

УТВЕРЖДЕНО
RU.48957919.501410-01 34-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА Dallas Lock 8.0-K

Руководство оператора (пользователя)



RU.48957919.501410-01 34

Листов 32

2015

Содержание

Введение.....	3
1. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ	4
1.1. Назначение системы защиты	4
1.2. Условия работы.....	5
2. ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР	7
2.1. Вход в операционную систему	7
2.2. Ошибки, возникающие при входе	10
3. ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ	13
3.1. Завершение работы.....	13
3.2. Смена пользователя.....	13
4. СМЕНА ПАРОЛЯ	15
5. БЛОКИРОВКА КОМПЬЮТЕРА	19
6. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ.....	21
6.1. Механизм очистки остаточной информации	21
6.2. Преобразование информации.....	23
Термины и определения	31

Введение

Данное руководство предназначено для пользователей рабочих станций, на которых установлена Системы защиты информации от несанкционированного доступа Dallas Lock 8.0-K (далее по тексту – система защиты, СЗИ НСД или Dallas Lock 8.0-K).

В руководстве содержатся сведения, необходимые пользователю для работы на защищенном Dallas Lock 8.0-K компьютере, и непосредственно с компонентами установленной системой защиты.

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

В руководстве представлены элементы графических интерфейсов системы защиты Dallas Lock 8.0-K и операционной системы, которые соответствуют работе Dallas Lock 8.0-K в ОС Windows 7 и Windows XP.

ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ

1.1. Назначение системы защиты

Система защиты Dallas Lock 8.0-K представляет собой программный комплекс средств защиты информации в ОС семейства Windows.

Система защиты информации от несанкционированного доступа Dallas Lock 8.0-K предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации.

СЗИ НСД Dallas Lock 8.0-K предназначена для использования на персональных компьютерах, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), также поддерживает виртуальные среды (к примеру, VMware).

В соответствии с требованиями безопасности предприятия лицами, ответственными за установку и эксплуатацию системы защиты, настраиваются соответствующие параметры и политики безопасности, механизмы которых реализованы в системе защиты Dallas Lock 8.0-K. Подробное описание настройки механизмов администрирования системы содержится в документе «Руководство по эксплуатации»¹.

Лицом, ответственным за управление системой защиты, считается администратор безопасности. Эту функцию могут выполнять и несколько сотрудников подразделения информационной безопасности предприятия.

Оператором системы защиты Dallas Lock 8.0-K является пользователь защищенного персонально компьютера, осуществляющий ввод и обработку информации любыми программными средствами.

¹ RU.48957919.501410-02 92

1.2. Условия работы

1.2.1. Данные учетной записи

Чтобы получить доступ к компьютеру, на который установлена система защиты Dallas Lock 8.0-K, необходимо иметь зарегистрированную в системе защиты учетную запись. Регистрация учетных записей осуществляется администратором безопасности.

Учетная запись пользователя, зарегистрированного в системе защиты Dallas Lock 8.0-K, 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 могут 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! Необходимо уточнить у администратора безопасности все авторизационные данные для входа на защищенный компьютер. Запомнить свое имя в системе защиты и пароль. Никому не сообщать пароль и никому не передавать персональный аппаратный идентификатор.

Авторизация пользователя осуществляется при каждом входе.

При вводе имени и пароля необходимо соблюдать следующие правила:

Для имени:

- ▶ максимальная длина имени – 20 символов;
- ▶ 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).

1.2.2. Права для работы под учетной записью

Так же 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. ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР

2.1. Вход в операционную систему

При загрузке компьютера, защищенного СЗИ НСД Dallas Lock 8.0-K, в зависимости от операционной системы, появляется экран приветствия (приглашение на вход в операционную систему) (Рис. 1).



Рис. 1. Экран приветствия в ОС Windows 7

Для входа на защищенный СЗИ НСД Dallas Lock 8.0-K компьютер каждому 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 соответствующий USB- или COM-порт, или прикоснувшись к считывателю.
2. Необходимо выбрать наименование идентификатора, которое появится в выпадающем меню в поле «аппаратные идентификаторы» (Рис. 2):

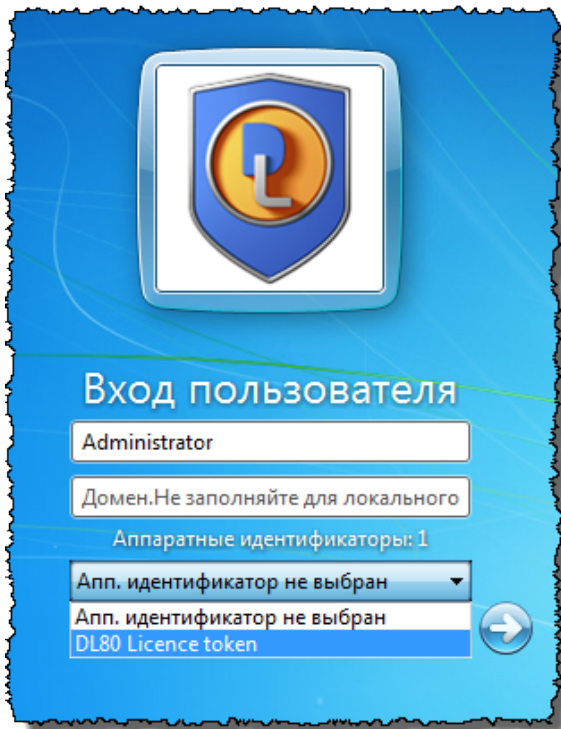


Рис. 2. Выбор аппаратного идентификатора при входе в ОС Windows

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

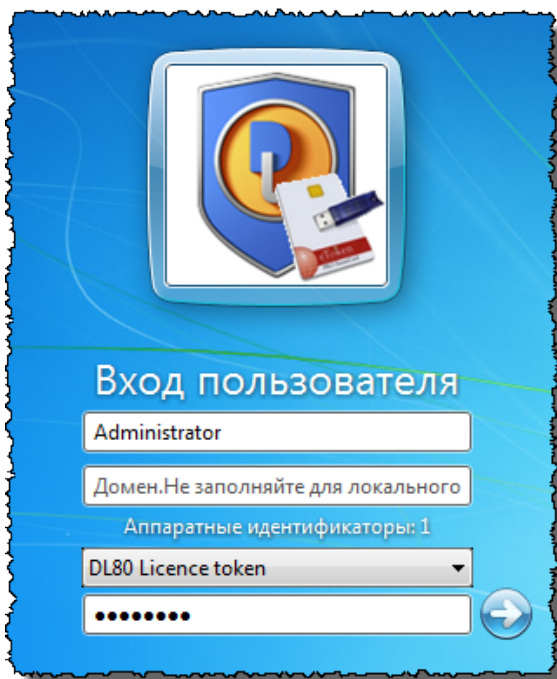


Рис. 3. Поля авторизации после предъявления идентификатора

- 3.2. Выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (Рис. 4):

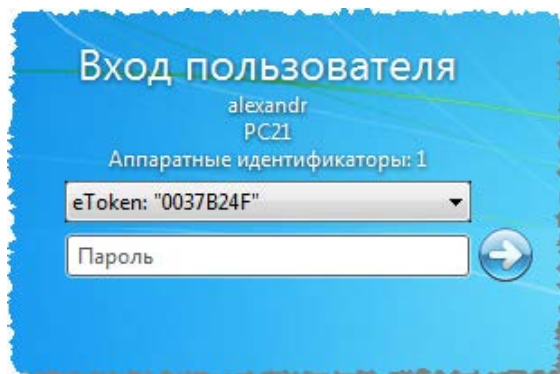


Рис. 4. Поля авторизации после предъявления идентификатора

- 3.3. Выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (Рис. 5):

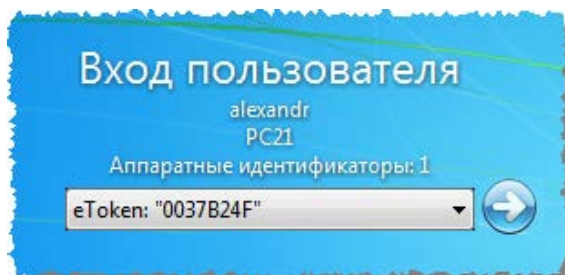


Рис. 5. Поля авторизации после предъявления идентификатора

- 3.4. Выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (Рис. 6):

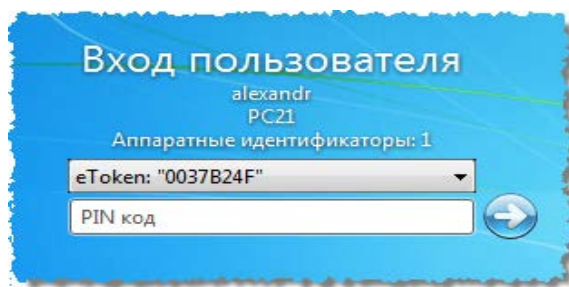


Рис. 6. Поля авторизации после предъявления идентификатора



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 получении аппаратного идентификатора 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 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 введенный пароль неверен, то на экране появится сообщение об ошибке, после чего система защиты предоставит возможность повторно ввести имя и пароль (Рис. 7).

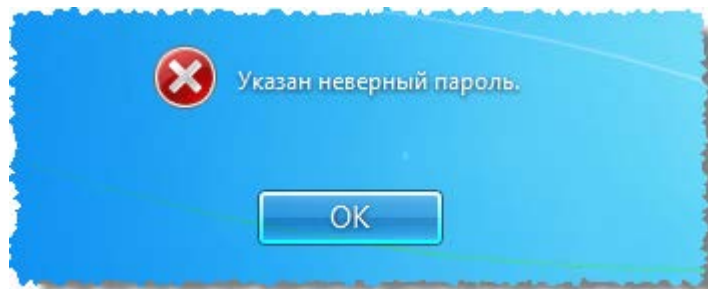


Рис. 7. Сообщение при вводе неправильного пароля

Подобное сообщение появится и при предъявлении неверного аппаратного идентификатора или, когда зарегистрированный за пользователем идентификатор не предъявлен вообще (Рис. 8).

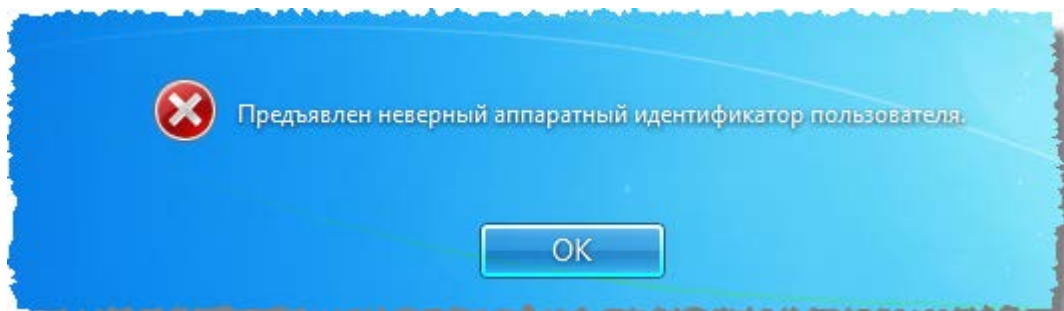


Рис. 8. Сообщение при неверном идентификаторе

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 (Рис. 9).

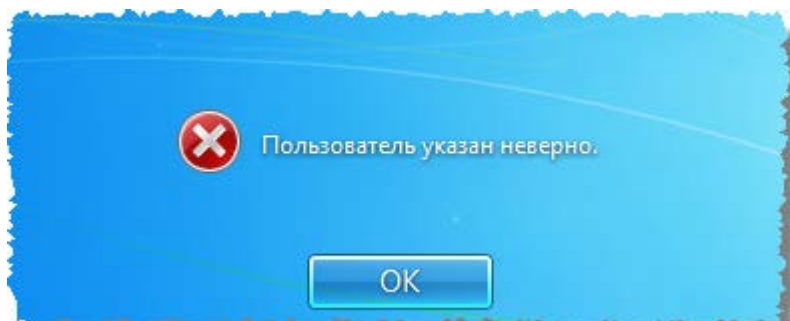


Рис. 9. Ошибка авторизации

Администратор может отключить учетную запись, тогда при авторизации, система защиты выведет соответствующее предупреждение (Рис. 10).

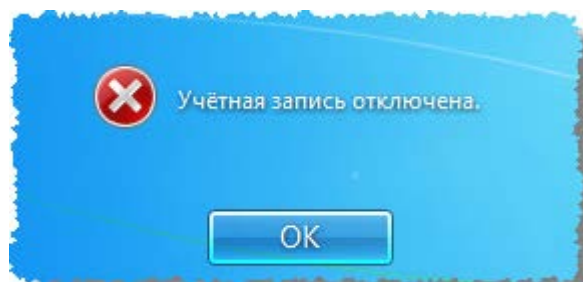


Рис. 10. Сообщение при отключенной учетной записи

В такой ситуации необходимо обратиться к администратору системы защиты.

При проблеме подключения по локальной сети или других может возникнуть ошибка авторизации доменных пользователей (Рис. 11).

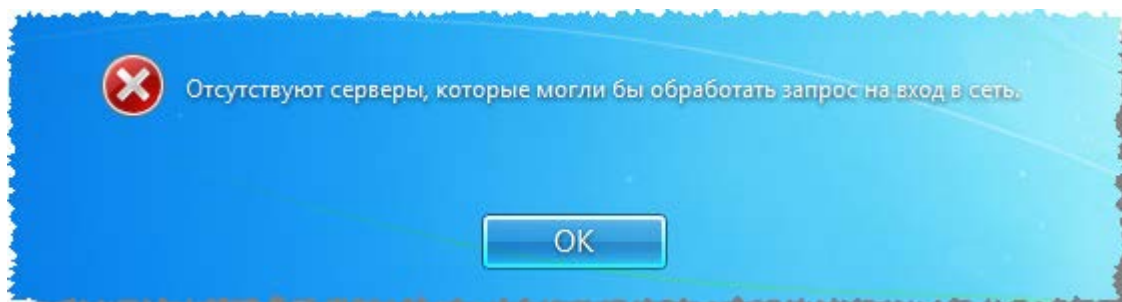


Рис. 11. Ошибка при вводе имени домена

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 и вход в операционную систему для пользователя будет запрещен (Рис. 12).

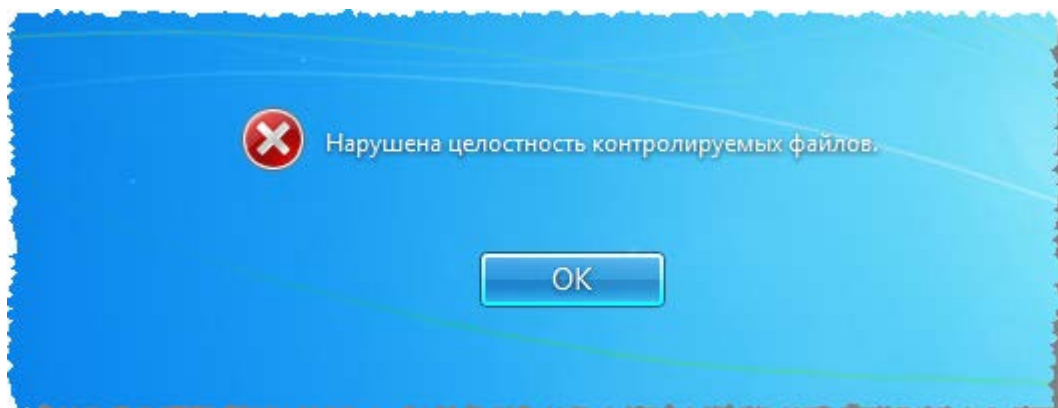


Рис. 12. Сообщение при входе

Также могут быть случаи, когда при нарушении целостности вход в ОС осуществляется, но на панели задач в области уведомлений появляется всплывающее предупреждение о нарушении целостности (Рис. 13).

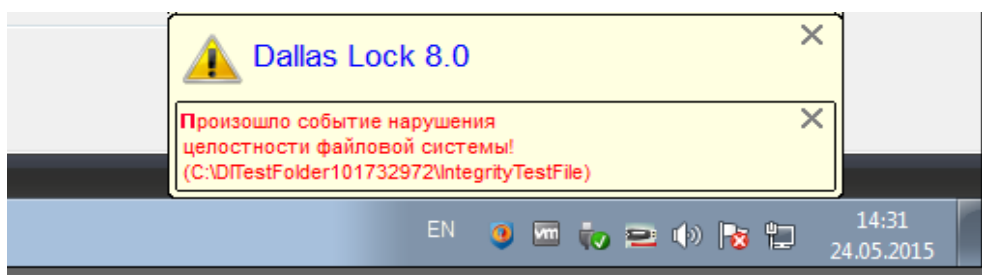


Рис. 13. Предупреждение о нарушенной целостности

В обоих случаях пользователю следует обратиться к администратору.

Администратором безопасности может быть задан особый механизм контроля доступа к информационным ресурсам, так называемый «мягкий» режим контроля доступа. При включенном «мягком» режиме проверяются все права доступа пользователем к ресурсам и программам, сообщения о запрете при попытке произвести запрещенную политиками безопасности операцию 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 так называемый «режим обучения» или «неактивный режим» (Рис. 14).

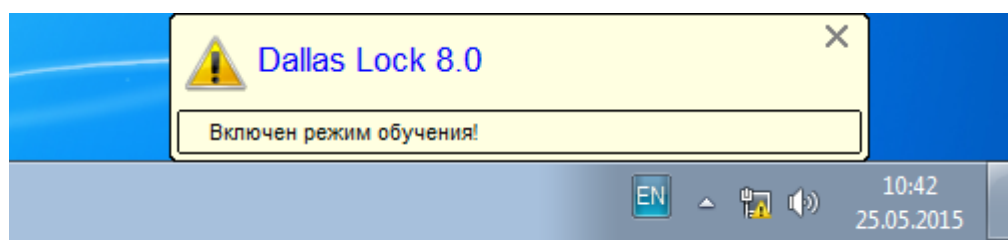


Рис. 14. Предупреждение о включенном режиме обучения

При появлении таких предупреждений работа на данном компьютере для пользователя осуществляется как обычно, ошибки никакой не происходит.




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

3. ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ

3.1. Завершение работы


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

1. Сохранить все данные и завершить работу всех приложений, так как выключение не сохраняет результатов работы.
2. В меню «Пуск»  в нижнем правом углу нажать кнопку «Завершение работы».
3. После нажатия кнопки «Завершение работы» компьютер закрывает все открытые программы, вместе с самой ОС Windows, а затем полностью выключает компьютер и монитор.

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. 15).

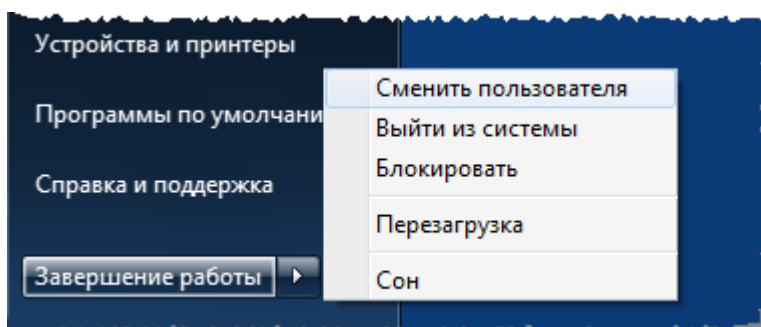

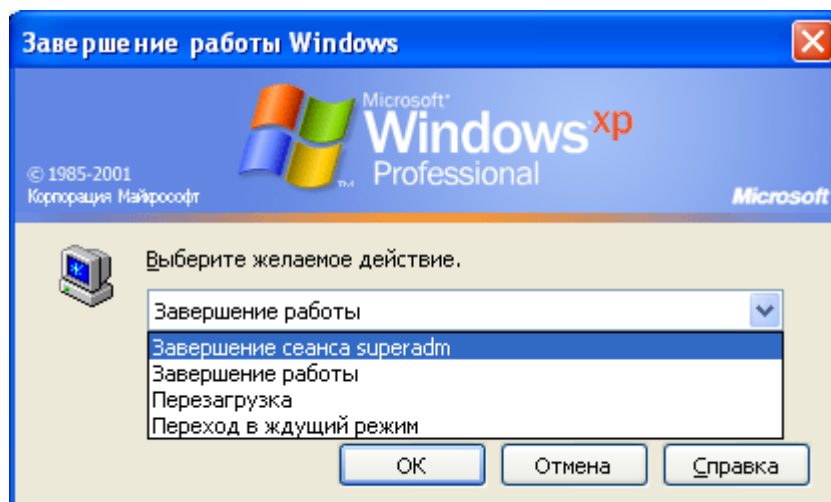


Рис. 15. Смена пользователя в ОС [Windows 7](#)

2. В ОС Windows XP в меню «Пуск»  в нижнем правом углу нажать кнопку «Завершение работы» и в появившемся окне выбрать пункт меню «Завершение сеанса ...» (Рис. 16).

Рис. 16. Смена пользователя в ОС Windows XP

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 предупреждение (Рис. 17).

Перед сменой пользователя рекомендуется сохранить все необходимые данные и закончить работу приложений, так как администратором безопасности в системе Dallas Lock 8.0-K 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. 17).

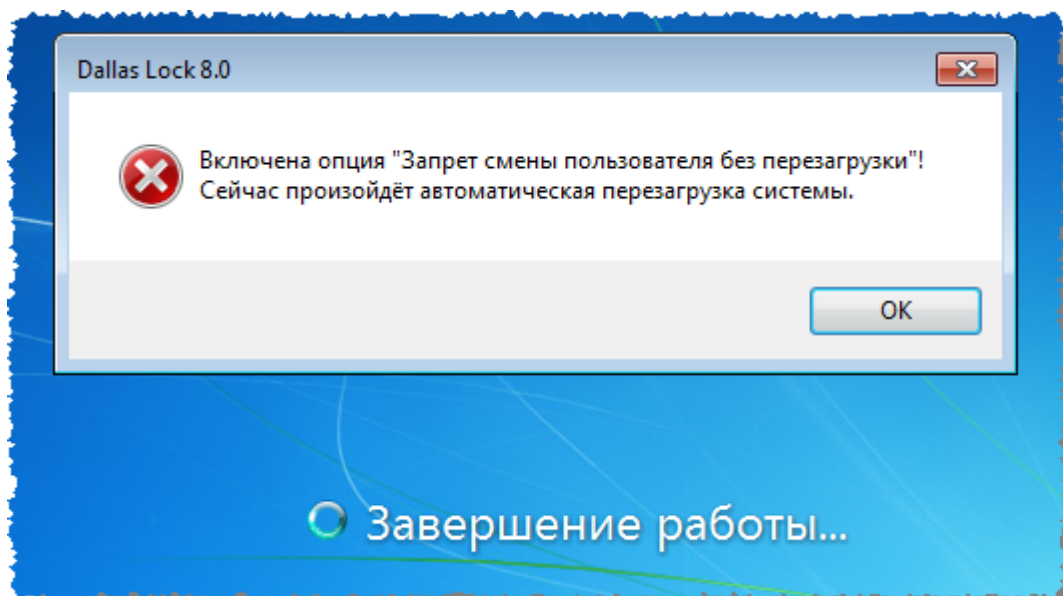


Рис. 17. Автоматическая перезагрузка при смене пользователя

Несохраненные другими пользователями результаты работы в этом случае не сохранятся.

4. СМЕНА ПАРОЛЯ

Пользователь может самостоятельно сменить свой пароль для авторизации.

1. Для этого, после входа в операционную систему, необходимо нажать комбинацию клавиш «Ctrl-Alt-Del» и выбрать операцию «Сменить пароль» (Рис. 18).

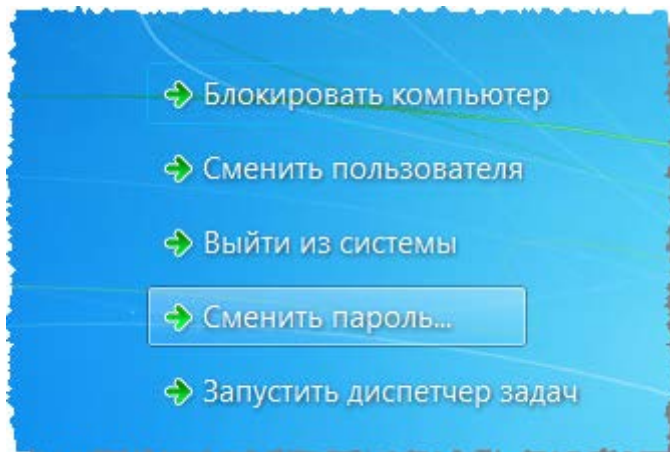


Рис. 18. Меню действий

На экране появится диалоговое окно, предлагающее ввести данные для смены пароля (Рис. 19).

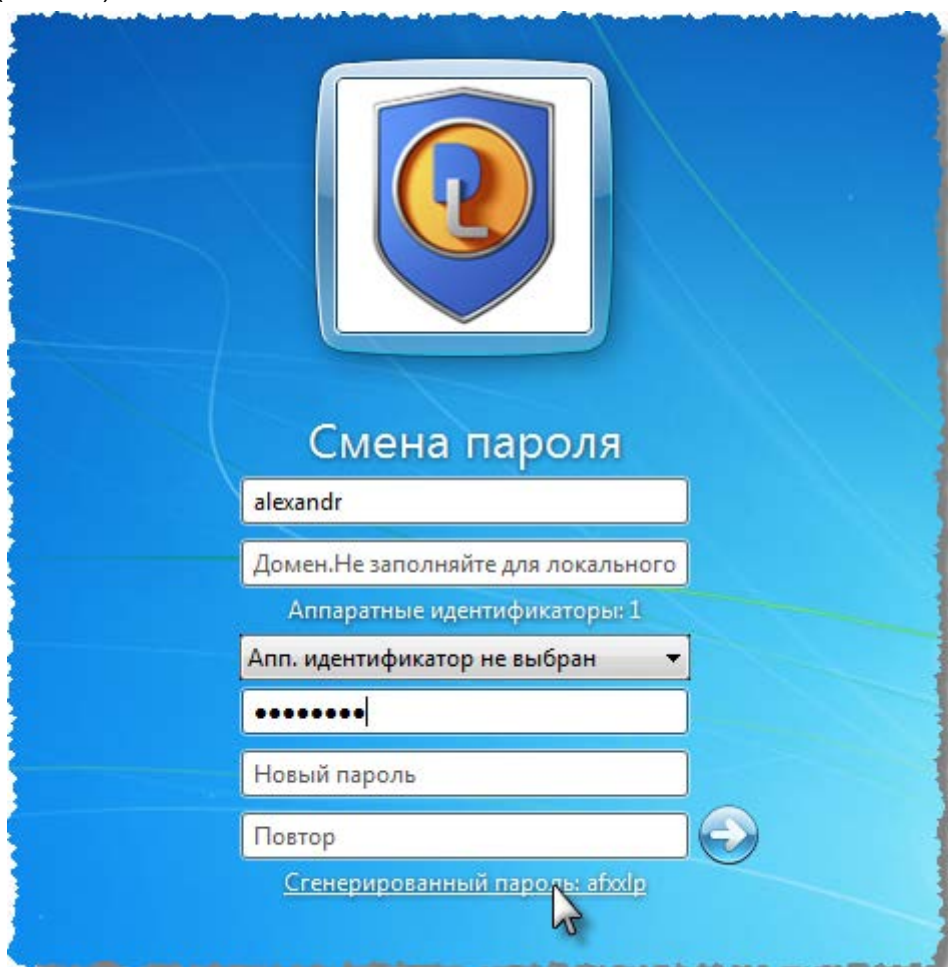


Рис. 19. Экран смены пароля

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 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;
- ▶ 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.

В соответствии с тем, какие из параметров включены, при смене пароля, на экране могут возникать сообщения об ошибках (Рис. 20- Рис. 24).

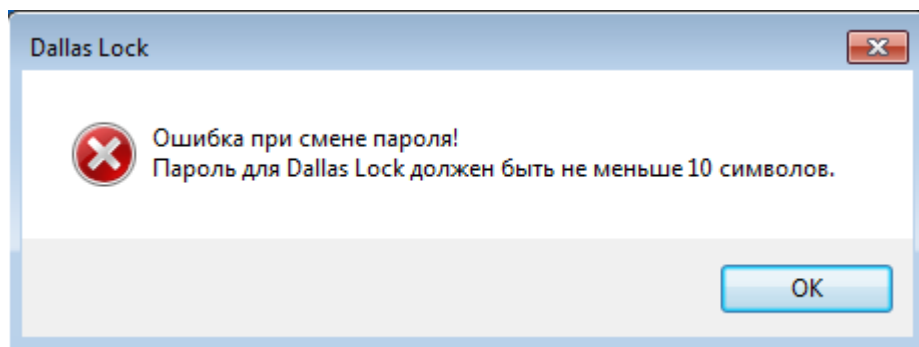


Рис. 20. Ошибка при смене пароля. Количество символов

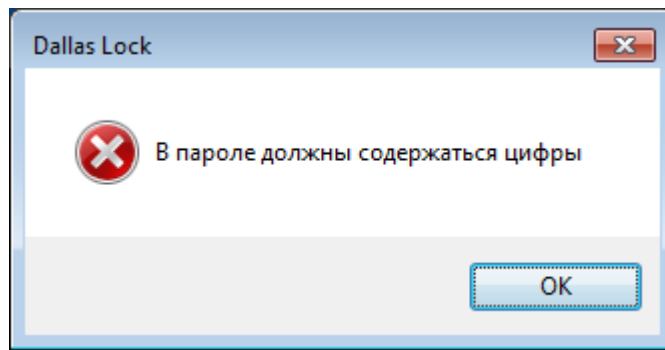


Рис. 21. Ошибка при смене пароля. Наличие цифр

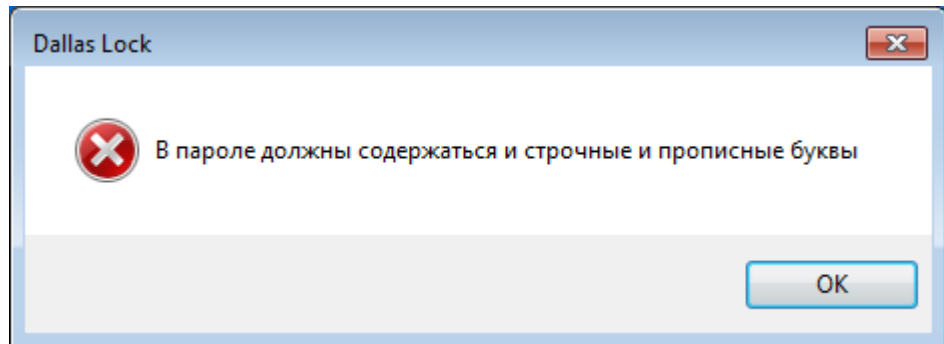


Рис. 22. Ошибка при смене пароля. Наличие заглавных букв

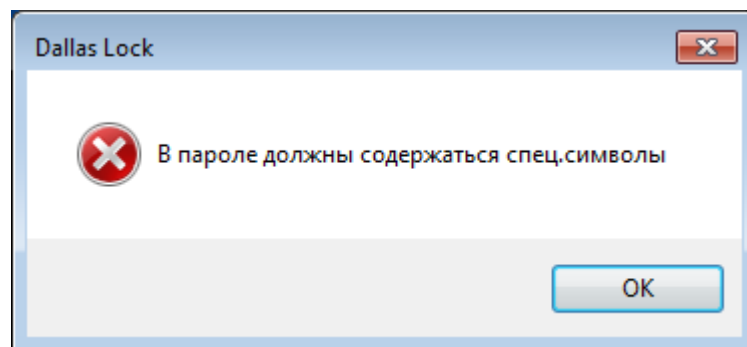


Рис. 23. Ошибка при смене пароля. Наличие спецсимволов

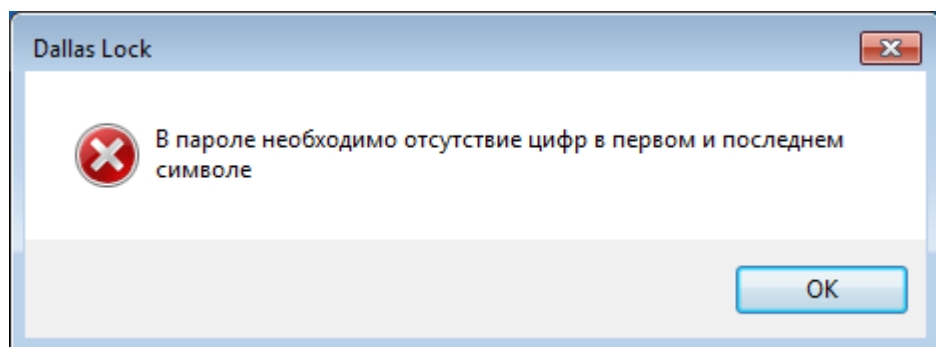


Рис. 24. Ошибка при смене пароля. Необходимость отсутствия цифр

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. 25).

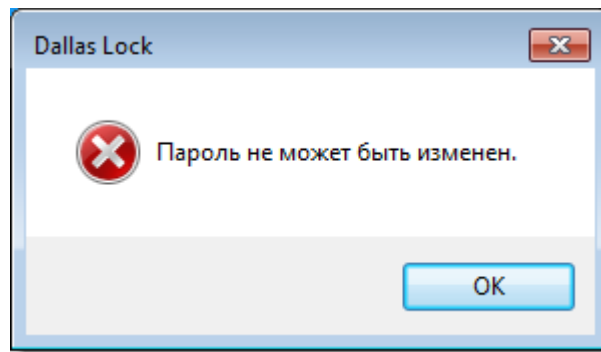


Рис. 25. Сообщение системы при смене пароля

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

Если все требования соблюдены, то пароль пользователя будет успешно сменен, и появится соответствующее сообщение (Рис. 26).

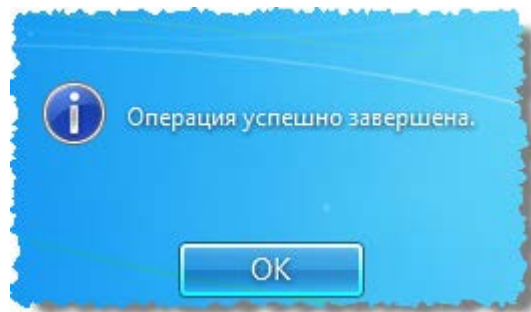


Рис. 26. Успешная смена пароля

Далее вход пользователя на защищенную СЗИ НСД Dallas Lock 8.0-K рабочую станцию будет осуществляться с новым паролем.

5. БЛОКИРОВКА КОМПЬЮТЕРА

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


1. Дважды кликнуть правой клавишей мыши на иконку  которая находится в нижнем правом углу экрана рядом с часами (Рис. 27).



Рис. 27. Иконка блокировки на панели задач

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



3. Нажать комбинацию клавиш «Ctrl+Alt+Del» и на появившемся экране выбрать кнопку «Блокировать компьютер» (Рис. 28).

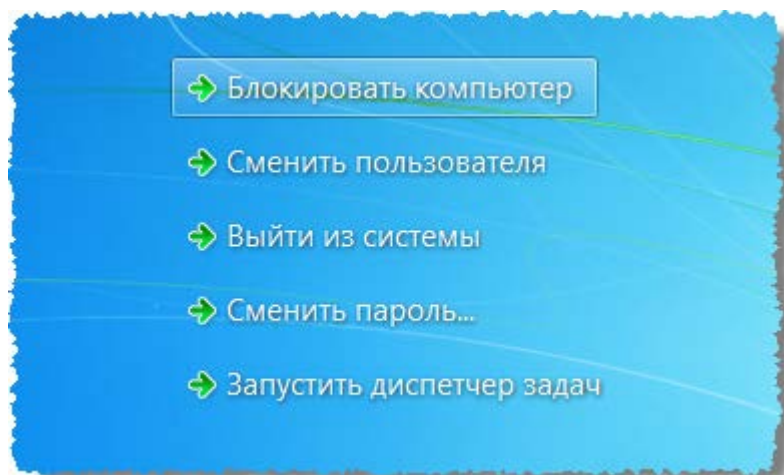


Рис. 28. Меню блокировки экрана

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 (Рис. 29).

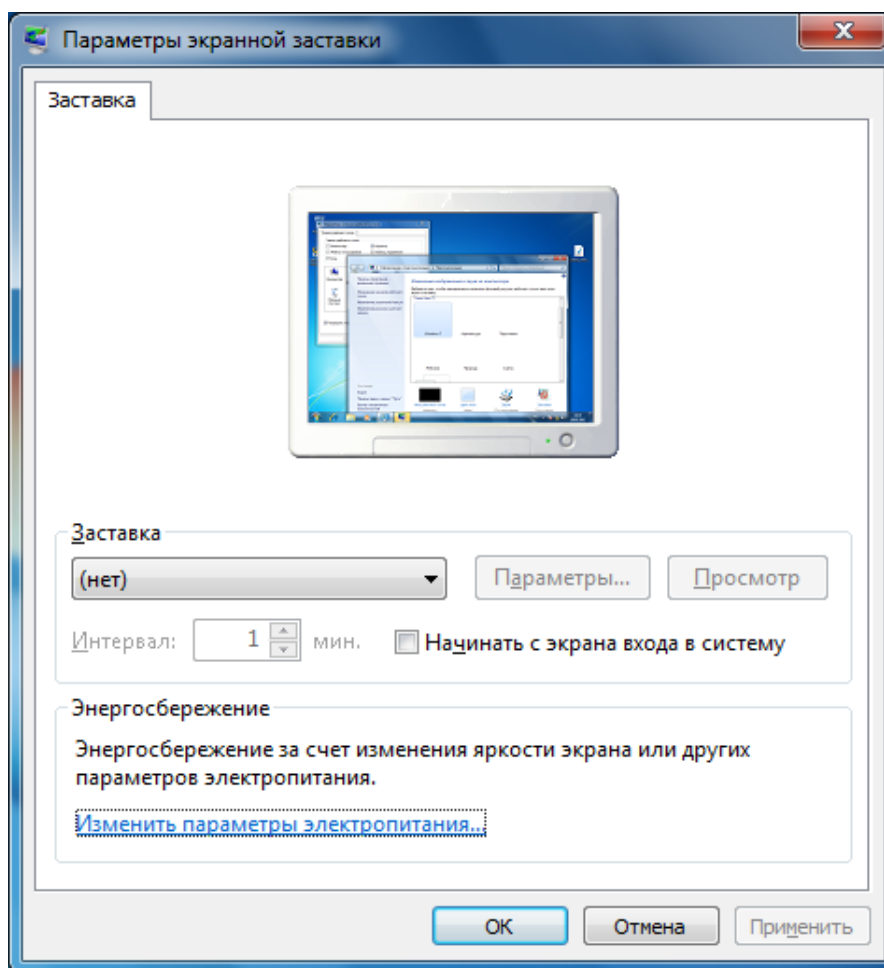


Рис. 29. Параметры автоматической блокировки экрана

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. 30).

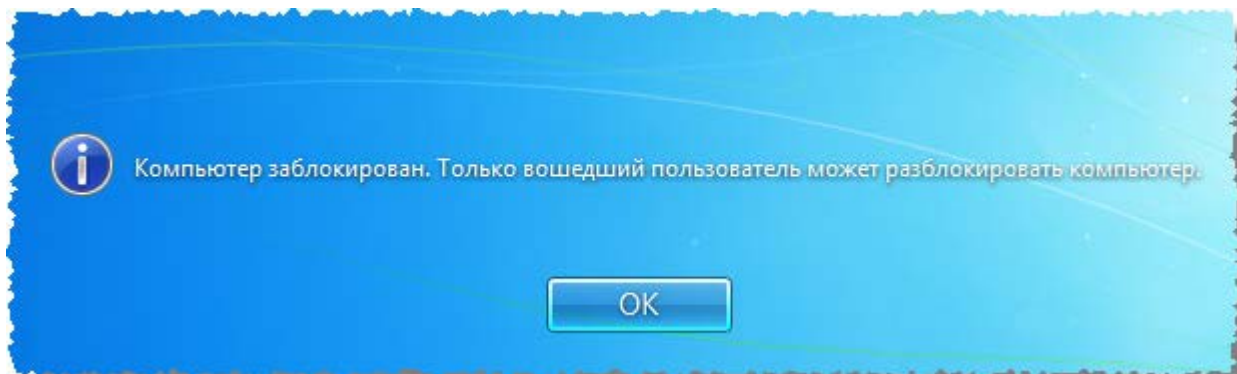


Рис. 30. Сообщение ОС при попытке входа на заблокированный компьютер

6. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Система защиты Dallas Lock 8.0-K 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 НСД Dallas Lock 8.0-K реализована функция очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

При необходимости удалить пользователю какие-либо данные без возможности их восстановления нужно выполнить следующие действия.

1. В контекстном меню объекта файловой системы, который необходимо удалить, выбрать пункт «DL8.0: Удалить и зачистить» (Рис. 31).

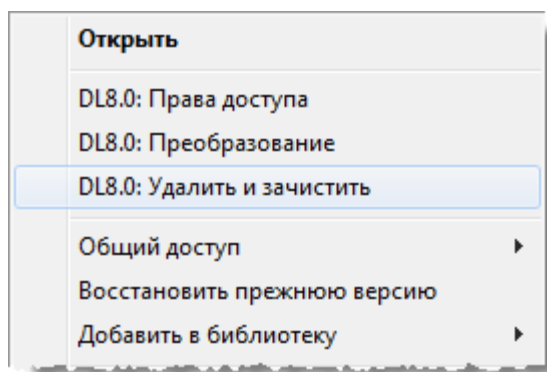


Рис. 31. Контекстное меню

2. Нажать «Да» в появившемся окне подтверждения операции (Рис. 32).

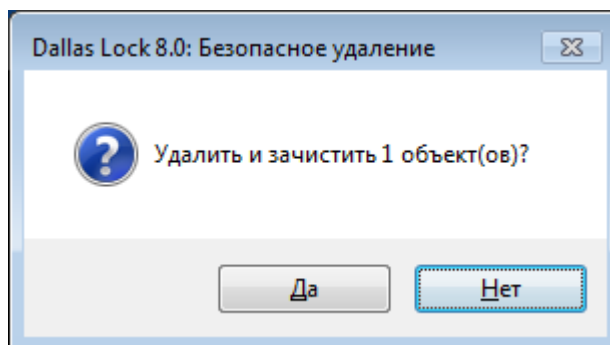


Рис. 32. Окно подтверждения операции

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. 33).

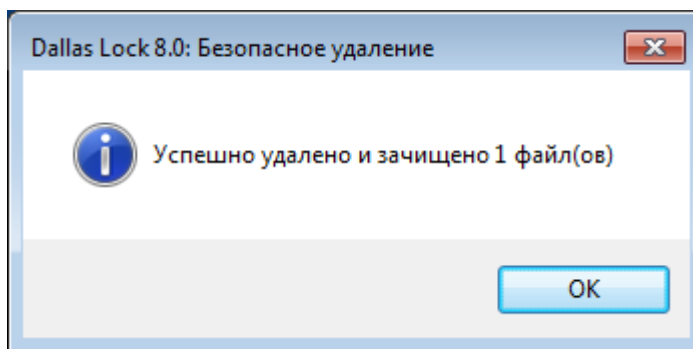


Рис. 33. Сообщение об удалении файлов



Примечание. При нескольких одновременно выделенных объектах, происходит их одновременное удаление и зачистка, как группы. 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 зачистить и удалить файл появится предупреждающее сообщение (Рис. 34).

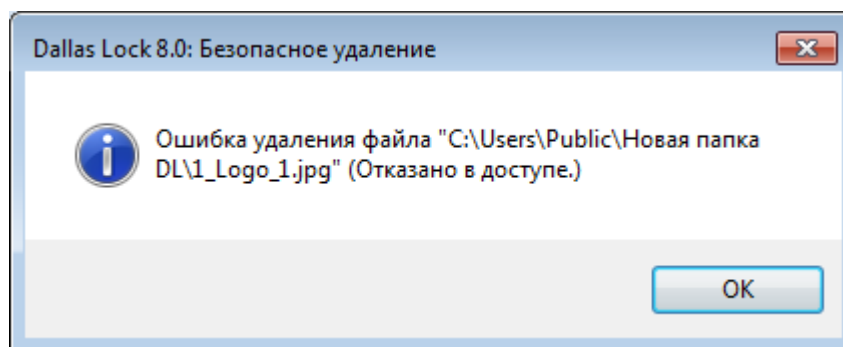


Рис. 34. Сообщение на запрет удаления файла

6.2. Преобразование информации

Для дополнительной защиты важных данных в системе защиты Dallas Lock 8.0-K имеется возможность преобразования этих данных или в процессе работы с ними или путем преобразования уже имеющегося объекта данных: файла или папки.

6.2.1. Преобразование данных в файл-контейнер

Имеющиеся на защищенном ПК файлы или папки могут быть преобразованы в файл-контейнер с помощью системы защиты с использованием ключевой информации (пароля и (или) аппаратного идентификатора). Преобразованные файлы или папки могут быть обратно преобразованы в исходные данные, при условии верного ввода ключевой информации.

Содержание данных, преобразованных в файл-контейнер, становится недоступным на ПК, не защищенном СЗИ НСД Dallas Lock 8.0-K, и также недоступным на ПК, защищенном СЗИ НСД Dallas Lock 8.0-K, в случае введения неверной ключевой информации.

Перед преобразованием необходимо уточнить у администратора безопасности о возможности использования аппаратного идентификатора.

1. Для того чтобы преобразовать объект файловой системы (файл или папку), необходимо в контекстном меню соответствующего файла или папки выбрать пункт «DL8.0: Преобразование» (Рис. 35).

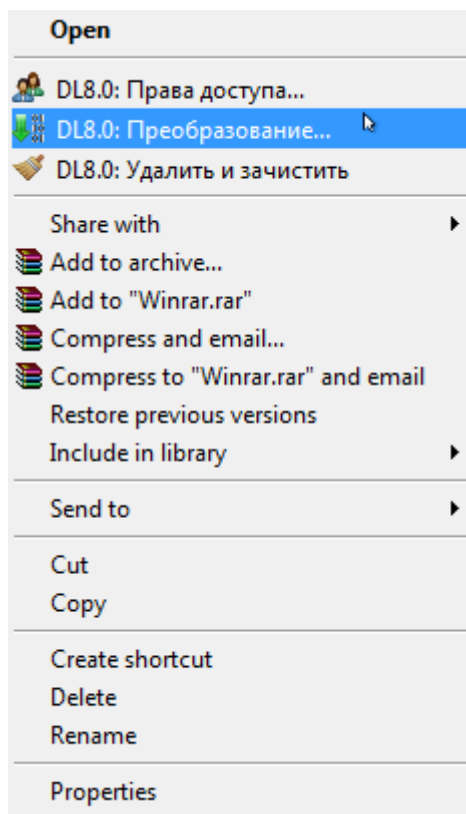


Рис. 35. Контекстное меню

2. На экране появится окно, в котором необходимо заполнить параметры преобразования (Рис. 36).

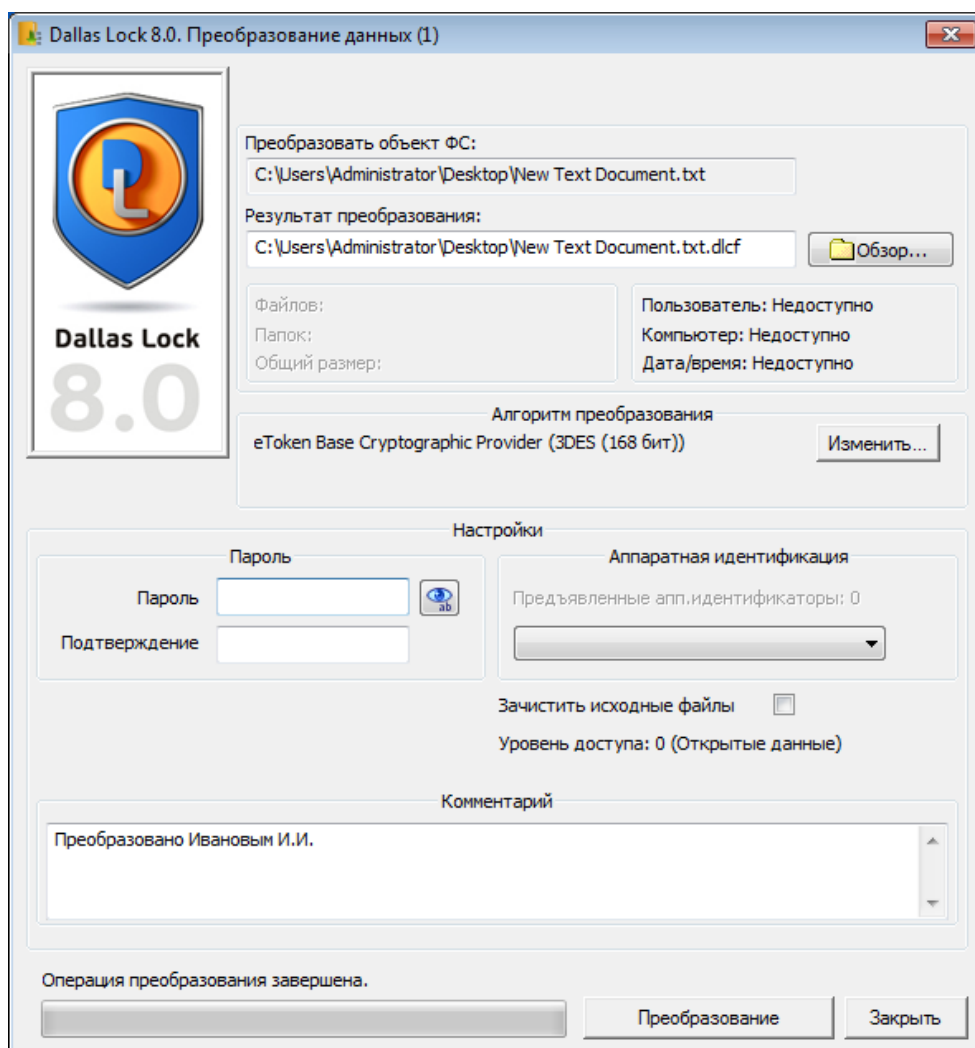


Рис. 36. Окно преобразования данных

Окно модуля преобразования объекта ФС содержит следующие поля для заполнения:

Наименование поля	Описание
Результат преобразования	Имя и путь к будущему файлу-контейнеру (по умолчанию, оно формируется из имени преобразовываемого объекта с добавлением специального расширения, в текущей папке). Имя будущего файла и путь к нему можно прописать вручную. Выбор другой папки возможен с помощью кнопки «Обзор...»
Алгоритм преобразования	Операции по настройке алгоритма преобразования. По умолчанию используется встроенный в Dallas Lock 8.0 алгоритм ГОСТ 28147-89
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей. Дополнительно можно воспользоваться генерацией пароля, соответствующего установленным параметрам и кнопкой, меняющей скрытые символы на явные

Наименование поля	Описание
Аппаратная идентификация	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка. Если аппаратный идентификатор не указывать, преобразование происходит только по паролю
Уровень доступа	Поле является информационным
Зачистить исходные файлы	Выбор операции по зачистке исходных данных после получения преобразованного файла-контейнера
Комментарий	Комментарий к файлу-контейнеру (он не преобразуется, является необязательным и доступен без пароля)

3. После заполнения всех необходимых параметров необходимо нажать «Преобразование».

Для назначения аппаратного идентификатора необходимо (в зависимости от типа устройства) вставить его в USB-порт или прикоснуться к считывателю и нажать кнопку «Назначить». В поле идентификатора появится его значок и серийный номер.

Процесс преобразования будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса будут выведены следующие сообщения: «Исходный файл удален!» (если операция по зачистке исходных файлов была включена) и сообщение об успешном преобразовании.

Файл–контейнер с расширением *.dlcf появится в указанной папке (Рис. 37).

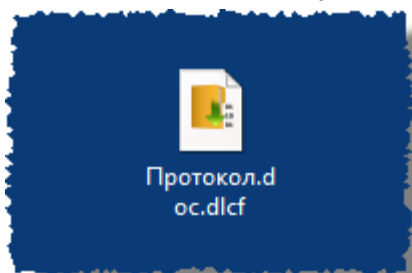


Рис. 37. Значок преобразованного файла-контейнера


Возможно одновременное преобразование сразу нескольких файлов. Для этого их нужно одновременно выделить (с помощью Ctrl) и, щелкнув правой кнопкой мыши, выбрать в контекстном меню пункт «DL8.0: Преобразование». Будущий файл-контейнер будет содержать все выбранные файлы. При этом имя и путь к будущему файлу-контейнеру будет по умолчанию состоять из имени первого из нескольких выбранных файлов. Преобразование завершится сообщениями системы с указанием количества файлов.



Примечание. При преобразовании и последующем обратном преобразовании папки, содержащей не только файлы, но и вложенные папки происходит следующее: если исходная папка содержит пустую подпапку (без файлов), то при преобразовании она удаляется. Соответственно и обратно – преобразованная структура вложенных папок будет отличаться от исходной.

6.2.1.1. Обратное преобразование файла-контейнера

В окне модуля преобразования объекта всегда присутствует кнопка, которая может переключить окно в режим обратного преобразования.

Выбрать и открыть файл-контейнер в данном окне можно с помощью кнопки проводника , или дважды кликнув по значку преобразованного объекта.

Появится окно подобное тому, что и при преобразовании, в котором нужно ввести ключевые параметры восстановления: папку для восстановления, пароль, и выбрать предъявленный аппаратный идентификатор.

Отмеченное флажком поле «Зачистить исходные файлы» активирует операцию по удалению исходного файла-контейнера.

В этом же окне будет выведен комментарий к файлу-контейнеру, общее количество файлов и папок, содержащихся в нем, их общий размер и криптопровайдер, который определила система защиты.

После ввода параметров восстановления и нажатия кнопки «Обратное преобразование» будет произведено восстановление информации. По окончании появится сообщение о подтверждении удаления исходного файла-контейнера и сообщение об удачном завершении процесса (Рис. 38).

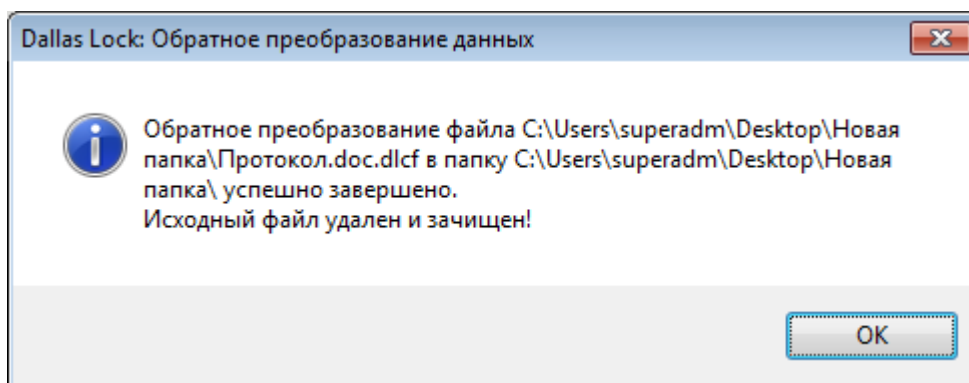


Рис. 38. Подтверждение успешного обратного преобразования файла


6.2.2. Преобразованные файл-диски

Для безопасности хранения и обработки информации в Dallas Lock 8.0 реализован механизм создания таких контейнеров информации, при работе с размещенными на которых объектами ФС параллельно работе и не заметно для пользователя выполняется преобразование информации. Данные контейнеры называются преобразованные файл-диски.

Особенностью данного механизма является то, что данные файл-диски могут подключаться (монтироваться и демонтироваться) в ОС Windows как логические диски и иметь свою букву диска и определенный объем. В то же время информация на таком диске будет преобразованной и подключение диска для работы с ним пользователем может быть произведено только на ПК, защищенном Dallas Lock 8.0, и только с указанием ключевой информации.

6.2.2.1. Работа на преобразованном файл-диске

Для работы с преобразованным файл-диском необходимо подключить такой диск в операционной системе и зайти на логический диск, появившийся в проводнике Windows.

Для подключения файл-диска необходимо выбрать пункт «Преобразованные файл-диски» в меню значка блокировки ПК на панели задач . Или дважды кликнуть кнопкой мыши на значке самого файл-диска (Рис. 39). Включение также доступно из контекстного меню значка самого файл-диска.

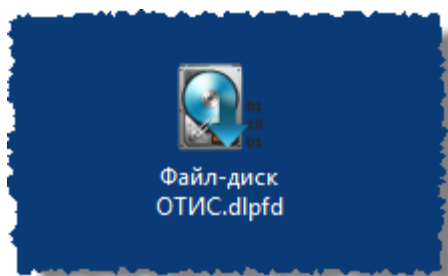


Рис. 39. Значок созданного преобразованного файл-диска

В появившемся окне при подключении файл-диска необходимо заполнить ключевую информацию:

- Выбрать путь к файл-диску.
- Указать букву, под которой он будет монтирован как логический диск в ОС.
- Предъявить аппаратный идентификатор, если он был назначен.
- Ввести пароль.

После нажатия кнопки «Подключить», если введенные данные были корректны, файл-диск подключится и отобразится в проводнике как логический диск с присвоенной ему буквой диска.

Пользователь может работать с таким диском в штатном режиме, но в то же время вся информация на нем является преобразованной, преобразование же выполняется по установленному алгоритму в процессе самой работы. Пользователь может размещать, создавать, изменять файлы на преобразованном файл-диске, копировать их с него. Для пользователя подключенный файл-диск в своей работе ничем не отличается от любого другого диска.

В меню «Преобразованные файл-диски» значка блокировки на панели задач также имеется пункт, позволяющий подключить последние использованные файл-диски – в выпадающем списке отображается список из 10 последних файл-дисков.

Чтобы отключить конкретный преобразованный файл-диск или все подключенные на данном ПК необходимо выбрать соответствующие пункты в меню «Преобразованные файл-диски». Отключение также происходит после выключения или перезагрузки ПК.

6.2.2.2. Создание преобразованного файл-диска

Если пользователь наделен полномочием, то он может создавать преобразованные файл-диски при работе на защищенном ПК.

Для того чтобы создать преобразованный файл-диск, необходимо в меню значка блокировки ПК на панели задач выбрать пункт меню «Создать преобразованный файл-диск» (Рис. 40).

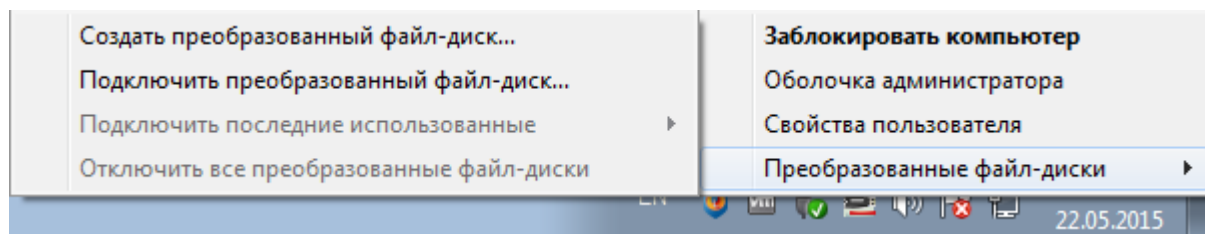


Рис. 40. Выбор пункта меню для создания преобразованного файл-диска

На экране появится окно свойств создаваемого файл-диска (Рис. 41).

Создание нового преобразованного файл-диска

Файл-диск(*.dlpfd): C:\Users\superadm\Desktop\SecDisk.dlpfd Обзор...

Описание: Преобразованный ФД Иванова П.

Размер файл-диска: 400 МБ ☒ Подключить после создания

Буква диска: Y: ▼

Алгоритм преобразования: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
GOST 28147-89(256 бит)
GOST R 34.11-94(256 бит) Изменить

Предъявленные апп.идентификаторы: 1

Апп. идентификатор: Апп. идентификатор не выбран ▼

Генерация пароля

Пароль: ••••• ab

Подтверждение:

Создать Отмена

Рис. 41. Окно параметров при создании преобразованного файл-контейнера

В данном окне необходимо указать следующие параметры преобразования:

Наименование поля	Описание
Файл-диск	Путь, по которому будет сохранен создаваемый файл-диск и его имя
Название	Описание для создаваемого файл-диска (не обязательное поле)
Размер файл-диска	Необходимо указать оптимальный объем создаваемого файл-диска в МБ (учитывая наличие необходимого места на физическом диске ПК)
Буква диска	Необходимо определить букву логического диска для монтирования в ОС (букву диска можно выбрать и во время подключения файл-диска)
Подключить после создания	Отмеченное поле позволяет автоматически монтировать данный созданный файл-диск в качестве логического диска в ОС и осуществлять на нем работу текущему пользователю
Алгоритм преобразования	Операции по выбору и настройке алгоритма преобразования, которым будет преобразовываться информация при работе в данном файл-диске. По умолчанию используется встроенный в Dallas Lock 8.0 алгоритм преобразования ГОСТ 28147-89, но можно использовать внешний алгоритм преобразования, для этого необходимо нажать «Изменить» и выбрать настройки

Наименование поля	Описание
Аппаратный идентификатор	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка (также необходимо предварительно зарегистрировать в СЗИ НСД считыватели). Если аппаратный идентификатор не указывать, то преобразование будет происходить только по паролю
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей (см. раздел «Настройка параметров входа»). Дополнительно можно воспользоваться генерацией пароля, соответствующего установленным параметрам и кнопкой, меняющей скрытые символы на явные

После заполнения всех необходимых параметров необходимо нажать «Создать».

После успешного создания пользователю будет выведено сообщение о том, что создан преобразованный файл-диск и, если было отмечено подключение, подключен как логический диск с указанной буквой диска.

Созданный таким образом файл будет иметь расширение *.dlpfd и иметь определённый значок

6.2.3. Использование внешних криптопровайдеров

Преобразование данных на различных носителях информации и в различных формах осуществляется встроенными алгоритмами преобразования: ГОСТ 28147-89 и XOR32.

Дополнительно доступно использование внешних криптопровайдеров.

Следует учесть, что наличие установленного на ПК криптопровайдера необходимо не только для преобразования, но также является обязательным условием для работы с объектом, преобразованным криптопровайдером.

В случае удаления (деинсталляции) криптопровайдера, с помощью которого было выполнено преобразование, или при переносе преобразованного объекта на защищенный ПК, не содержащий необходимый криптопровайдер, работа с преобразованным объектом будет невозможна.

Криптопровайдеры устанавливаются на ОС в соответствии со своими инструкциями по установке. Установленные криптопровайдеры появляются в списке доступных в окне настройки преобразования.

Для использования внешнего криптопровайдера необходимо выбрать поле «Алгоритм преобразования» и выбрать использование внешнего криптопровайдера.

В появившемся окне нужно выбрать криптопровайдер и задать все необходимые настройки (Рис. 42).

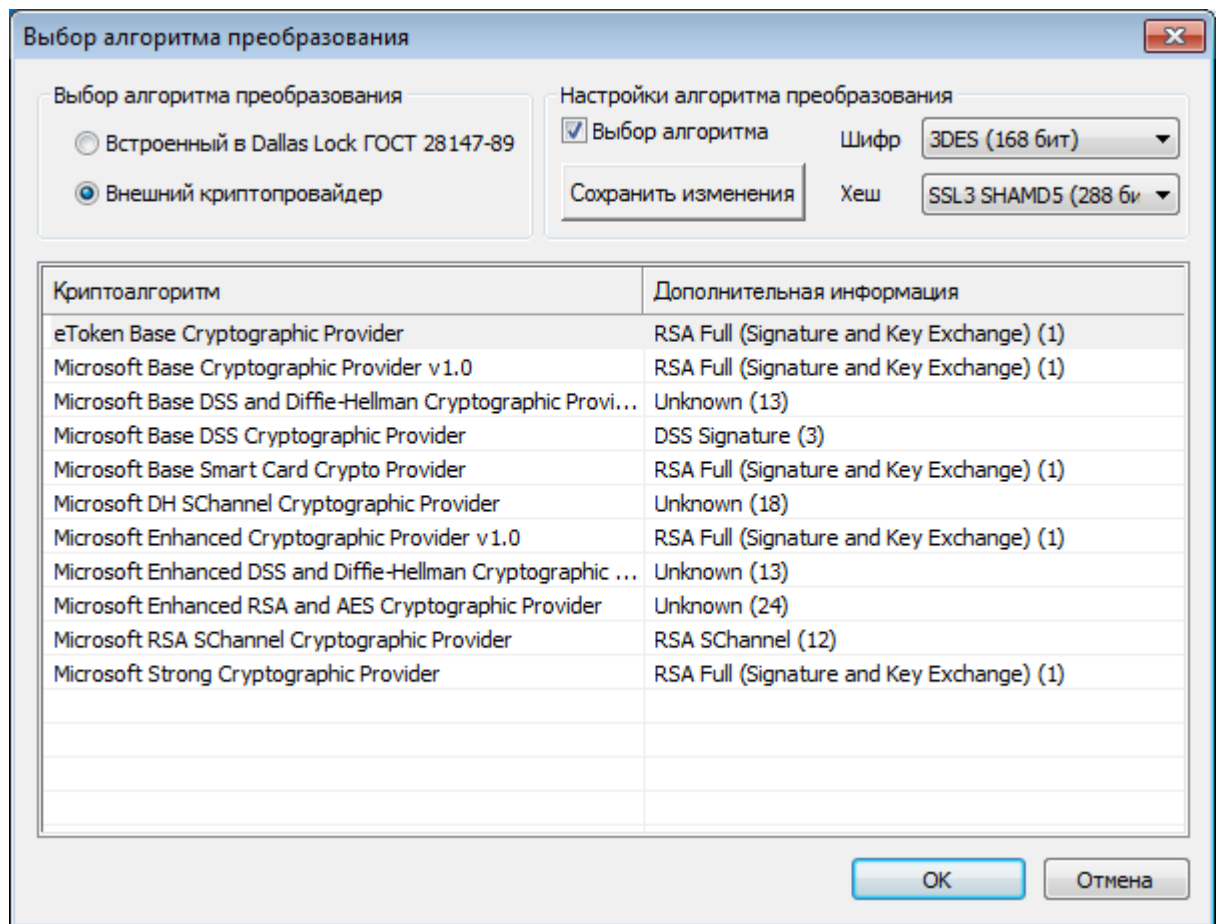


Рис. 42. Настройка криптопровайдера при создании файла-контейнера

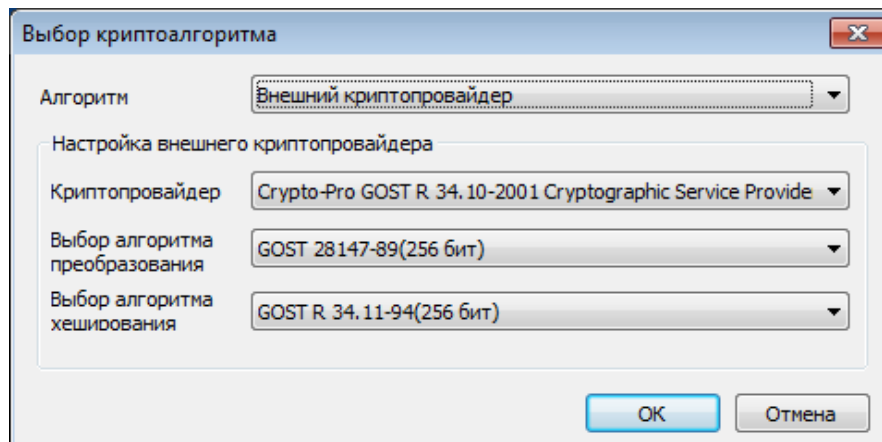


Рис. 43. Настройка криптопровайдера при создании файл-диска

При создании преобразованных файлов-контейнеров параметры последнего использованного криптопровайдера будут сохраняться в реестре для каждого пользователя и все последующие контейнеры данного пользователя, по умолчанию, будут создаваться с использованием указанного криптопровайдера.

При запуске преобразованных объектов можно увидеть название криптопровайдера, который был использован для создания, даже если данный криптопровайдер не установлен на используемом ПК.

Термины и определения

Некоторые термины, содержащиеся в тексте руководства, уникальны для системы защиты Dallas Lock 8.0-K, другие используются для удобства, третьи выбраны из соображений краткости.

Термины «компьютер» и «ПК» считаются эквивалентными, и используются в тексте руководства.

Термин	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
Криптопровайдер	Модуль, позволяющий осуществлять криптографические операции в операционных системах
Мышь	Ручной манипулятор, преобразующий механические движения в движение курсора на экране
ОС	Операционная система
СЗИ НСД	Система защиты информации от несанкционированного доступа
ПК	Персональный компьютер

Изменения

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

[illegible]