

УТВЕРЖДЕН
RU.48957919.26.20.40.142.001 34-ЛУ
(взамен RU.48957919.501410-01 34-ЛУ)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock 8.0

(версия 12.10.4.877)



Руководство оператора (пользователя)

RU.48957919.26.20.40.142.001 34
(взамен RU.48957919.501410-01 34)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ	4
1.1 НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ	4
1.2 УСЛОВИЯ РАБОТЫ	4
1.2.1 Параметры (настройки) безопасности средства, доступные пользователю.....	4
1.2.2 Данные учетной записи	5
1.2.3 Перечень ролей пользователей	6
1.2.4 Данные учетной записи	7
1.2.5 Режимы работы пользователя в системе	7
2 ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР	9
2.1 ВХОД В ОПЕРАЦИОННУЮ СИСТЕМУ	9
2.1.1 Вход с использованием смарт-карт с сертификатом УЦ Windows	10
2.1.2 Вход с аппаратным идентификатором	10
2.1.3 Вход с PayControl.....	13
2.2 ОШИБКИ, ВОЗНИКАЮЩИЕ ПРИ ВХОДЕ	16
3 ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ	19
3.1 ЗАВЕРШЕНИЕ РАБОТЫ.....	19
3.2 СМЕНА ПОЛЬЗОВАТЕЛЯ.....	19
4 СМЕНА ПАРОЛЯ	20
5 БЛОКИРОВКА КОМПЬЮТЕРА	23
6 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	25
6.1 МЕХАНИЗМ ОЧИСТКИ ОСТАТОЧНОЙ ИНФОРМАЦИИ	25
6.2 ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ	26
6.2.1 Преобразование данных в файл-контейнер.....	26
6.2.2 Обратное преобразование файла-контейнера	28
6.3 ПРЕОБРАЗОВАННЫЕ ФАЙЛ-ДИСКИ.....	29
6.3.1 Работа с преобразованным файл-дискон.....	29
6.3.2 Создание преобразованного файл-диска.....	29
6.4 ПРЕОБРАЗОВАННЫЕ СЪЕМНЫЕ НАКОПИТЕЛИ	31
6.4.1 Работа с преобразованным съемным накопителем	31
7 ИНТЕРФЕЙСЫ, ДОСТУПНЫЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ	34
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	36

ВВЕДЕНИЕ

Данное руководство предназначено для пользователей рабочих станций, на которых установлена Система защиты информации «Dallas Lock 8.0» (далее по тексту — система защиты, **СЗИ** или **Dallas Lock 8.0**).

В руководстве содержатся сведения, необходимые пользователю для работы на защищенном **Dallas Lock 8.0** компьютере и с компонентами установленной системы защиты.

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

В руководстве представлены элементы графических интерфейсов системы защиты **Dallas Lock 8.0** и операционной системы (далее по тексту — ОС), которые соответствуют работе **Dallas Lock 8.0** в ОС Windows 7, Windows 10 и Windows 11.

1 ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ

1.1 Назначение системы защиты

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

СЗИ Dallas Lock 8.0 предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации.

СЗИ Dallas Lock 8.0 предназначена для использования на персональных компьютерах (далее по тексту — ПК), 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**. Подробное описание настройки механизмов администрирования системы содержится в документе «Руководство по эксплуатации».

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** является пользователь защищенного персонального компьютера, осуществляющий ввод и обработку информации любыми программными средствами.

К основным принципам безопасности работы **Dallas Lock 8.0** относятся:

- 1) Выполнение ограничений по эксплуатации **Dallas Lock 8.0** перечисленных в п.3.3 документа RU.48957919.26.20.40.142.001 30 Формуляр.
- 2) Осуществление работы **Dallas Lock 8.0** строго в соответствии с эксплуатационной документацией.

1.2 Условия работы

1.2.1 Параметры (настройки) безопасности средства, доступные пользователю

Доступ к управлению системой защиты и права для работы аудитора и пользователя в **Dallas Lock 8.0** назначаются администратором безопасности. Для предоставления аудитору и пользователю разрешенных полномочий администратору безопасности необходимо в оболочке администратора на вкладке основного меню **Параметры безопасности** открыть категорию *Права пользователей* (рис. 1).

Безопасность значений доступных параметров интерфейсов для всех ролей пользователя обусловлены множеством детерминированных значений для каждого параметра, покрывающем все возможные значения, а также валидностью данного множества в контексте безопасности.

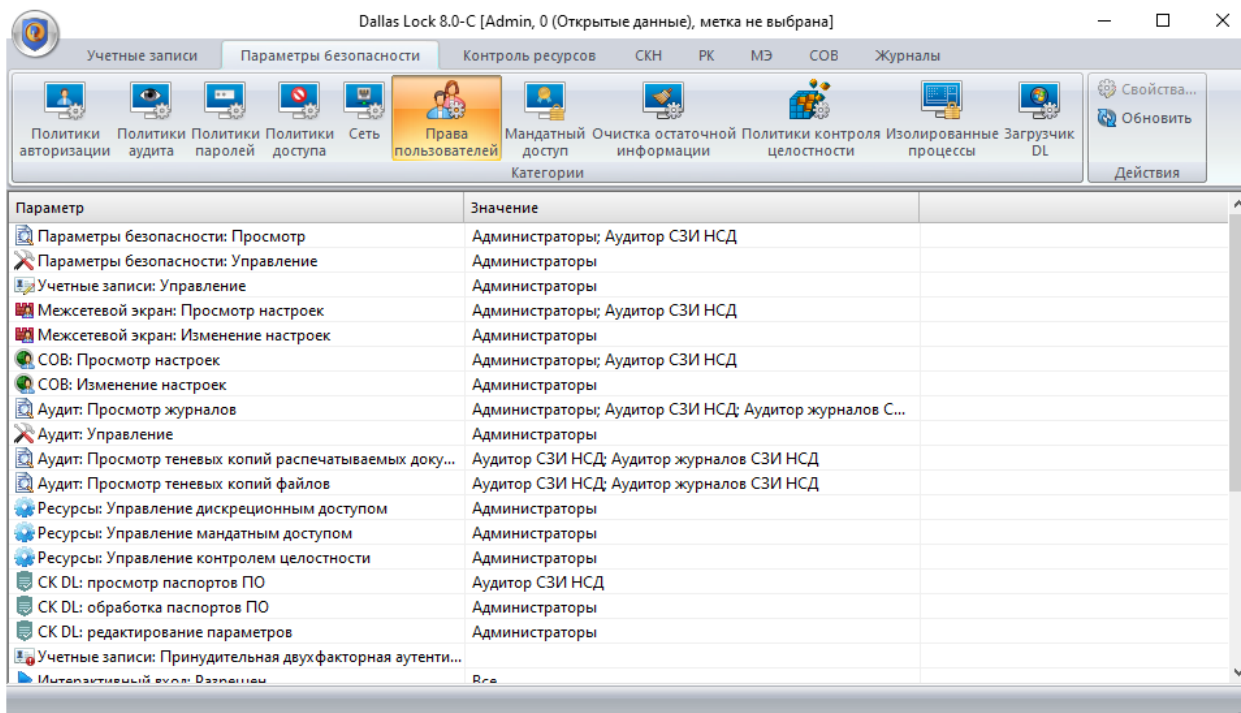


Рис. 1. Параметры пользователей

Параметры безопасности доступны пользователю:

- вход в систему и смена пароля в соответствии с правилами, если есть разрешение от администратора безопасности;
- просмотр журналов системы.

Исходя из параметров безопасности, доступных пользователям, выделяют такие события безопасности, как:

- вход в систему (события аутентификации);
- информирование об инцидентах безопасности системы.

Следует уточнить у администратора какие параметры безопасности доступны для аудитора.

Подробное описание параметров безопасности для пользователей содержится в документе «Руководство по эксплуатации» RU.48957919.26.20.40.142.001 92.

1.2.2 Данные учетной записи

Чтобы получить доступ к компьютеру, на который установлена система защиты **Dallas Lock 8.0**, 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**, 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 аппаратный идентификатор

Дополнительные

PIN-код аппаратного идентификатора	Если учетной записи пользователя назначен аппаратный идентификатор, то для авторизации дополнительно может быть использован PIN-код идентификатора
------------------------------------	--

Пользователю необходимо:



- уточнить у администратора безопасности все авторизационные данные для входа на защищенный компьютер.
- запомнить свое имя 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 прописные и строчные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

Для пароля:

- максимальная длина пароля — 31 символ;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
- разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что прописные и строчные буквы воспринимаются как различные (Password и password являются разными паролями).

1.2.3 Перечень ролей пользователей

Администратор безопасности относит каждого пользователя к определенной группе в соответствии с его должностными обязанностями. Пользователю системы защиты следует уточнить у администратора безопасности какими правами доступа он обладает. Ниже представлены роли, которые могут быть назначены для пользователей **Dallas Lock 8.0**.

Группы	Роль	Параметры
Аудитор СЗИ НСД	Аудитор	Привилегированный пользователь — наделенный некоторыми полномочиями на администрирование системы защиты
Аудитор журналов СЗИ НСД	Аудитор	
Криптографический оператор	Аудитор	
Оператор настройки сети	Аудитор	
Оператор помощи по контролю учетных записей	Аудитор	
Пользователь удаленного управления	Аудитор	
Гость	Пользователь	Рядовой пользователь — не имеющий полномочий на администрирование системы защиты, но в соответствии с политиками безопасности имеющий
Пользователь DCOM	Пользователь	
Оператор архива	Пользователь	

Группы	Роль	Параметры
Пользователь журналов производительности	Пользователь	возможность выполнения некоторых операций (осуществление входа/выхода, преобразования объектов ФС и прочие)
Пользователь системного мониторинга	Пользователь	
Пользователь удаленного рабочего стола	Пользователь	
Читатель журнала событий	Пользователь	

В разделах 2 — 6 представлено описание общих для всех пользователей интерфейсов, их параметров и порядок работы с ними.

В разделе 7 приведены описание и перечень интерфейсов, с привязкой к ролям пользователей, для которых они доступны.

Перечень интерфейсов, доступных для ролей аудитора определяться администратором безопасности, их описание приведено в RU.48957919.26.20.40.142.001 ПФС и в эксплуатационной документации **Dallas Lock 8.0**.

1.2.4 Данные учетной записи

Также 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.

1.2.5 Режимы работы пользователя в системе

Администратором безопасности может быть задан особый режим контроля доступа к информационным ресурсам: режим обучения, неактивный режим, «мягкий» режим, замкнутая программная среда.

Режим обучения

Режим обучения позволяет одновременно фиксировать события о запрете доступа и автоматически назначать права на ресурсы, к которым доступ блокируется.

Администратор назначает пользователю доступ к ресурсам, к которым блокируется доступ. В процессе работы на необходимые для работы объекты ФС будет происходить назначение тех дескрипторов, которые настроены при включении режима обучения, тем самым определяется настройка замкнутой программной средой. Событие включения (выключения) режима обучения фиксируется в журнале управления политиками.

Неактивный режим

В неактивном режиме происходит полное отключение подсистем **СЗИ Dallas Lock 8.0**. Включение данного режима позволяет пользователю работать при несовместимости **Dallas Lock 8.0** со сторонним программным или аппаратным обеспечением, инфраструктурой сети и т. д.

Мягкий режим

При включенном «мягком» режиме проверяются все права доступа пользователем к ресурсам и программам, сообщения о запрете, при попытке осуществления запрещенной политиками безопасности операции, заносятся в журнал системы защиты, и в то же время доступ к запрещенным объектам предоставляется несмотря на запрет.

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

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

События включения и выключения режима фиксируются в журнале управления политиками. Подобное сообщение после загрузки ОС можно увидеть, если администратор включил так называемый «режим обучения» или «неактивный режим» (рис. 2).

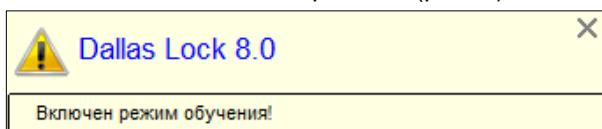


Рис. 2. Предупреждение о включенном режиме обучения

Замкнутая программная среда

Администратор назначает права для специальной группы пользователей для замкнутой программной среды (далее — ЗПС).

Первый вход пользователя осуществляется без ограничений ЗПС, так как при первом входе в системной папке создается профиль пользователя. Таким же образом, если на компьютере установлен Microsoft Office, то, при первом входе пользователя до включения ограничений ЗПС, нужно запустить какое-либо приложение Microsoft Office, так как он производит локальную установку в профиль. Если пользователю необходима программа, которую он после первого входа не может открыть, следует обратиться к администратору безопасности для расширения доступа к программному обеспечению.

2 ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР

2.1 Вход в операционную систему

При загрузке компьютера, защищенного **СЗИ Dallas Lock 8.0**, в зависимости от ОС, появляется экран приветствия (приглашение на вход в ОС) (рис. 3).

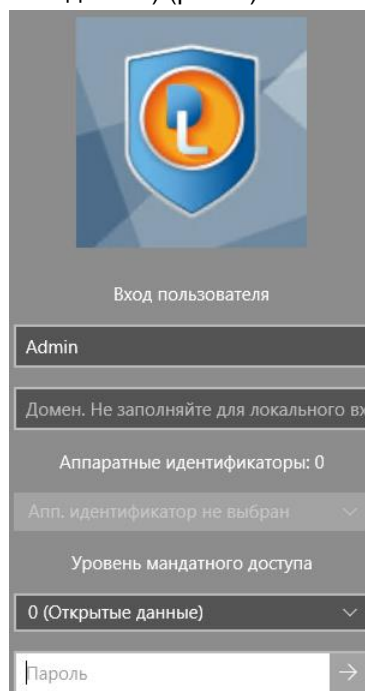


Рис. 3. Экран приветствия в ОС Windows 10

Для входа на защищенный **СЗИ Dallas Lock 8.0** компьютер каждому пользователю предлагается выполнить следующую последовательность шагов.

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе. В зависимости от настроек системы защиты 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 (см. ниже).
4. Выбрать уровень доступа и (или) мандатную метку (если включен параметр **Мандатный доступ** → **Выбор мандатной метки при входе в ОС**), назначенный пользователю администратором безопасности (*только для Dallas Lock 8.0 редакции «С»*).
5. Ввести пароль. При вводе пароля поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «•» (точка).
6. При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
7. Нажать кнопку **Enter**.

После нажатия кнопки **Enter** в системе защиты сначала проверяется возможность входа пользователя с данным именем и доменом, 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 в систему, иначе вход в систему пользователю запрещается.



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

2.1.1 Вход с использованием смарт-карт с сертификатом УЦ Windows

Для возможности входа на защищенный системой защиты **Dallas Lock 8.0** компьютер при помощи смарт-карт, через удостоверяющий центр MS Windows, необходимо соблюдение следующих условий:

- компьютер, на который осуществляется вход, должен быть введен в доменную сеть Windows и находиться под управлением AD;
- включена политика **Dallas Lock 8.0 Политики авторизации → Разрешить использование смарт-карт.**

Если все условия соблюдены, экран приветствия будет содержать отдельную опцию, позволяющую войти в ОС с использованием смарт-карт.

Для перехода к выбору входа по смарт-карте в ОС Windows 10 выбор типа входа отобразится внизу экрана слева (рис. 4).

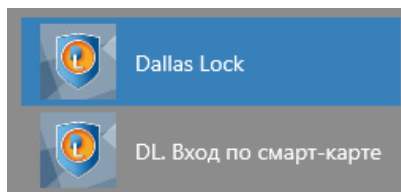


Рис. 4. Выбор типа входа в ОС Windows 10

При выборе входа по смарт-карте необходимо вставить смарт-карту в считывающее устройство, ввести PIN-код и нажать кнопку **Enter** (рис. 5).

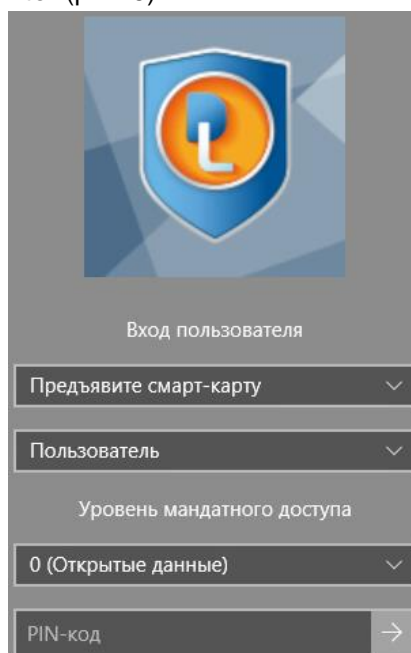


Рис. 5. Экран входа по смарт-карте в ОС Windows 10

2.1.2 Вход с аппаратным идентификатором

Если пользователю в процессе работы назначен аппаратный идентификатор, то для того, чтобы его предъявить, 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. 6).

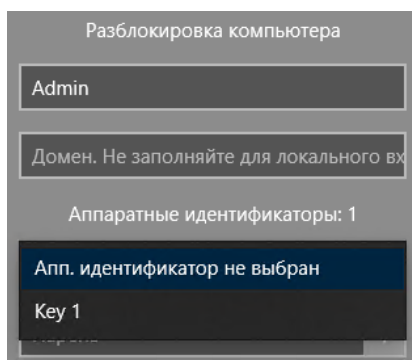


Рис. 6. Выбор аппаратного идентификатора при входе в ОС Windows

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 формы¹ (рис. 7);

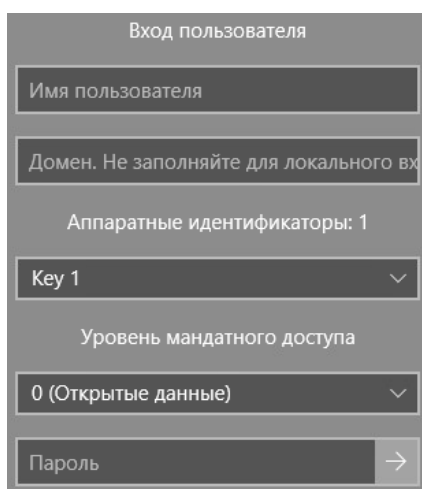


Рис. 7. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (рис. 8);

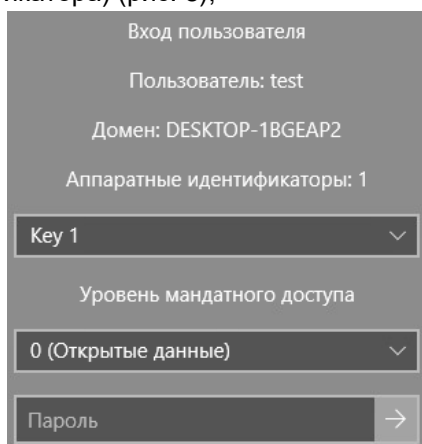


Рис. 8. Поля авторизации после предъявления идентификатора

¹ Для Dallas Lock 8.0 редакции «С» выбор мандатного уровня останется обязательным при любом способе авторизации. Для Dallas Lock 8.0 редакции «К» данные поля отображаться не будут.

- выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 9);

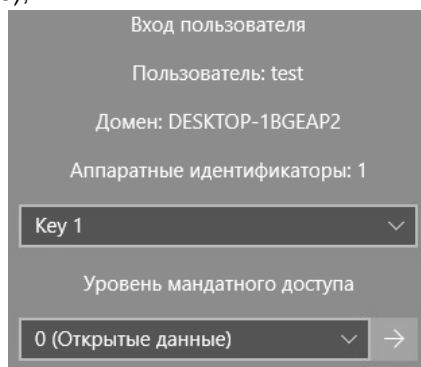


Рис. 9. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 10).

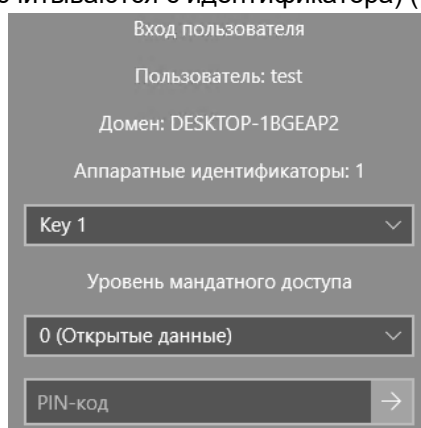


Рис. 10. Поля авторизации после предъявления идентификатора

При использовании идентификаторов типа USB-ключи и смарт-карты JaCarta PKI/BIO, в память которых записана биометрическая информация, возможны следующие способы авторизации в зависимости от произведенных администратором безопасности настроек:

- ввод PIN-кода и биометрических данных (рис. 11);

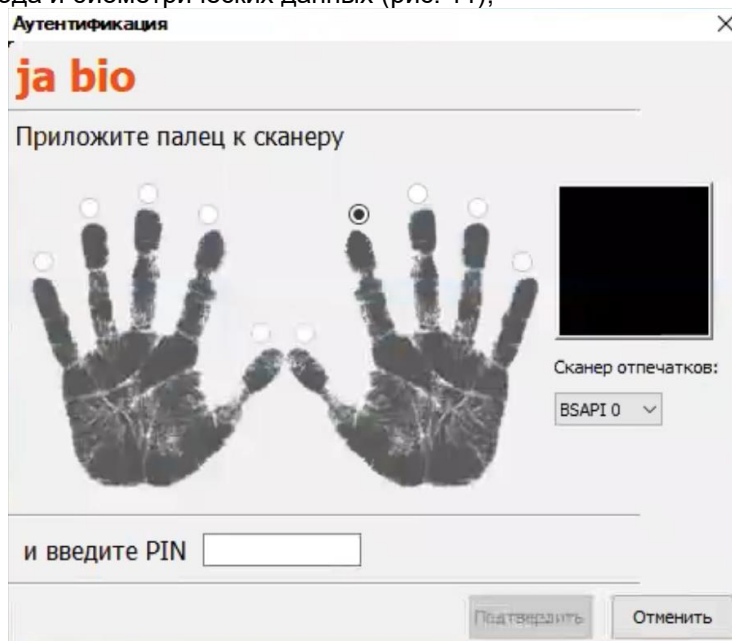


Рис. 11. Ввод авторизационных данных (PIN-код и биометрия)

- ввод PIN-кода или биометрических данных (рис. 12);

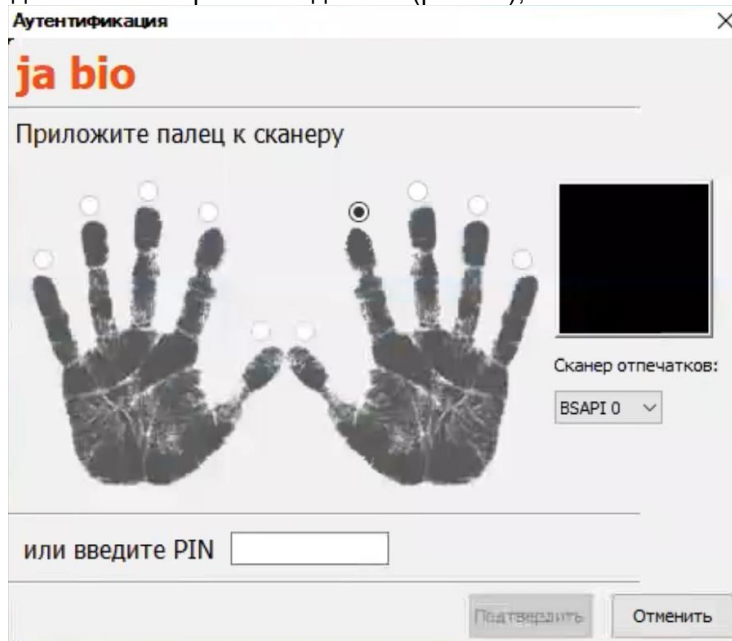


Рис. 12. Ввод авторизационных данных (PIN-код или биометрия)

- ввод только биометрических данных (рис. 13).



Рис. 13. Ввод авторизационных данных (биометрия)



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.

2.1.3 Вход с PayControl

После передачи администратором ссылки или QR-кода и кода активации пользователю необходимо скачать приложение PayControl и пройти регистрацию. Пользователю необходимо ввести код активации, который был передан ранее администратором информационной безопасности, нажать кнопку **Далее** (рис. 14).

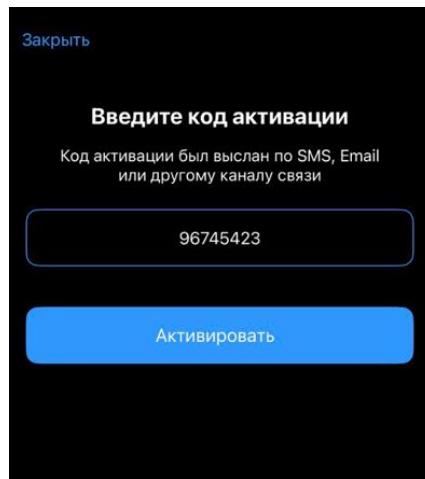


Рис. 14. Код активации

На следующей странице ввести имя ключа (может быть несколько ключей) для дальнейшей авторизации, нажать кнопку **Далее** (рис. 15).

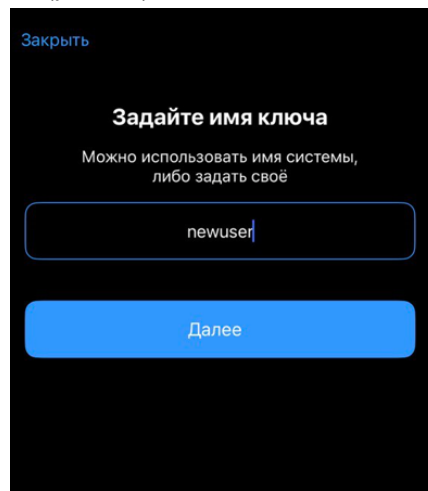


Рис. 15. Имя ключа

На следующей странице пользователю необходимо придумать пароль не менее 6 символов (рис. 16). После проделанной операции пользователем, он будет окончательно занесен в реестр сервера подключения PayControl.

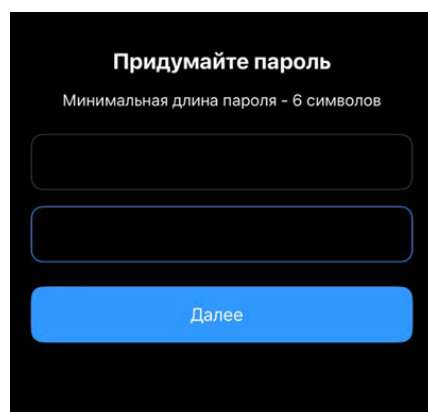


Рис. 16. Пароль для ключа

При авторизации пользователя в системе появится сообщение о необходимости подтверждения авторизации пользователя в мобильном приложении PayControl (рис. 17).

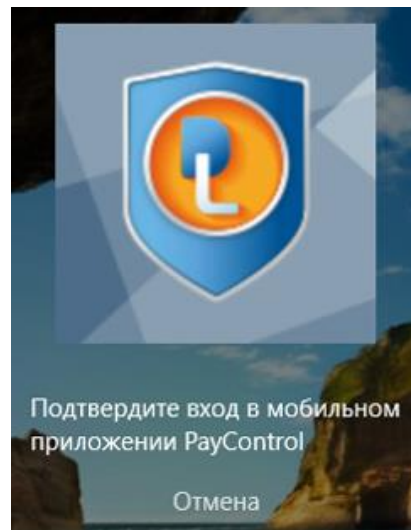


Рис. 17. Сообщение о подтверждении входа в мобильном приложении PayControl

На мобильном устройстве пользователю необходимо подтвердить вход в систему (рис. 18). У пользователя есть 2 минуты, чтобы подтвердить операцию входа в мобильном приложении. Если подключить аппаратный идентификатор к компьютеру в момент ожидания подтверждения, то операция входа будет отменена.

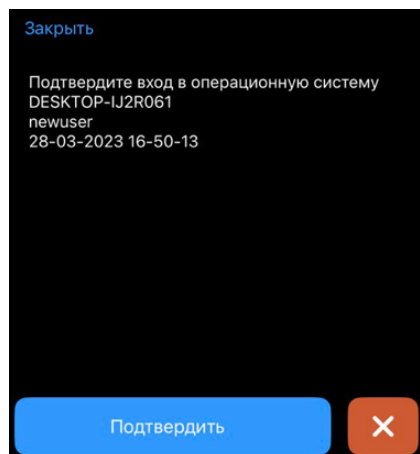


Рис. 18. Подтверждение авторизации на мобильном устройстве

При ошибке или не подтверждении операции входа будет отображено соответствующее сообщение (рис. 19).

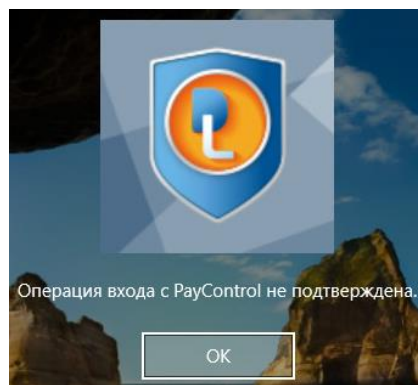


Рис. 19. Ошибка подтверждения входа

2.2 Ошибки, возникающие при входе



При всех возникающих затруднительных ситуациях следует обращаться к администратору безопасности.

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. 20).

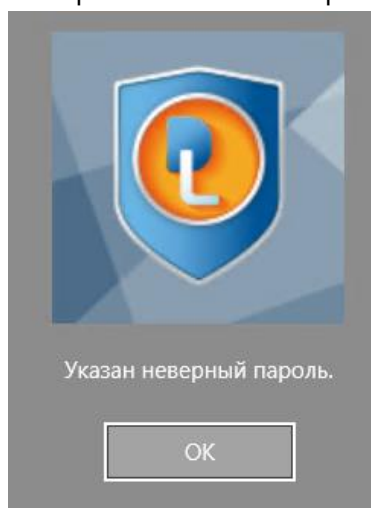


Рис. 20. Сообщение при вводе неправильного пароля

Подобное сообщение появится и при предъявлении неверного аппаратного идентификатора или в случае, когда зарегистрированный за пользователем идентификатор не предъявлен вообще (рис. 21).

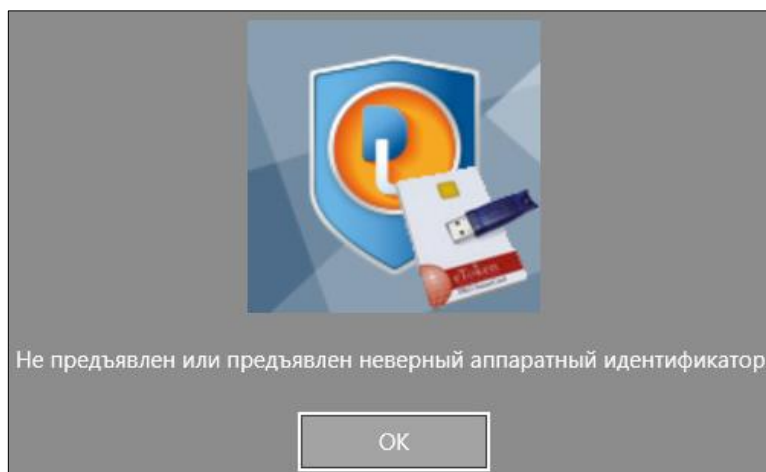


Рис. 21. Сообщение при неверном идентификаторе

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

Также при ошибочном вводе данных в поле имени или домена могут возникнуть соответствующие сообщения (рис. 22).

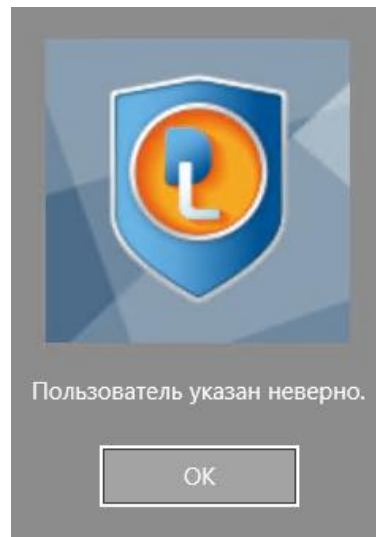


Рис. 22. Ошибка авторизации

Администратор безопасности может отключить учетную запись, тогда при авторизации система защиты выведет соответствующее предупреждение (рис. 23).

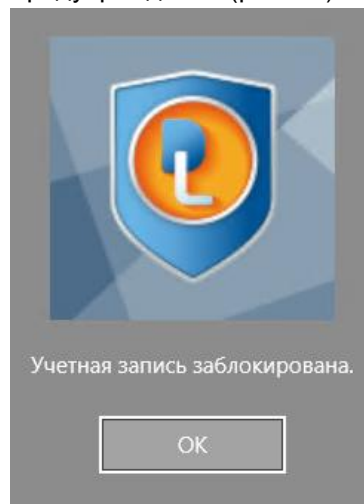


Рис. 23. Сообщение при отключенной учетной записи

При проблеме подключения по локальной сети может возникнуть ошибка авторизации доменных пользователей (рис. 24).

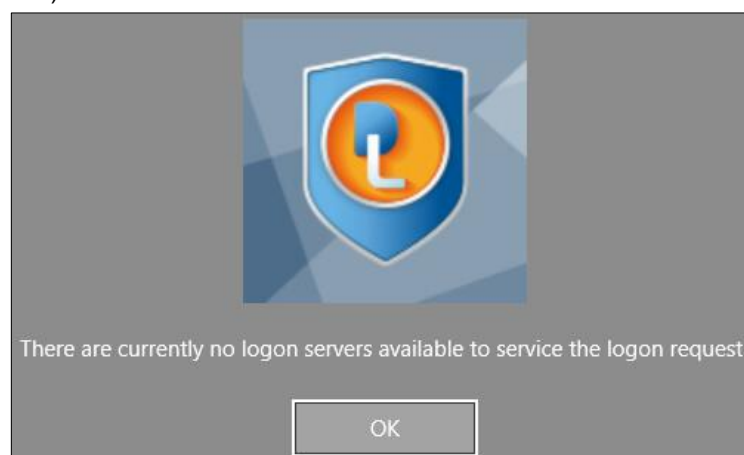


Рис. 24. Ошибка при вводе имени домена

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 ОС для пользователя будет запрещен (рис. 25).

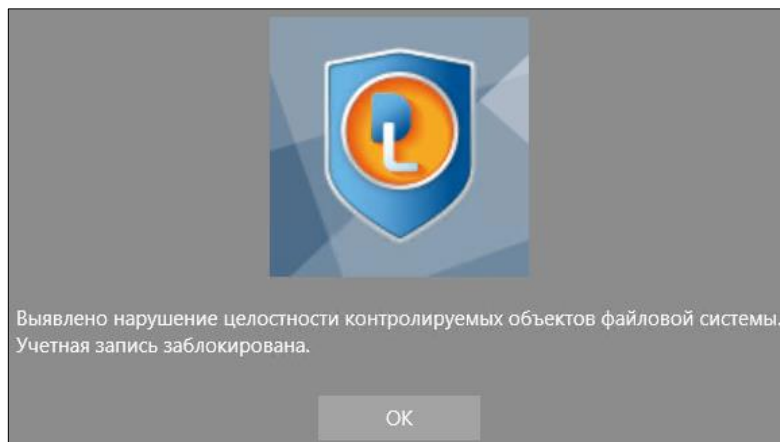


Рис. 25. Сообщение при входе

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. 26).

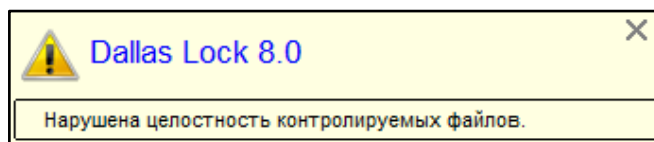


Рис. 26. Предупреждение о нарушенной целостности

Если пользователю назначен вход через PayControl, но на компьютере или сервере отсутствует подключение, то **СЗИ** через некоторое время отображает ошибку о соединении с сервером PayControl.

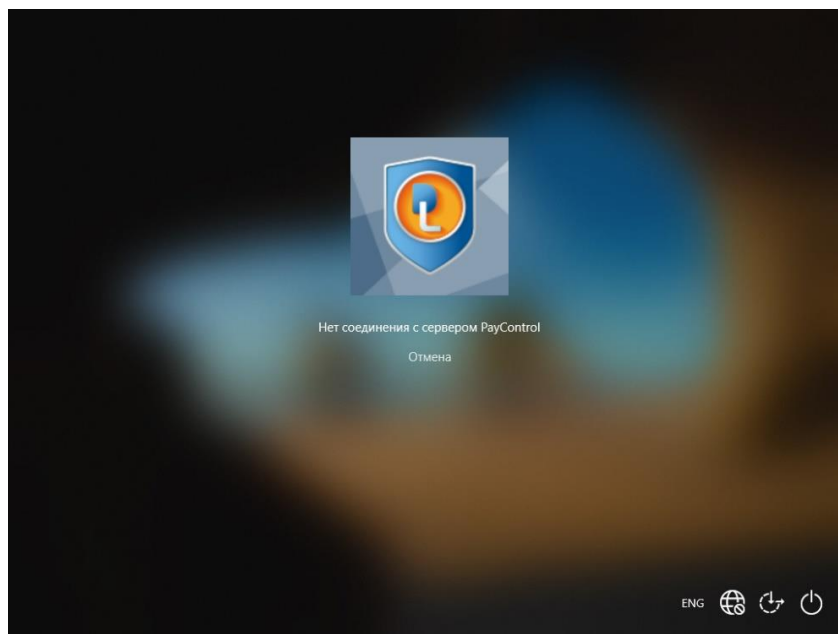


Рис. 27. Ошибка отсутствия соединения

Во всех сложных ситуациях, связанных с работой **СЗИ**, которые пользователь не в состоянии разрешить самостоятельно, необходимо 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 **Выключение**.
3. После нажатия кнопки **Выключение** 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 ОС Windows 10 в меню **Пуск**  слева вверху нажать на кнопку учетной записи пользователя и в появившемся окне выбрать пункт меню **Сменить пользователя** (рис. 28).

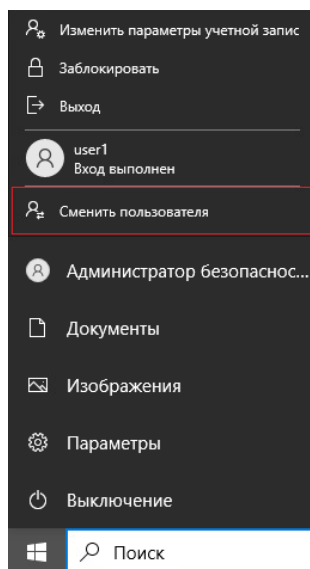


Рис. 28. Смена пользователя в ОС Windows 10

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



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** может быть включен режим запрета смены пользователя без перезагрузки компьютера.

В этом случае при смене пользователя ОС автоматически завершит работу и выполнит перезагрузку (рис. 29).

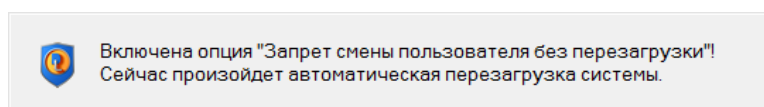


Рис. 29. Автоматическая перезагрузка при смене пользователя

Несохраненные другими пользователями результаты работы в этом случае не сохраняются.

4 СМЕНА ПАРОЛЯ

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 **Изменить пароль** (рис. 30).

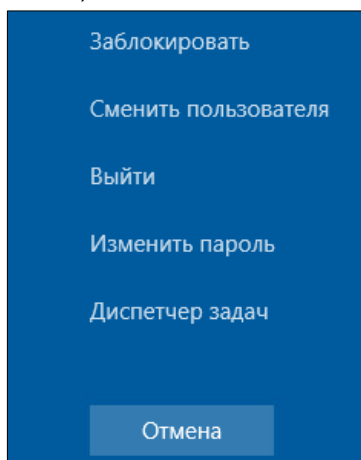


Рис. 30. Меню действий

На экране появится диалоговое окно, предлагающее ввести данные для смены пароля (рис. 31).

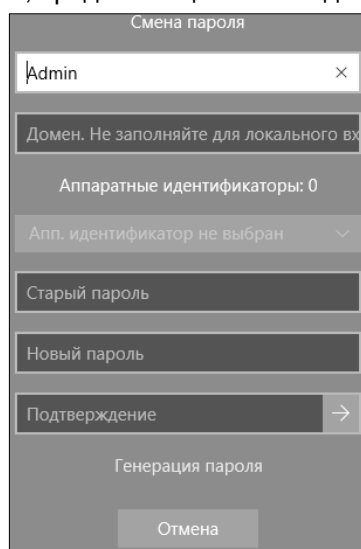


Рис. 31. Экран смены пароля

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.



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 *Подтверждение*.
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. 32 — рис. 37).

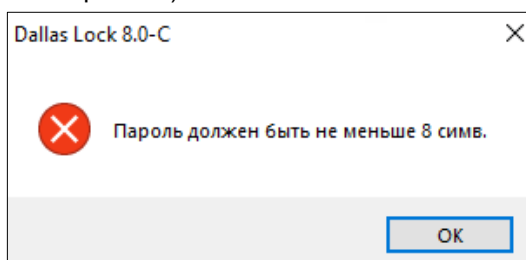


Рис. 32. Ошибка при смене пароля. Требования к длине пароля

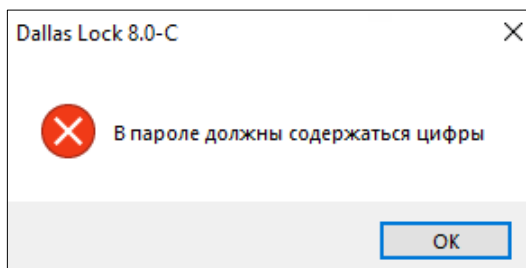


Рис. 33. Ошибка при смене пароля. Необходимость наличия цифр

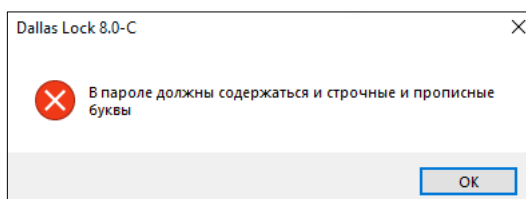


Рис. 34. Ошибка при смене пароля. Необходимость наличия строчных букв

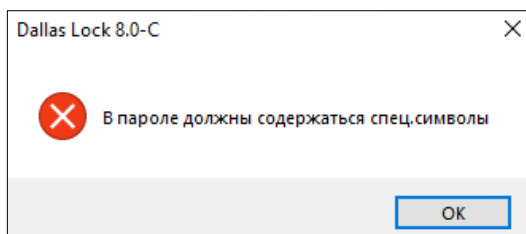


Рис. 35. Ошибка при смене пароля. Необходимость наличия спецсимволов

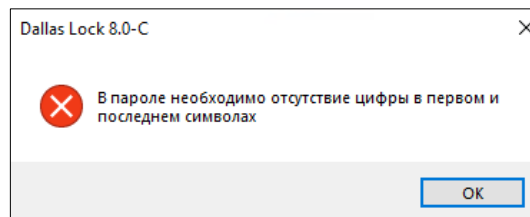


Рис. 36. Ошибка при смене пароля. Необходимость отсутствия цифр

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. 37).

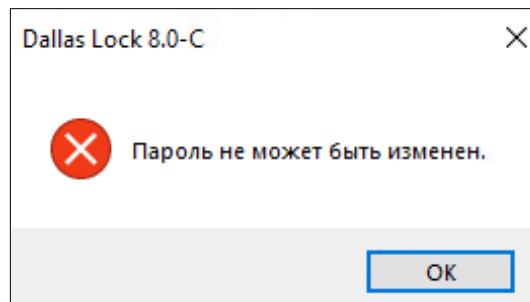


Рис. 37. Сообщение системы при смене пароля

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, появится соответствующее сообщение (рис. 38).

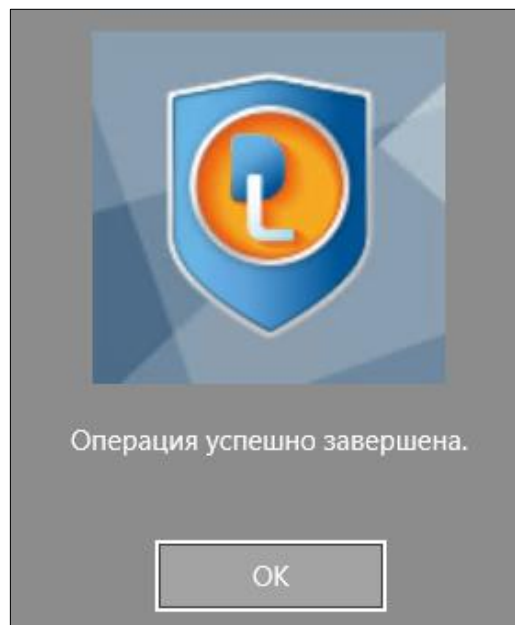



Рис. 38. Успешная смена пароля

Далее вход пользователя на защищенную **СЗИ Dallas Lock 8.0** 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 тремя способами, приведенными ниже.

1. Дважды нажать правой клавишей мыши на иконку , которая находится в нижнем правом углу экрана в выпадающем меню области уведомлений (рис. 39).

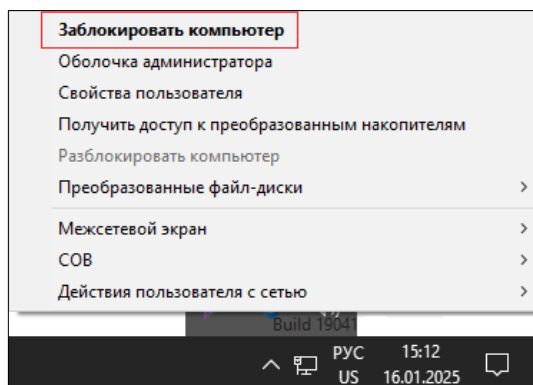


Рис. 39. Иконка блокировки на панели задач

2. Нажать комбинацию клавиш «Win» + «L» (рис. 40).

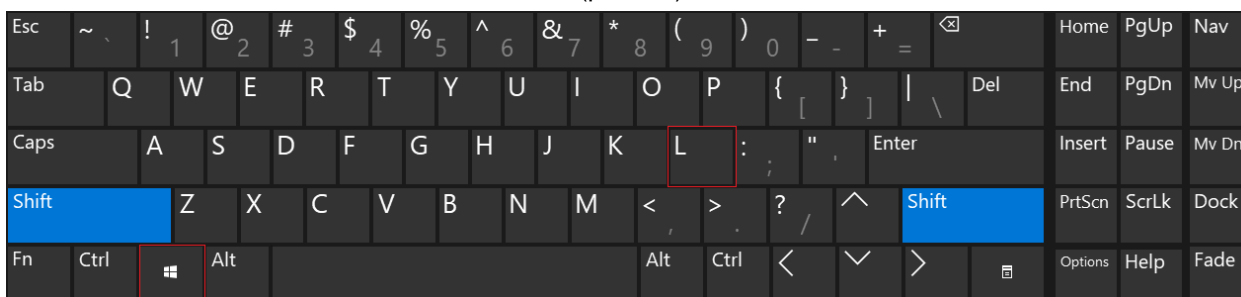


Рис. 40. Комбинация клавиш

3. Нажать комбинацию клавиш **Ctrl+Alt+Del** и на появившемся экране выбрать кнопку **Заблокировать** (рис. 41).

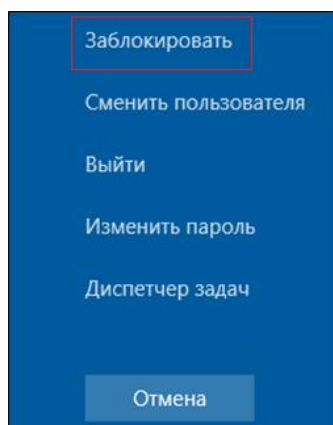


Рис. 41. Меню блокировки экрана

Компьютер может заблокироваться автоматически по истечении заданного периода неактивности пользователя. Период неактивности, после которого компьютер будет автоматически заблокирован, задается стандартными средствами ОС (рис. 42).

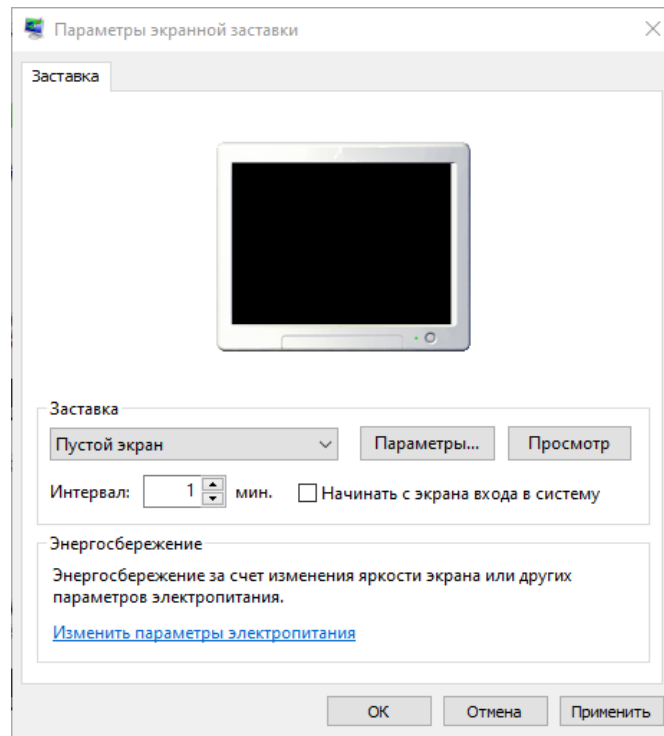


Рис. 42. Параметры автоматической блокировки экрана

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. 43)

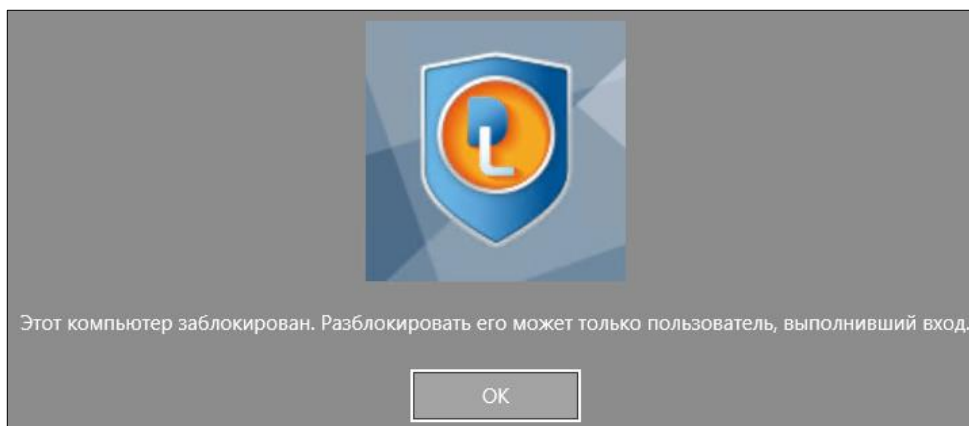


Рис. 43. Сообщение ОС при попытке входа на заблокированный компьютер

6 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Система защиты **Dallas Lock 8.0** предоставляет пользователю несколько дополнительных возможностей, позволяющих увеличить уровень защищенности информации.

6.1 Механизм очистки остаточной информации

Большинство ОС 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 ОС заново не использует это пространство для хранения новых данных. Такая остаточная информация может легко привести к непреднамеренному распространению конфиденциальной информации.

В **СЗИ Dallas Lock 8.0** реализована функция очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

При необходимости удаления пользователем каких-либо данных 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. 44).

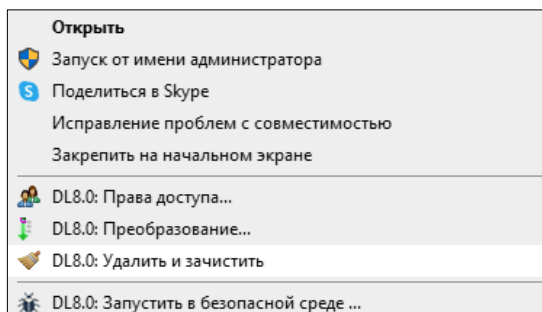


Рис. 44. Контекстное меню

2. Нажать **Да** в появившемся окне подтверждения операции (рис. 45).

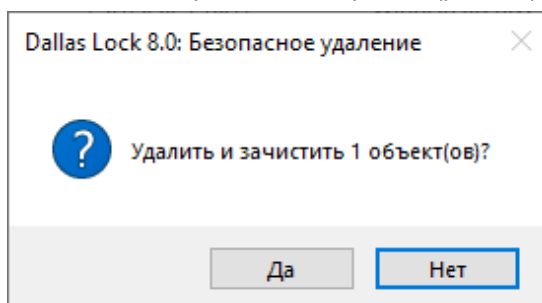


Рис. 45. Окно подтверждения операции

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. 46).

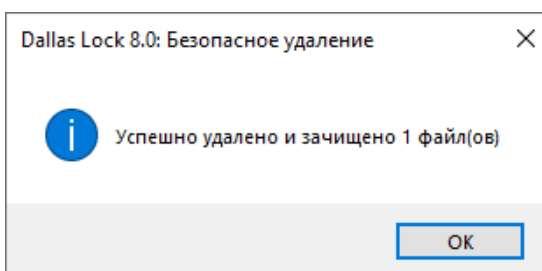


Рис. 46. Сообщение об удалении файлов



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. 47).

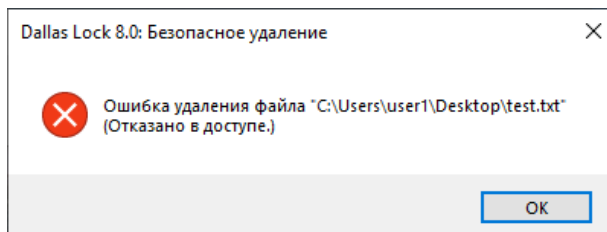


Рис. 47. Сообщение на запрет удаления файла

6.2 Преобразование информации

Для дополнительной защиты важных данных в системе защиты **Dallas Lock 8.0** имеется возможность преобразования этих данных 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 Dallas Lock 8.0**, и также недоступным на ПК, защищенном **СЗИ Dallas Lock 8.0**, 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. 48).

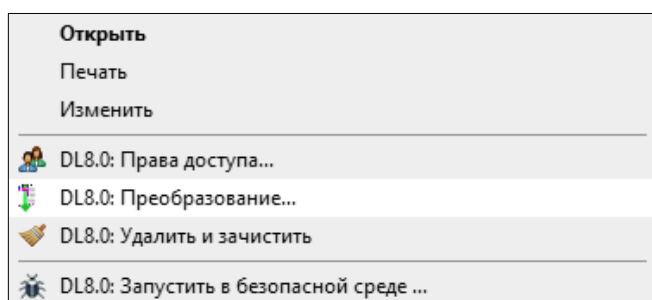


Рис. 48. Контекстное меню

2. На экране появится окно, в котором необходимо заполнить параметры преобразования (рис. 49).

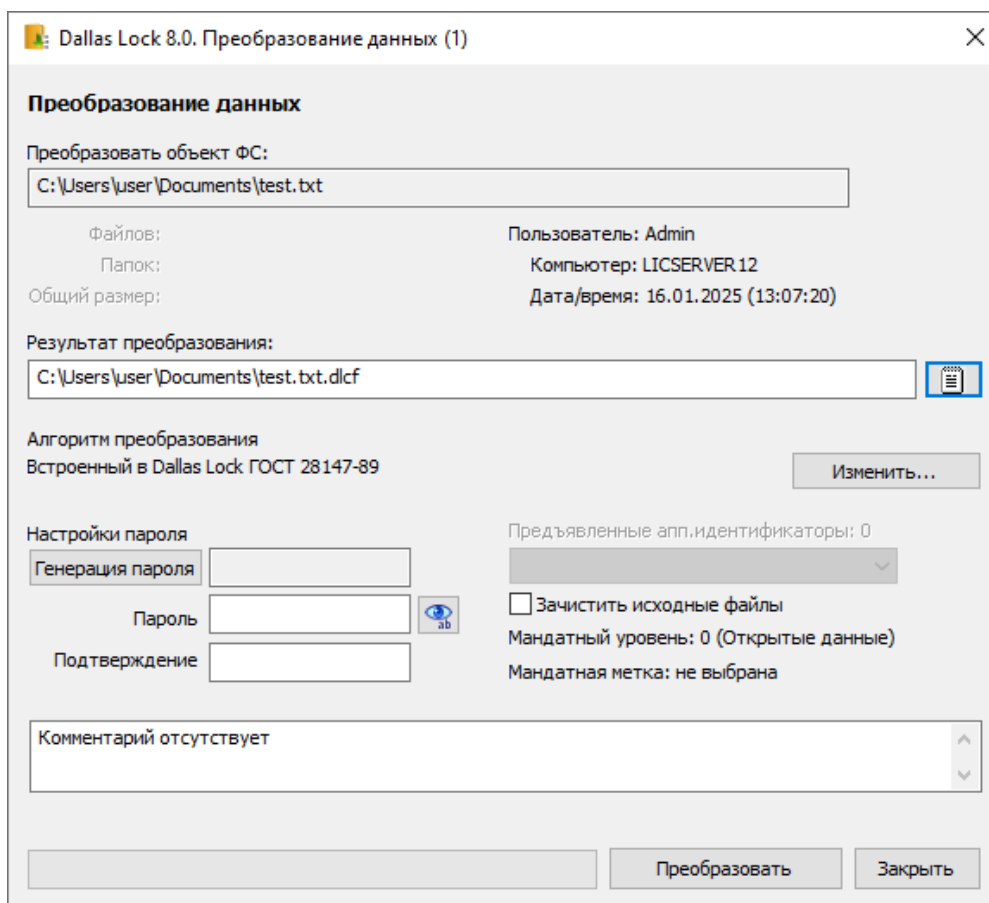


Рис. 49. Окно преобразования данных

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 в текущей папке из имени преобразовываемого объекта с добавлением специального расширения). 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
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
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 **Преобразовать**.

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. 50).



Рис. 50. 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.



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.

6.2.2 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, 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, 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. 51).

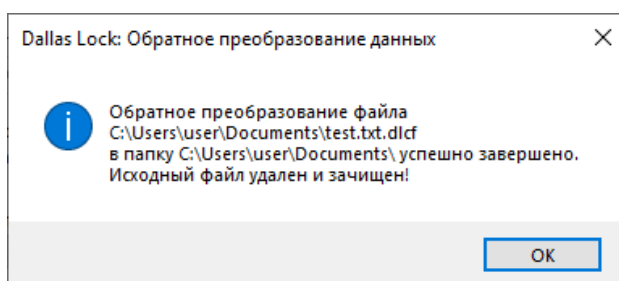


Рис. 51. Подтверждение успешного обратного преобразования файла


6.3 Преобразованные файл-диски

Для безопасности хранения и обработки информации в **Dallas Lock 8.0** реализован механизм создания таких контейнеров информации, на которых при работе с размещенными в них 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, подключение диска для работы пользователя с ним может быть произведено только на ПК, защищенном **Dallas Lock 8.0**, и только с указанием ключевой информации.

6.3.1 Работа с преобразованным файл-диском

Для работы с преобразованным файл-диском необходимо подключить такой диск в ОС 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. 52). Включение также доступно из контекстного меню значка самого файл-диска.

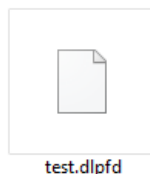



Рис. 52. Значок созданного преобразованного файл-диска

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

- выбрать путь к файл-диск;
- 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 будет 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 файл-диски, необходимо выбрать соответствующие пункты в меню **Преобразованные файл-диски**. Отключение также происходит после выключения или перезагрузки ПК.

6.3.2 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. 53).

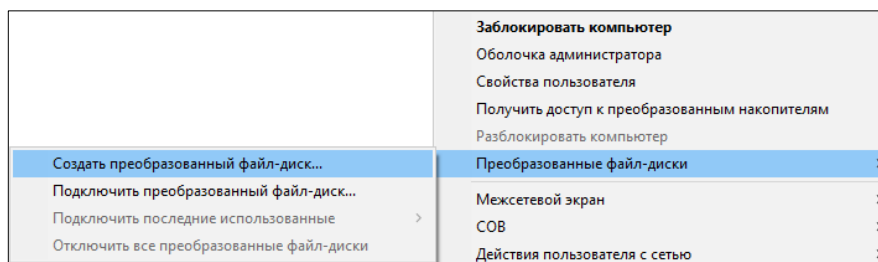


Рис. 53. Выбор пункта меню для создания преобразованного файл-диска

На экране появится окно свойств создаваемого файл-диска (рис. 54).

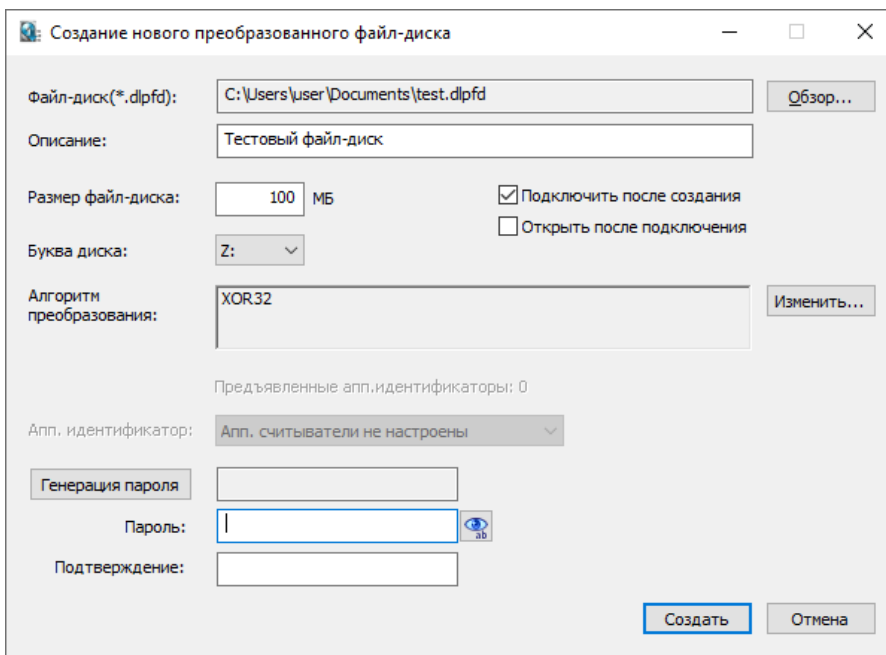


Рис. 54. Окно параметров при создании преобразованного файл-контейнера

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 (необязательное 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
Открыть после подключения	Отмеченное поле позволяет автоматически открыть файл-диск в проводнике Windows, после того как данный файл-диск был смонтирован в качестве логического диска в ОС
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, но можно использовать внешний алгоритм преобразования, для чего необходимо нажать Изменить и выбрать параметры настройки

Наименование поля	Описание
Аппаратный идентификатор	Для назначения аппаратного идентификатора необходимо предъявить идентификатор и выбрать его из выпадающего списка (также необходимо предварительно зарегистрировать в СЗИ считыватели). Если аппаратный идентификатор не указан, 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 преобразованный файл-диск создан и подключен как логический диск с указанной буквой диска (если было отмечено подключение).

Созданный таким образом файл будет иметь расширение *.dplfd и иметь определенный значок.

6.4 Преобразованные съемные накопители

В системе защиты **Dallas Lock 8.0** реализована возможность преобразования съемных накопителей. Преобразование съемных накопителей может быть использовано, например, при передаче секретных документов между автономными рабочими станциями.

Понятие «*преобразование съемных накопителей*» подразумевает, что данный накопитель при подключении его к ПК будет отмечен в **СЗИ** таким образом, что вся информация на нем при ее обработке (создании и изменении файлов) будет автоматически преобразована.

6.4.1 Работа с преобразованным съемным накопителем

Чтобы получить доступ к преобразованному съемному накопителю с установленным паролем, необходимо подключить данный накопитель к ПК, после чего появится окно **Доступ к накопителям** (рис. 55).

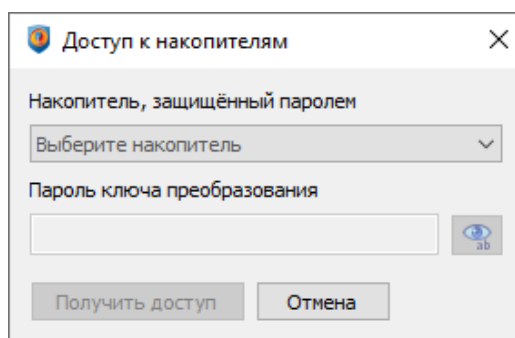



Рис. 55. Доступ к накопителям

В данном окне необходимо выбрать накопитель, ввести пароль и нажать кнопку **Получить доступ**.

Также возможно открыть данное окно используя меню значка блокировки на панели задач , выбрав пункт меню **Получить доступ к преобразованным накопителям** (рис. 56).

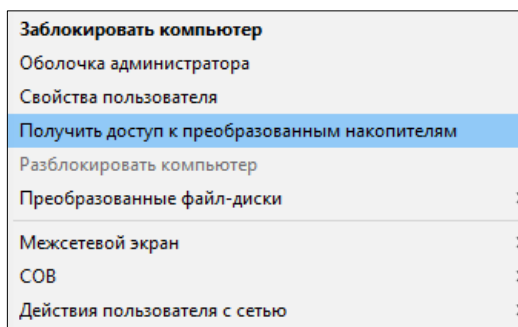


Рис. 56. Выбор пункта меню для получения доступа к накопителю

В результате на экране отобразится окно, в котором нужно выбрать накопитель, к которому необходимо получить доступ, и ввести пароль ключа преобразования для него (рис. 57).

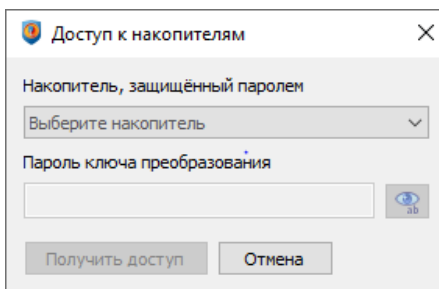


Рис. 57. Получение доступа к преобразованным съемным носителям

При попытке открытия преобразованного съемного накопителя из проводника возникает сообщение об отказе доступа (рис. 58).

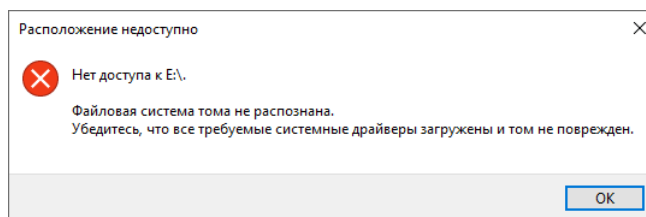


Рис. 58. Отказ доступа

При вводе неверного пароля на экране появляется сообщение об ошибке (рис. 59).

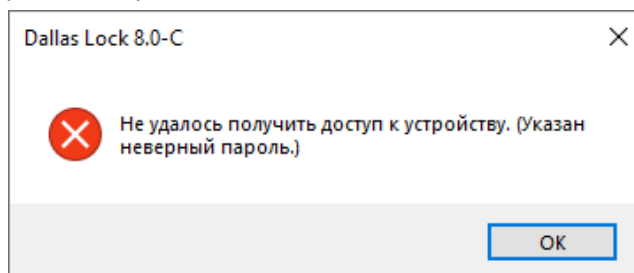


Рис. 59. Попытка доступа к устройству с неверным паролем

При превышении допустимого количества неуспешных попыток ввода пароля ключа преобразования доступ к защищаемому устройству для данного пользователя блокируется. На экране появляется соответствующее сообщение (рис. 60).

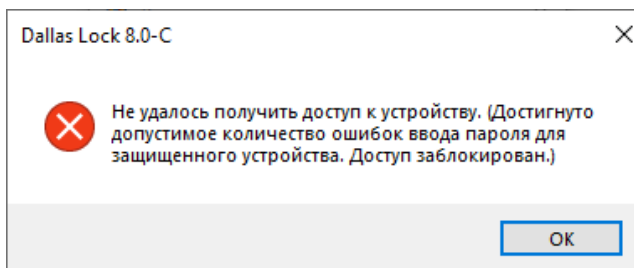


Рис. 60. Блокировка доступа к устройству



Восстановление информации после блокировки доступа к преобразованному съемному накопителю осуществляется администратором **СЗИ**. Подробная информация содержится в документе «Руководство по эксплуатации».

При указании верного пароля для устройства пользователю предоставляется доступ. На экране появляется соответствующее сообщение (рис. 61).

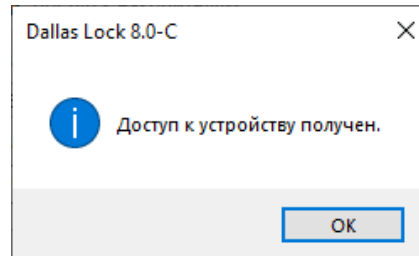


Рис. 61. Доступ к устройству

7 ИНТЕРФЕЙСЫ, ДОСТУПНЫЕ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Для пользователей, которые состоят в определенных группах, назначенных администратором безопасности в соответствии с их должностями обязанностями, доступны определенные параметры интерфейса в системе защиты **Dallas Lock 8.0**.

Для пользователей, которые состоят в следующих группах: операторы архива, пользователи журналов производительности, читатели журнала событий, в оболочке администратора доступна только вкладка *Журналы*. Пользователи данных групп могут выполнять следующие действия посредством использования управляющих кнопок (параметры интерфейса): архивация и экспорт журнала, фильтрация и группировка журнала (рис. 62). Для групп пользователей системного мониторинга и пользователей DCOM доступен вход в оболочку администратора, где доступна только вкладка *Журналы* с действиями: экспорт, фильтрация и группировка журнала.

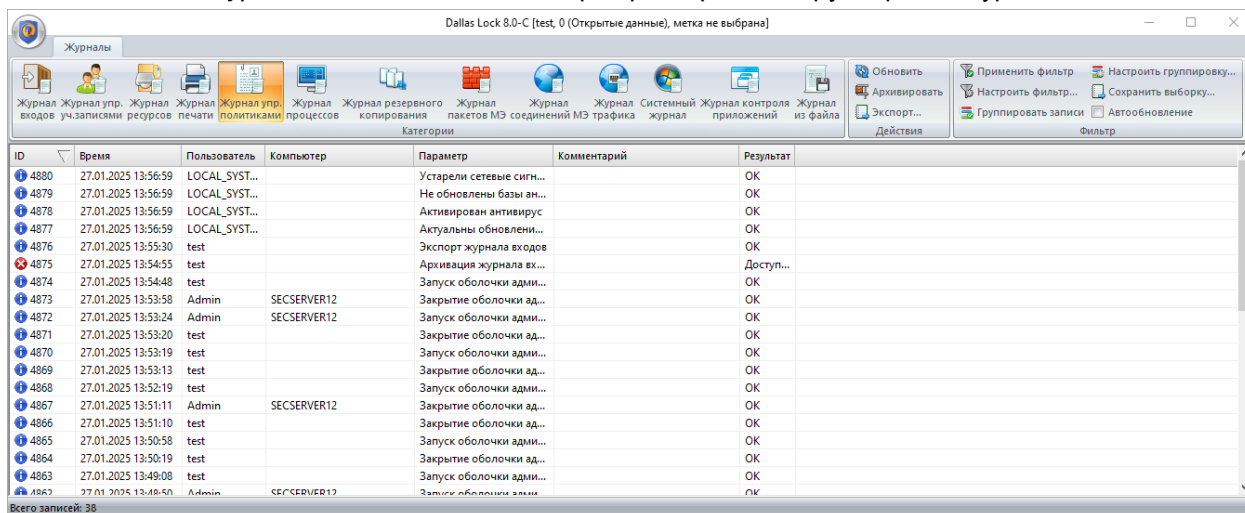


Рис. 62. Вкладка «Журналы» для пользователя

В Консоли сервера безопасности пользователи с ролью *Аудитор СБ* могут просматривать все вкладки, включая установленные параметры и журналы аудита (рис. 63). Пользователи с ролью *Аудитор домена* могут просматривать все вкладки, за исключением вкладок *Журналы СБ* и *Администрирование на СБ*.

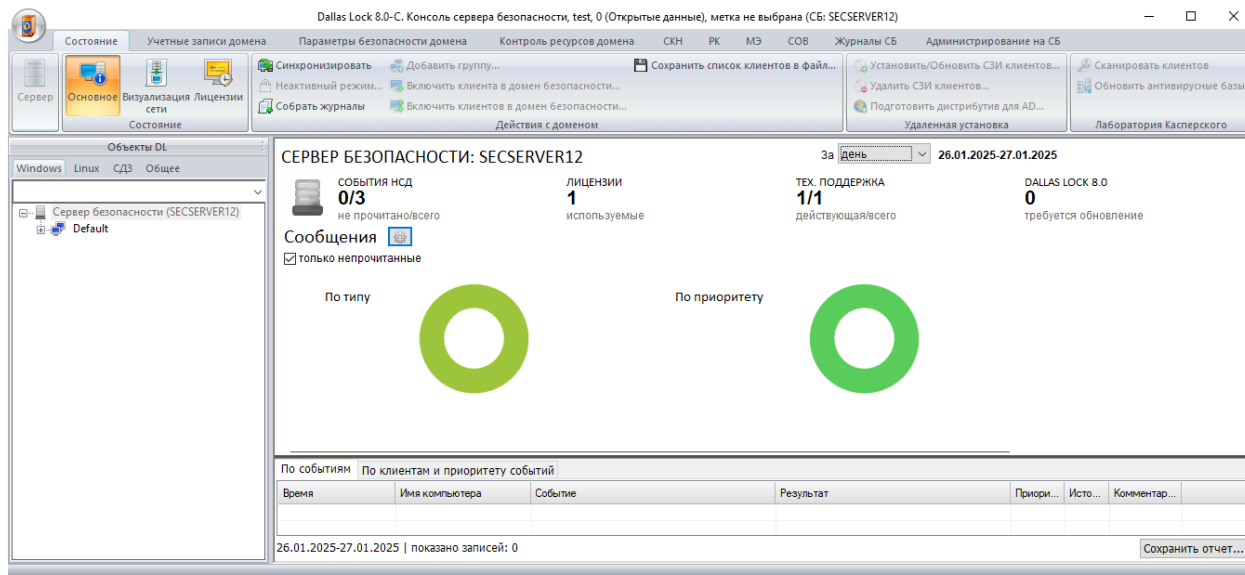


Рис. 63. Вкладка «Состояние» для пользователя

Пользователи данных ролей могут выполнять следующие действия посредством использования управляющих кнопок (параметры интерфейса): экспорт, фильтрация и группировка журнала. Когда пользователь с ролью *Аудитор СБ* или *Аудитор домена* входит в Консоль сервера безопасности, параметры безопасности отображаются, но отсутствует возможность их редактировать или настраивать. Кроме того, любые другие действия, связанные с настройками, будут невозможны; кнопки для изменения настроек будут недоступны, а при попытке выполнить какие-либо действия возникнет ошибка с уведомлением о запрете доступа.

Для гостей или других пользователей, которым запрещено входить в оболочку администратора или в консоль сервера безопасности появляется окно о запрете доступа (рис. 64, рис. 65).

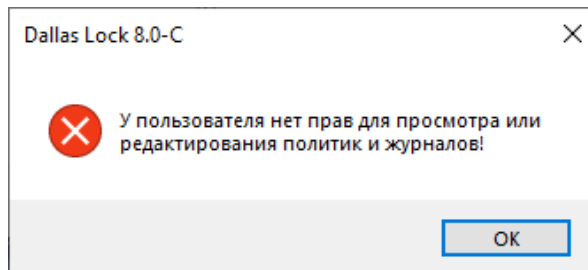


Рис. 64. Сообщение для гостя в оболочке администратора

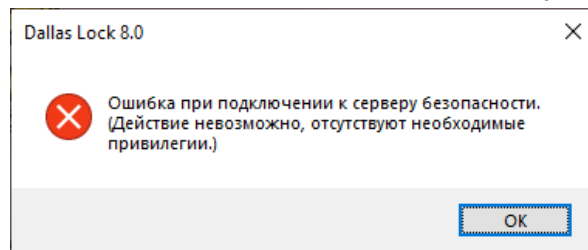


Рис. 65. Сообщение для гостя в консоли сервера безопасности

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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 запуск ОС
ЗПС	замкнутая программная среда
ОС	операционная система
СЗИ	система защиты информации Dallas Lock 8.0
ПК	персональный компьютер
РК	резервное копирование
МЭ	межсетевой экран
СОВ	система обнаружения вторжений