.

1. Для этого, после входа в ОС, необходимо нажать комбинацию клавиш «Ctrl-Alt-Del» и выбрать операцию «Сменить пароль» (рис. 19).

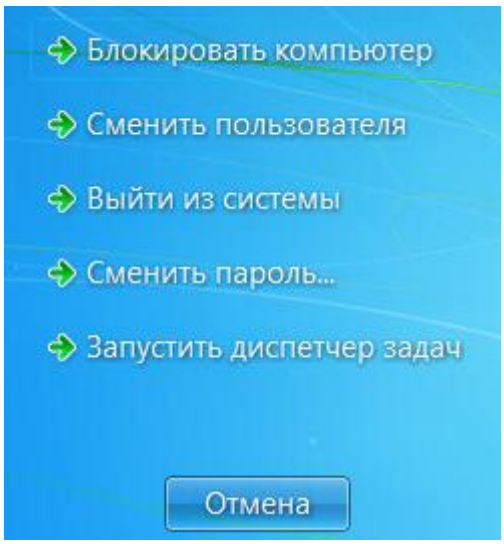

Рис. 19. Меню действий в ОС Windows 7

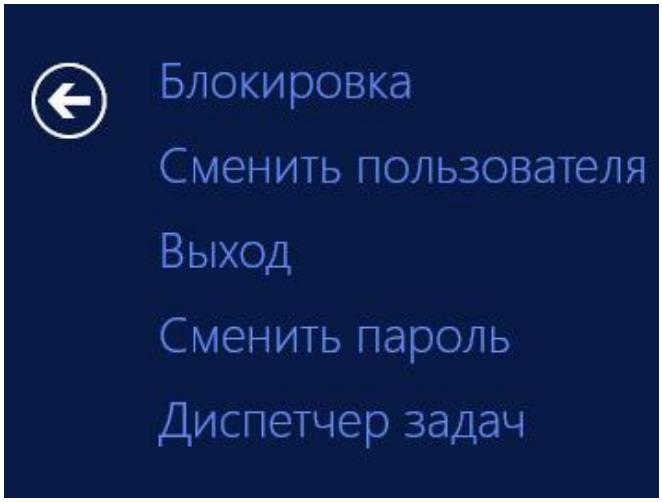

Рис. 20. Меню действий в ОС Windows Server 2012 R2

На экране появится диалоговое окно, предлагающее ввести данные для смены пароля (рис. 21).

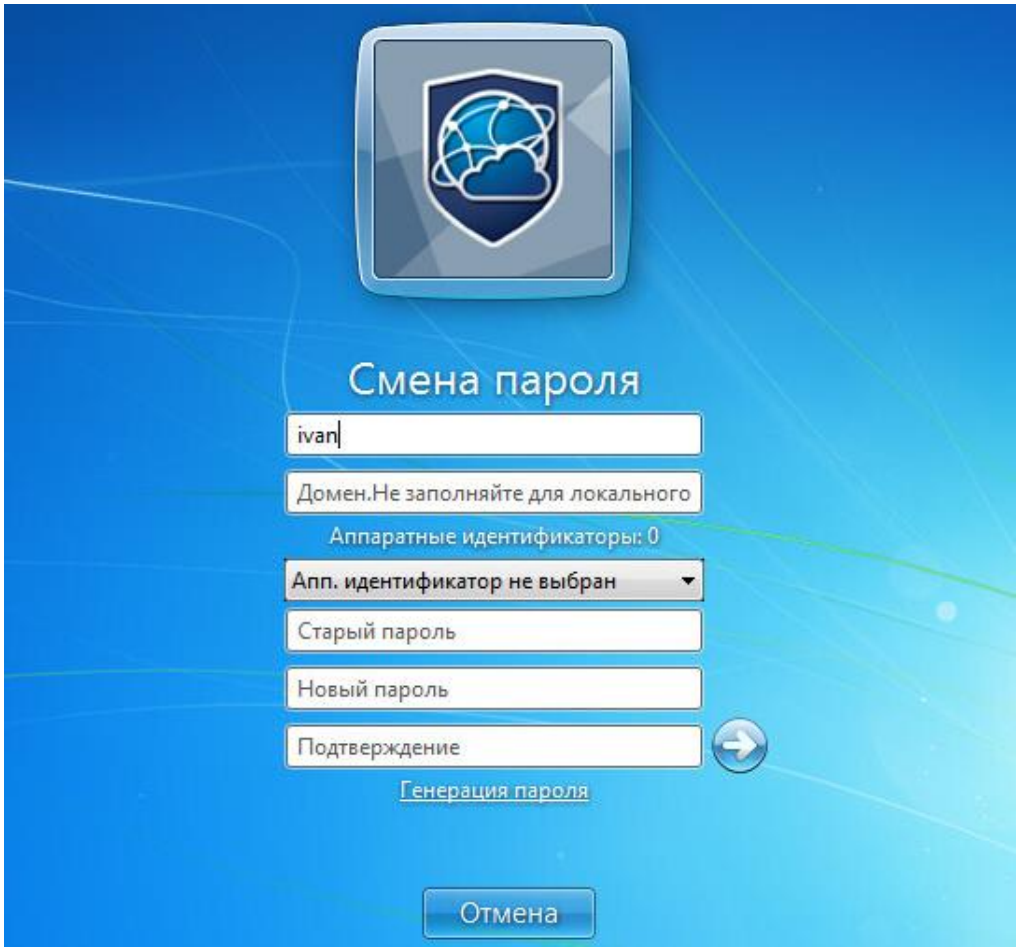

Рис. 21. Экран смены пароля в ОС Windows 7

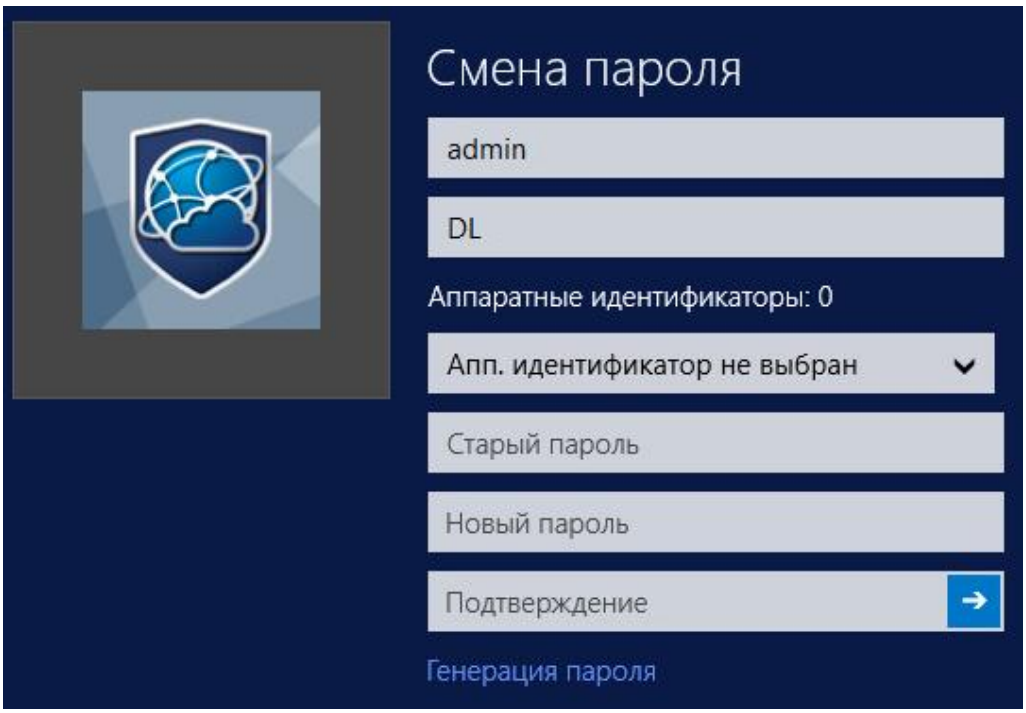

Рис. 22. Экран смены пароля в ОС Windows Server 2012 R2

2. В открывшемся диалоговом окне необходимо ввести в соответствующие поля имя пользователя, имя домена (для доменного пользователя, для локального — оставить это поле пустым), старый пароль, новый пароль и подтверждение нового пароля.
3. Предъявить назначенный аппаратный идентификатор, выбрав его из выпадающего меню.

Примечание. Если текущему оператору (пользователю) назначен аппаратный идентификатор, на который записаны авторизационные данные, то при смене пароля, помимо заполнения других полей, необходимо предъявить идентификатор и ввести PIN-код пользователя идентификатора.

4. Для создания пароля, отвечающего всем требованиям параметров безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать поле с надписью: «Генерация пароля». Система защиты автоматически создаст случайный пароль, значение которого необходимо ввести в поля «Новый пароль» и «Повтор».
5. Далее нажать кнопку «ОК» для сохранения нового пароля или кнопку «Отмена».

В соответствии с политиками безопасности 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;
- напоминание 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.

В соответствии с тем, какие из параметров включены, при смене пароля на экране могут возникать сообщения об ошибках (рис. 23 — рис. 27).

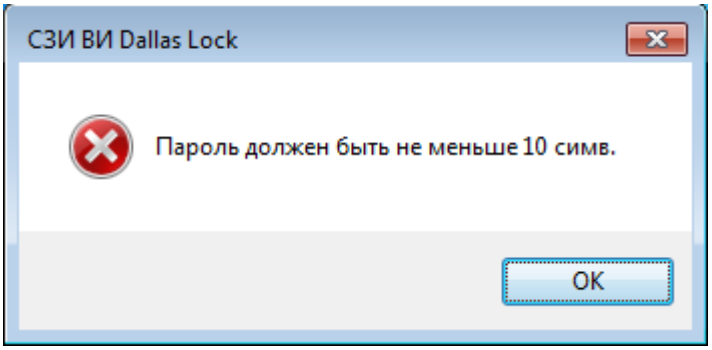

Рис. 23. Ошибка при смене пароля. Требования к длине пароля

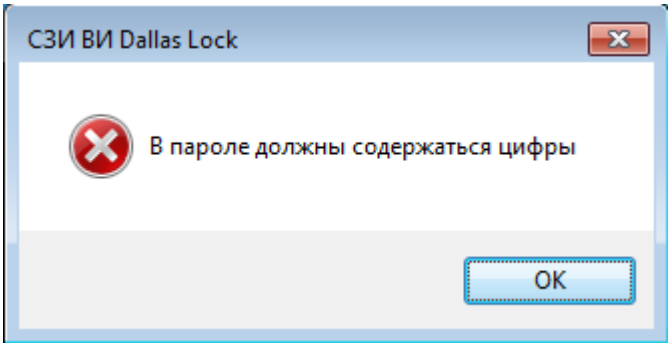

Рис. 24. Ошибка при смене пароля. Необходимость наличия цифр

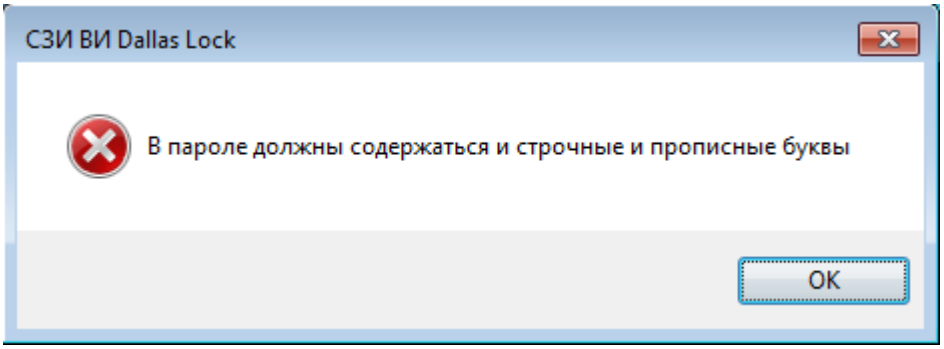

Рис. 25. Ошибка при смене пароля. Необходимость наличия заглавных букв

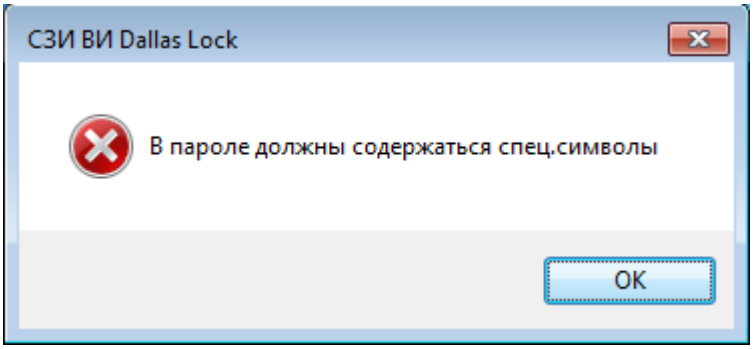

Рис. 26. Ошибка при смене пароля. Необходимость наличия спецсимволов

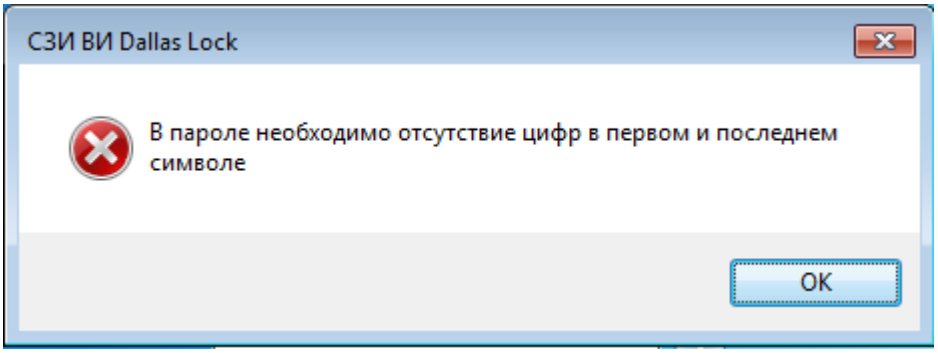

Рис. 27. Ошибка при смене пароля. Необходимость отсутствия цифр

При возникновении подобных сообщений необходимо изменить пароль в соответствии с требованиями администратора безопасности.

Может возникнуть сообщение о том, что пароль не может быть изменен (рис. 28).

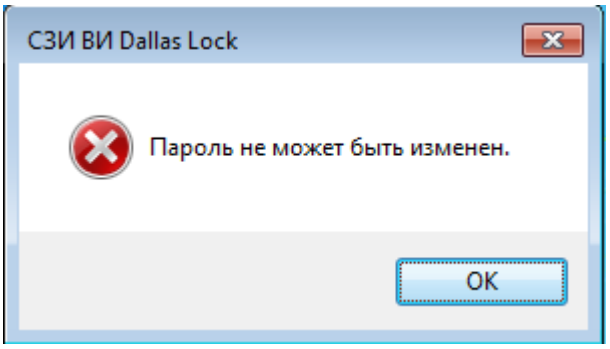

Рис. 28. Сообщение системы при смене пароля

Появление этого сообщения означает, что администратор запретил данному оператору (пользователю) самостоятельно менять пароль. В этом случае необходимо обратиться к администратору безопасности системы защиты.

Если все требования соблюдены, то пароль пользователя будет успешно сменен, появится соответствующее сообщение (рис. 29).

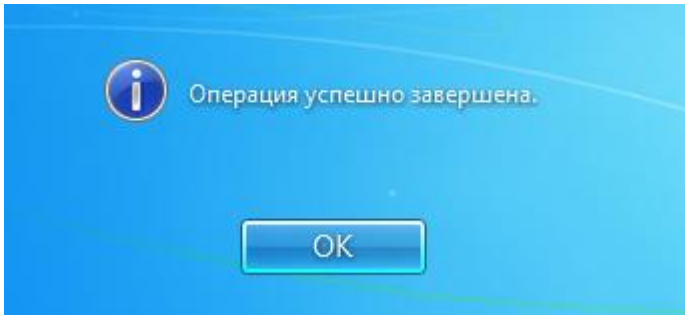

Рис. 29. Успешная смена пароля

Далее вход оператора (пользователя) на защищенную СЗИ ВИ рабочую станцию будет осуществляться с новым паролем.

5 БЛОКИРОВКА КОМПЬЮТЕРА

В некоторых случаях возникает необходимость временной блокировки компьютера без завершения сеанса работы пользователя. Заблокировать защищенный системой защиты компьютер можно 3-мя способами, приведенными ниже.

1. Дважды кликнуть правой клавишей мыши на иконку , которая находится в нижнем правом углу экрана в выпадающем меню области уведомлений (рис. 30).

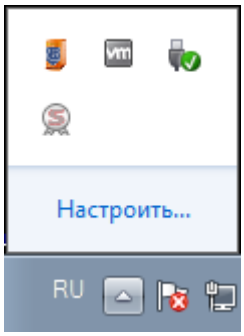

Рис. 30. Иконка блокировки на панели задач

2. Нажать комбинацию клавиш «Win» + «L» (рис. 31).

Рис. 31. Комбинация клавиш «Win» + «L»

3. Нажать комбинацию клавиш «Ctrl+Alt+Del» и на появившемся экране выбрать кнопку «Блокировать компьютер» (рис. 32).

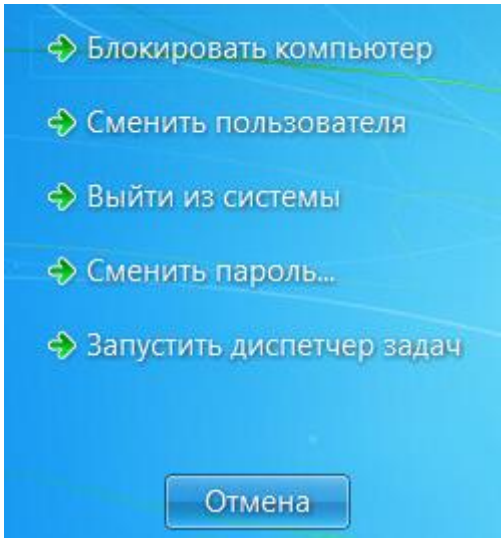

Рис. 32. Меню блокировки экрана

Компьютер может заблокироваться автоматически по истечении заданного периода неактивности пользователя. Период неактивности, после которого компьютер будет автоматически заблокирован, задается стандартными средствами операционной системы (рис. 33).

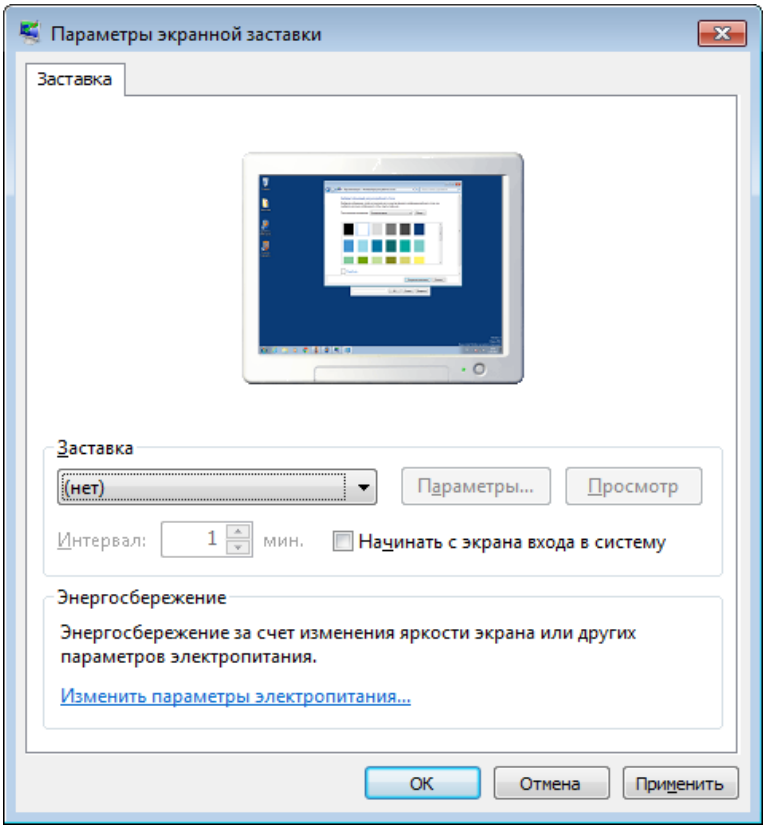

Рис. 33. Параметры автоматической блокировки экрана

После того, как компьютер заблокирован, разблокировать его может только пользователь, выполнивший блокировку, либо администратор безопасности. В случае разблокировки компьютера администратором, сеанс работы пользователя будет автоматически завершен.

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

При попытке войти на заблокированный пользователем компьютер под учетной записью другого пользователя, на экране появится предупреждение (рис. 34)

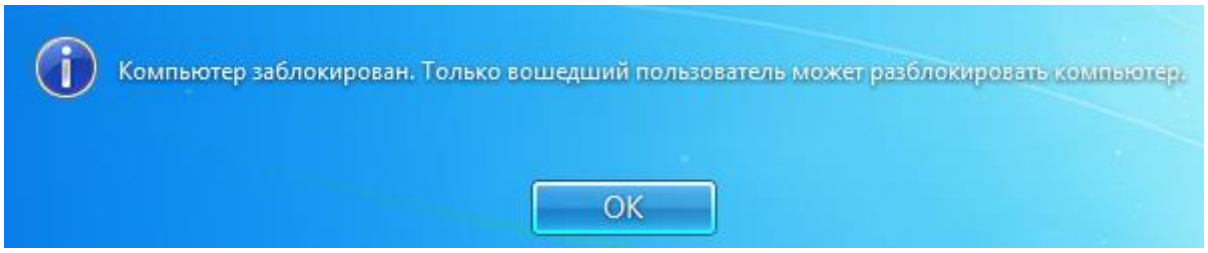

Рис. 34. Сообщение ОС при попытке входа на заблокированный компьютер

6 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

СЗИ ВИ предоставляет пользователю несколько дополнительных возможностей, позволяющих увеличить уровень защищенности информации.

6.1 Механизм очистки остаточной информации

Большинство операционных систем при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории файловой системы.
Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть, по крайней мере, до тех пор, пока операционная система заново не использует это пространство для хранения новых данных. Такая остаточная информация может легко привести к непреднамеренному распространению конфиденциальной информации.
В СЗИ ВИ реализована функция очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.
При необходимости удаления пользователем каких-либо данных без возможности их восстановления, необходимо выполнить следующие действия.

1. В контекстном меню объекта файловой системы, который необходимо удалить, выбрать пункт «СЗВИ: Удалить и зачистить» (рис. 35).

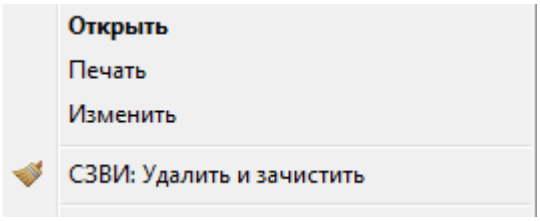

Рис. 35. Контекстное меню

2. Нажать «Да» в появившемся окне подтверждения операции (рис. 36).

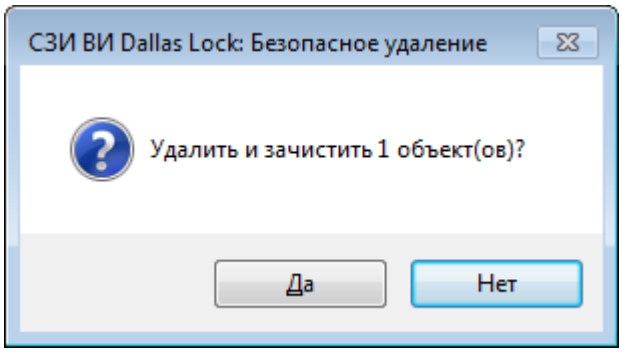

Рис. 36. Окно подтверждения операции

При активации удаления происходит зачистка данного объекта путем однократной перезаписи файла. После однократного цикла перезаписи восстановить хоть сколько-нибудь значимый фрагмент файла становится практически уже невозможно.
После успешного удаления объектов система защиты выведет соответствующее подтверждение (рис. 37).

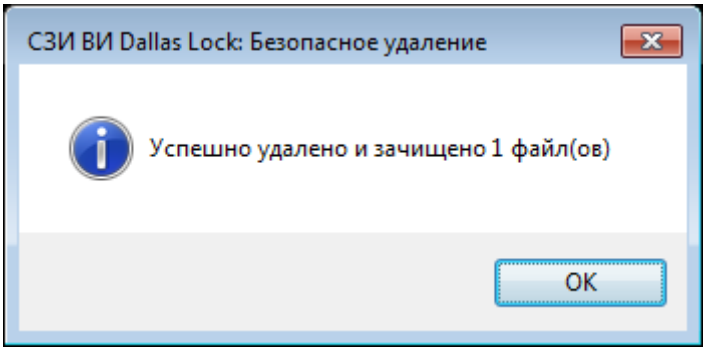

Рис. 37. Сообщение об удалении файлов

Примечание. При нескольких одновременно выделенных объектах происходит их одновременное удаление и зачистка. При этом появляется окно подтверждения удаления с количеством зачищаемых объектов.

Права на очистку остаточной информации конкретному пользователю для конкретного файла определяются параметрами безопасности, установленными администратором безопасности. Если у пользователя данные права отсутствуют, то при попытке зачистки и удаления файла появится предупреждающее сообщение (рис. 38).

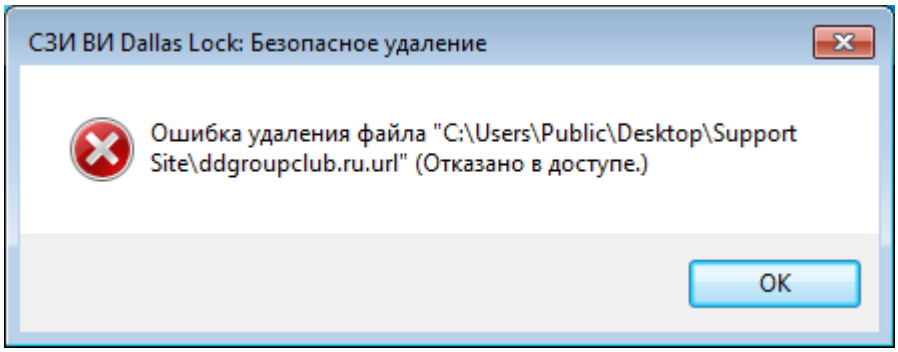

Рис. 38. Сообщение на запрет удаления файла