



**ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО**  
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН  
11443195.509000.055 34 -ЛУ

**Специальное программное обеспечение  
средств защиты информации от  
несанкционированного доступа  
«АККОРД-Win32 К»**

**РУКОВОДСТВО ОПЕРАТОРА  
(ПОЛЬЗОВАТЕЛЯ)**

**11443195.509000.055 34**

**Литера О<sub>1</sub>**

## **АННОТАЦИЯ**

Руководство предназначено для конкретизации действий операторов (пользователей) при эксплуатации специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win32 К» (ТУ 509000-055-11443195-2013) (далее по тексту – СПО «Аккорд-Win32 К», «Аккорд-Win32 К», СПО «Аккорд», «Аккорд») и содержит описание способов использования средств защиты СПО «Аккорд-Win32 К», его интерфейса с пользователем в процессе обработки информации.

Перед эксплуатацией СПО «Аккорд-Win32 К» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов СПО «Аккорд-Win32 К» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ и ее средств.

## СОДЕРЖАНИЕ

<b>1. Назначение и краткая характеристика СПО «Аккорд-Win32 К»</b> .....	<b>4</b>
<b>2. Порядок работы на защищенной СВТ</b> .....	<b>5</b>
2.1. Выполнение контрольных процедур .....	5
2.1.1. Процедура идентификации .....	5
2.1.2. Процедура аутентификации .....	6
2.1.3. Проверка ограничения на время входа в систему .....	7
2.1.4. Проверка целостности файлов реестра, программ и данных .....	8
2.2. Работа пользователя в соответствии с функциональными обязанностями .....	9
2.2.1. Проверка полномочий по доступу .....	9
2.2.2. Работа с хранителем экрана .....	9
2.3. Завершение работы и выход из системы .....	10
<b>3. Сообщение программных средств СПО «Аккорд» и порядок     действий пользователя по ним</b> .....	<b>11</b>

11443195.509000.055 34

## **1. Назначение и краткая характеристика СПО «Аккорд-Win32 К»**

Специальное программное обеспечение «Аккорд-Win32 К» (далее – СПО «Аккорд») предназначен для применения на ПЭВМ (рабочих станциях ЛВС) типа IBM PC, функционирующих под управлением ОС Microsoft Windows 8.1 Professional и Microsoft Windows Server 2008 Enterprise с целью обеспечения защиты от несанкционированного доступа (НСД) к СВТ и информационным ресурсам АС, обеспечения конфиденциальности информации, обрабатываемой и хранимой в СВТ при многопользовательском режиме эксплуатации.

СПО «Аккорд-Win32 К» (ТУ 509000-055-11443195-2013) поставляется в составе:

1) Специальное ПО разграничения доступа в среде Windows Windows 8.1 Professional/ Windows Server 2008 Enterprise - СПО «Аккорд-Win32 К», размещаемое на жестком диске СВТ при установке СПО «Аккорд».

2) Эксплуатационная документация<sup>1</sup>.

3) Формуляр.

---

<sup>1</sup> Поставляется на диске совместно с СПО разграничения доступа

11443195.509000.055 34

## 2. Порядок работы на защищенной СВТ

Процесс работы пользователя на СВТ, защищенном СПО «Аккорд», можно разделить на 3 этапа:

- 1) выполнение контрольных процедур;
- 2) работа пользователя в соответствии с функциональными обязанностями и правами доступа;
- 3) завершение работы и выход из системы.

### 2.1. Выполнение контрольных процедур

Контрольные процедуры делятся на обязательные и необязательные, выполняемые при выполнении заданных условий.

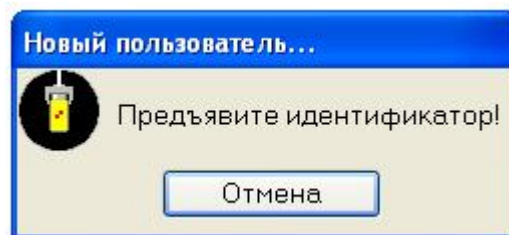
К обязательным процедурам относятся

- процедура идентификации;
- процедура аутентификации;
- проверка целостности файлов реестра, программ и данных.

К необязательным процедурам относится проверка ограничения на время входа в систему.

#### 2.1.1. Процедура идентификации

При загрузке СВТ на экран выводится сообщение:

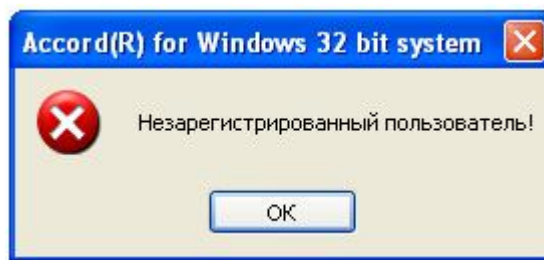


**Рисунок 1 – Запрос данных для идентификации пользователя**

Окно остается на мониторе до предъявления данных для идентификации пользователя. Внизу окна выводится отсчет времени, отведенного для предъявления данных для идентификации пользователя.

Если данные для идентификации не зарегистрированы в системе, то на экране появляется сообщение:

11443195.509000.055 34

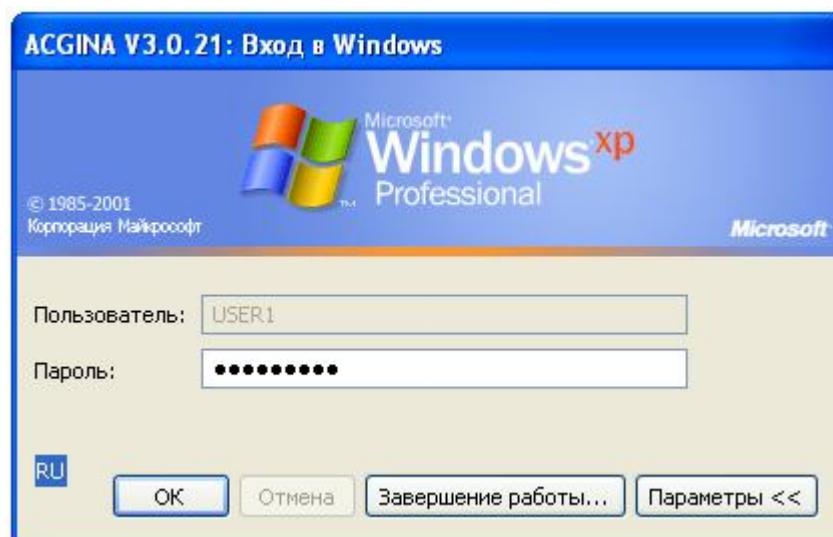


**Рисунок 2 – Данные для идентификации не зарегистрированы**

При успешном завершении процедуры идентификации происходит выполнение процедуры аутентификации (запрос пароля пользователя).

### 2.1.2. Процедура аутентификации

После успешного выполнения процедуры идентификации пользователя, при условии, что ему при регистрации был задан пароль для входа в систему, на экране появляется окно для ввода пароля (рисунок 3):



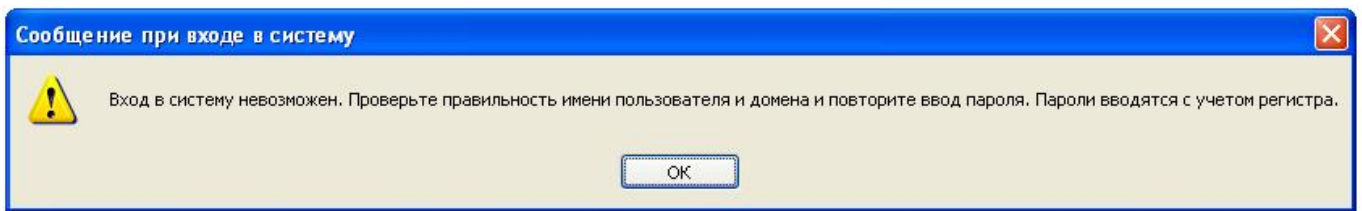
**Рисунок 3 – Аутентификация пользователя**

По этой команде пользователю необходимо набрать пароль, при этом символы пароля выводятся на экран в виде звездочек. Время, отведенное для ввода пароля, отображается в правом нижнем углу, так же как при запросе идентификатора.

Если процедура аутентификации успешно завершилась, начинается загрузка ОС.

При неправильно введенном пароле на экран выводится оповещение (рисунок 4):

11443195.509000.055 34



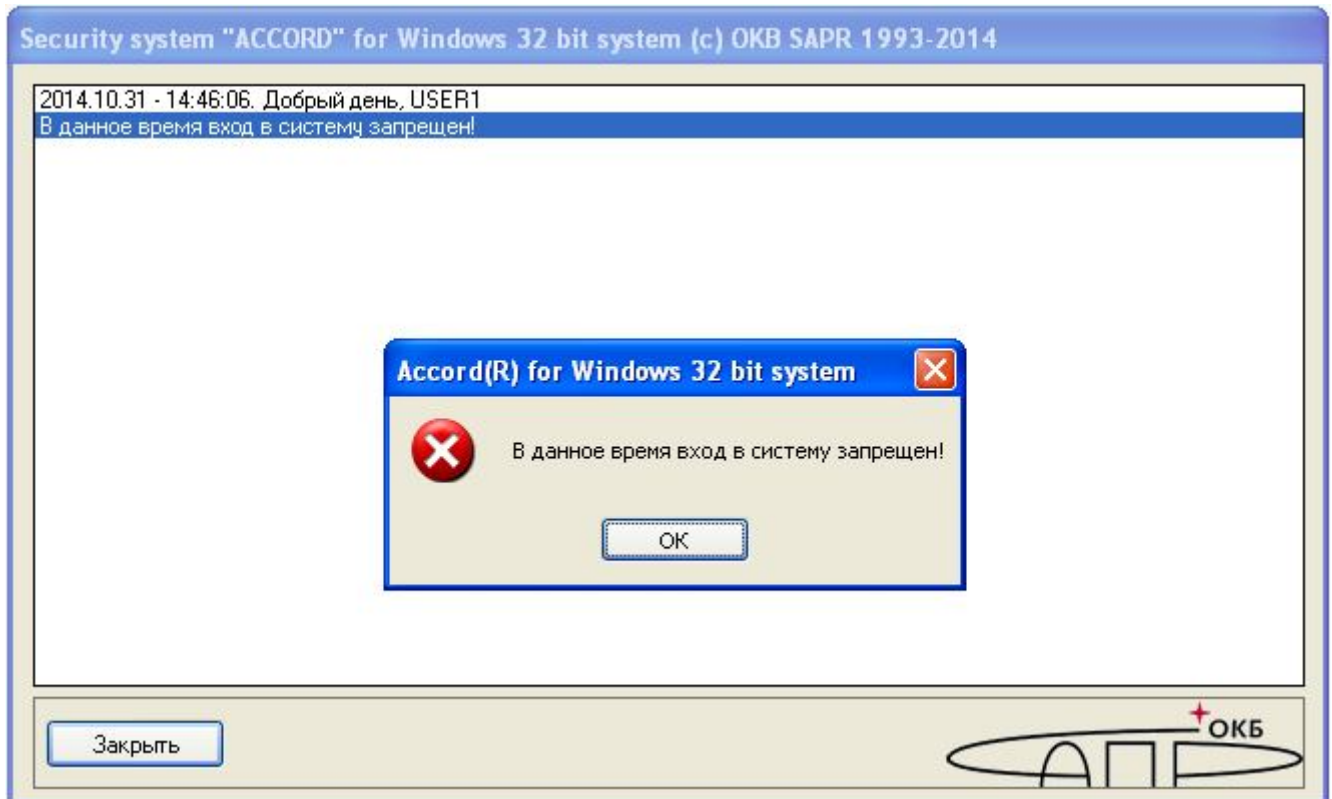
**Рисунок 4 – Оповещение о некорректном вводе пароля**

В таком случае необходимо нажать кнопку <Ok> в оповещении 4, затем повторить процедуру ввода пароля.

В случае если при регистрации пользователю не был назначен пароль, процедура аутентификации не выполняется, и после успешного выполнения процедуры идентификации начинается загрузка ОС.

### 2.1.3. Проверка ограничения на время входа в систему

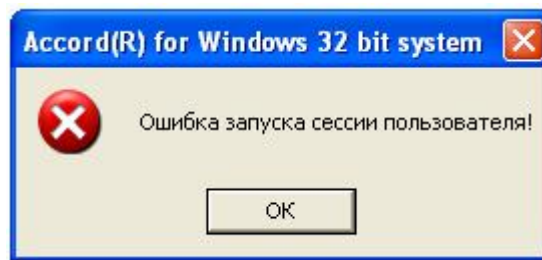
Администратор может установить временной интервал (по дням недели с дискретностью 0.5 часа), в который загрузка данного СВТ данным пользователем запрещена. Если для пользователя установлены такие ограничения, то при попытке загрузки в неположенное время после процедуры идентификации/аутентификации выводится сообщение (рисунок 5):



**Рисунок 5 – Ограничение доступа по времени**

По нажатии кнопки <Ok> в окне, показанном на рисунке 5, на экране появляется сообщение (рисунок 6), загрузка ОС при этом не производится.

11443195.509000.055 34

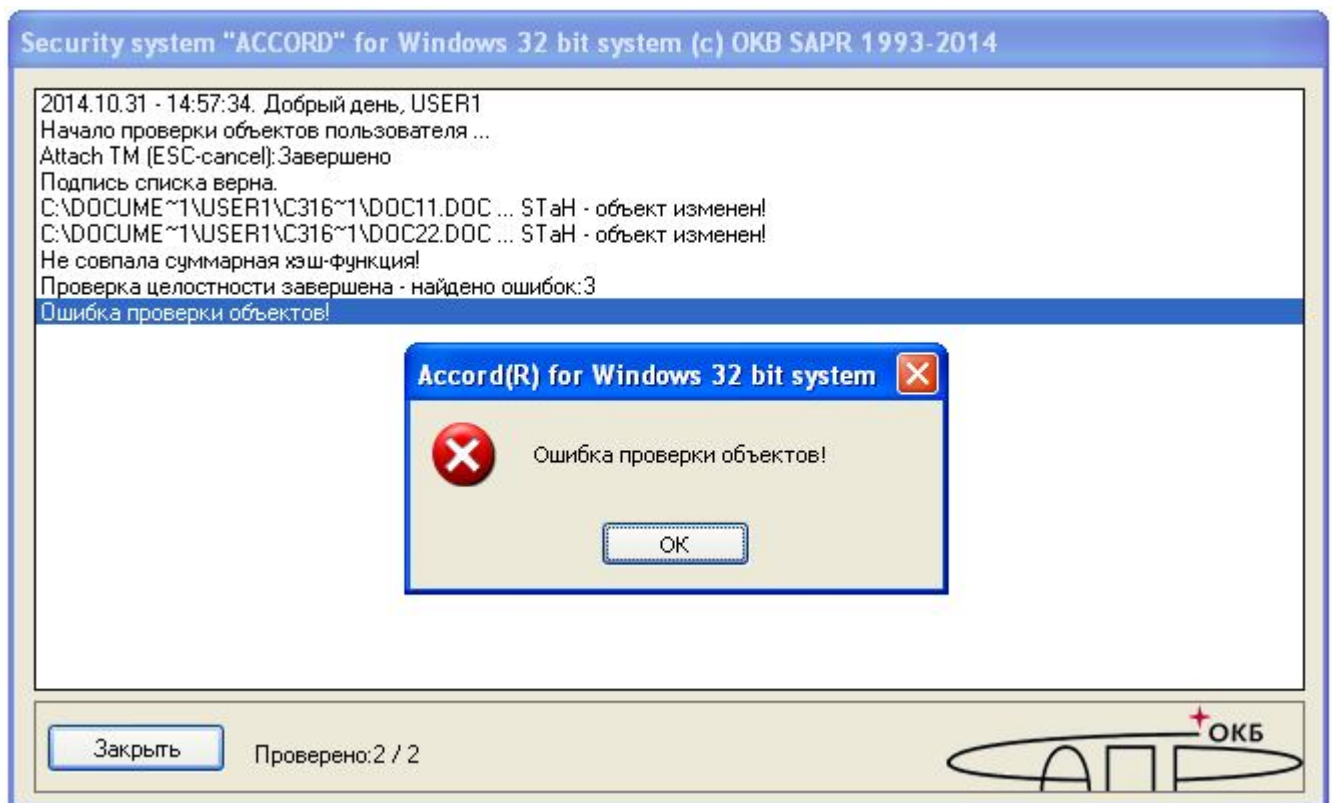
**Рисунок 6 – Ошибка запуска сессии**

#### 2.1.4. Проверка целостности файлов реестра, программ и данных

Данная процедура предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) обрабатываемых пользователем данных, программ, а также файлов реестра, если они поставлены на контроль целостности.

При проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным значением. Эти данные могут меняться в процессе эксплуатации СВТ.

В случае если нарушена целостность контролируемых файлов, то на экране появляется сообщение (рисунок 7) и загрузка ОС не производится.

**Рисунок 7 – Сообщение о нарушении целостности защищаемых объектов**

Загрузка будет возможна только после вмешательства администратора БИ (входа в систему с помощью его данных для идентификации).



11443195.509000.055 34

## **2.2. Работа пользователя в соответствии с функциональными обязанностями**

После выполнения контрольных процедур пользователь может приступить к работе, определяемой его функциональными обязанностями и правами доступа к ресурсам СВТ.

При регистрации пользователя для него создается функционально изолированная программная среда, которая позволяет контролировать права доступа пользователя к объектам доступа.

### **2.2.1. Проверка полномочий по доступу**

Выполняется при запуске пользователем какой-либо программы или при попытке получить доступ к какому-либо ресурсу. Средствами СПО «Аккорд» выполняется проверка полномочий пользователя, которая заключается в том, что в списке прав доступа пользователя осуществляется поиск описания данного ресурса.

Если в списке прав доступа пользователя разрешена работа с данной программой или файлом, то пользователь может легально работать в соответствии со своими функциональными обязанностями.

Если в списке прав доступа пользователя не разрешена работа с данной программой или файлом (или ограничен набор функций, которые может выполнить пользователь с данным ресурсом), то выводится стандартное сообщение операционной системы, например: «Файл не найден», «Невозможно удалить файл» и т. д.

### **2.2.2. Работа с хранителем экрана**

#### **Принудительное гашение экрана**

В СЗИ АККОРД процедура гашения экрана используется для временной блокировки компьютера по истечении установленной паузы в работе пользователя или с помощью «горячих» клавиш. Комбинацией клавиш <Ctrl><F12> пользователь может самостоятельно включить режим «*Screen-saver*» при кратковременном перерыве в работе. После включения хранителя экрана клавиатура и мышь блокируются.

**ВНИМАНИЕ!** В терминальном режиме, чтобы включить режим «*Screen-saver*» необходимо использовать комбинацию клавиш <Win><L>. После включения хранителя экрана клавиатура и мышь блокируются, на экране появляется сообщение «Предъявите идентификатор».

#### **Возобновление работы.**

Для возобновления работы на СВТ пользователь должен предъявить свои данные для идентификации и после того как система опознает их как подлинные, режим «*Screen-saver*» отключается и можно продолжить работу.

11443195.509000.055 34

### **2.3. Завершение работы и выход из системы**

Завершение работы прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения, описанном в соответствующих руководствах. Никаких специфических окон или сообщений «Аккорд-Win32 К» при этом не выводит. Перед завершением работы ОС выводится окно с заголовком «Комплекс Аккорд» и остается на экране, пока монитор разграничения доступа не завершит корректно свою работу.

11443195.509000.055 34

### 3. Сообщение программных средств СПО «Аккорд» и порядок действий пользователя по ним

При работе на СВТ, оснащенный СПО «Аккорд», могут возникать ситуации, при появлении которых выдаются различные сообщения. Текст сообщений, причины их появления и методы устранения проблем приведены в таблице 1.

**Таблица 1 – Сообщения программных средств СПО «Аккорд» и методы их устранения.**

Сообщение на экране	Причины появления сообщения	Порядок действий
«Ошибка запуска сессии пользователя»	Установлено ограничение на время входа в систему. Нарушена целостность защищаемых файлов	Вызвать администратора БИ
«В данное время вход в систему запрещен»	Для данного пользователя не разрешен вход в систему в данное время	Вызвать администратора БИ и уточнить разрешенное время работы
«Не зарегистрированный пользователь»	Не зарегистрированные данные для идентификации	Обратиться к администратору БИ для регистрации. Повторить процедуры идентификации / аутентификации.
«Проверить целостность объектов пользователя? (Y/N)»	Это сообщение означает, что администратор БИ установил пользователю опцию проверки целостности файлов <sup>1)</sup> , в соответствии с правилами настройки.	Пользователь должен осуществить выбор в соответствии со своими предпочтениями. (Рекомендуется периодически проводить проверку)
«Обновить контрольные суммы объектов пользователя? (Y/N)»	Это сообщение появляется, если пользователю установлен режим пересчета контрольных сумм файлов после завершения задачи пользователя с подтверждением, в соответствии с правилами настройки.	Пользователь может записать новое значение КС. Для этого необходимо выбрать [Y] и после появления сообщения: «Предъявите идентификатор, или ESC для отмены» нужно предъявить данные для идентификации
«Ошибка проверки объектов!»	Ошибка возникает, если объект, включенный в список контроля, недоступен.	Проверить правильность списка объектов контроля

<sup>1)</sup> Режим контроля целостности с подтверждением

## 11443195.509000.055 34

«Такую комбинацию символов недопустимо использовать в качестве пароля»	Это сообщение появляется в случае, если пользователь вводит комбинацию символов, которую легко подобрать (например, qwerty).	Ввести более сложную комбинацию символов
Не следует в качестве пароля использовать старый пароль или его часть	Это сообщение появляется в случае, если пользователь в качестве нового пароля вводит комбинацию символов (или ее часть) старого пароля	Ввести комбинацию символов, не совпадающую с комбинацией символов (или ее частью) старого пароля