ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
37222406.26.20.40.140.091 34 -ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win64 К»

РУКОВОДСТВО ОПЕРАТОРА (ПОЛЬЗОВАТЕЛЯ)

37222406.26.20.40.140.091 34

АННОТАЦИЯ

Руководство предназначено для конкретизации действий операторов (пользователей) при эксплуатации специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) (далее по тексту – СПО «Аккорд-Win64 K», «Аккорд-Win64 K», СПО «Аккорд», «Аккорд») и содержит описание способов использования средств защиты специального программного обеспечения «Аккорд-Win64 K», его интерфейса с пользователем в процессе обработки информации.

Перед эксплуатацией СПО «Аккорд-Win64 K» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов СПО «Аккорд-Win64 K» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ и его ресурсов.

СОДЕРЖАНИЕ

1. Назначение и краткая характеристика СПО «Аккорд-Win64 K»

Специальное программное обеспечение «Аккорд-Win64 K» предназначено для применения на ПЭВМ (рабочих станциях ЛВС) типа IBM PC, функционирующих под управлением ОС Windows 10 Professional, Windows Server 2012 Enterprise Edition R2, Windows Server 2016 Enterprise Edition, Windows Server 2019 (64-bit) или Windows 10 Professional (32- bit) 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-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) поставляется в составе:

1) Специальное ПО разграничения доступа в среде Windows 10 Professional, Windows Server 2012 Enterprise Edition R2, Windows Server 2016 Enterprise Edition (64-bit) или Windows 10 Professional (32- bit) - СПО «Аккорд-Win64 K», размещаемое на жестком диске СВТ при установке СПО «Аккорд».
2) Эксплуатационная документация[1].
3) Формуляр.

[1] Поставляется на диске с СПО разграничения доступа

2. Порядок работы на защищенном 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 времени входа в систему.

2.1.1. Процедура идентификации

При загрузке СВТ на экран выводится сообщение:

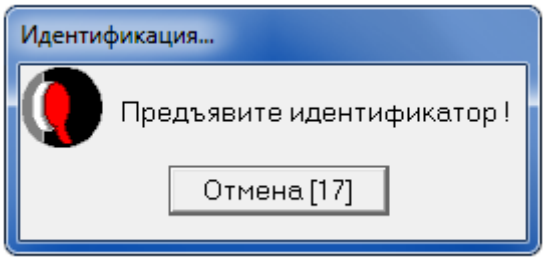

Рисунок 1 – Запрос данных для идентификации пользователя

В случае если для пользователя администратором установлен режим прохождения идентификации по клавиатуре, поверх данного окна выводится окно с запросом ввода ключевого слова, которое используется в качестве идентификатора для данной клавиатуры:

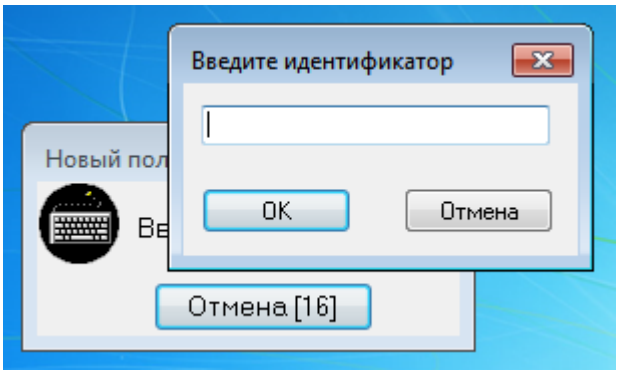

Рисунок 2 - Окно с запросом идентификатора для клавиатуры

Окно (рисунок 1) 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, на экране появляется сообщение:

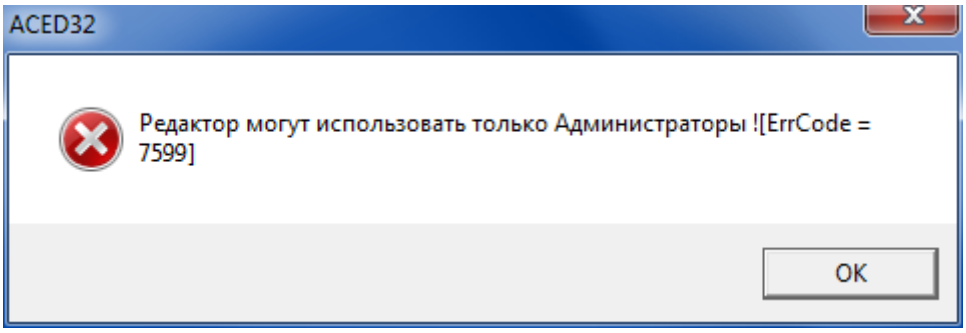

Рисунок 3 – Данные для идентификации не зарегистрированы

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

Если пользователь недостаточно плотно приложил ТМ-идентификатор к контактному устройству (при его использовании), то в верхней части окна запроса идентификатора пользователя (рисунок 1) появляется надпись «Чтение секретного ключа». В таком случае необходимо предъявить идентификатор еще раз.

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 4):

Рисунок 4 – Аутентификация пользователя

По этой команде пользователю необходимо набрать пароль, при этом символы пароля выводятся на экран в виде звездочек.

Если процедура аутентификации успешно завершилась, начинается загрузка ОС.

При неправильно введенном пароле на экран выводится оповещение (рисунок 5):

Рисунок 5 – Оповещение о некорректном вводе пароля

В таком случае необходимо нажать кнопку <OK> в оповещении 5, 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 времени 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 6):

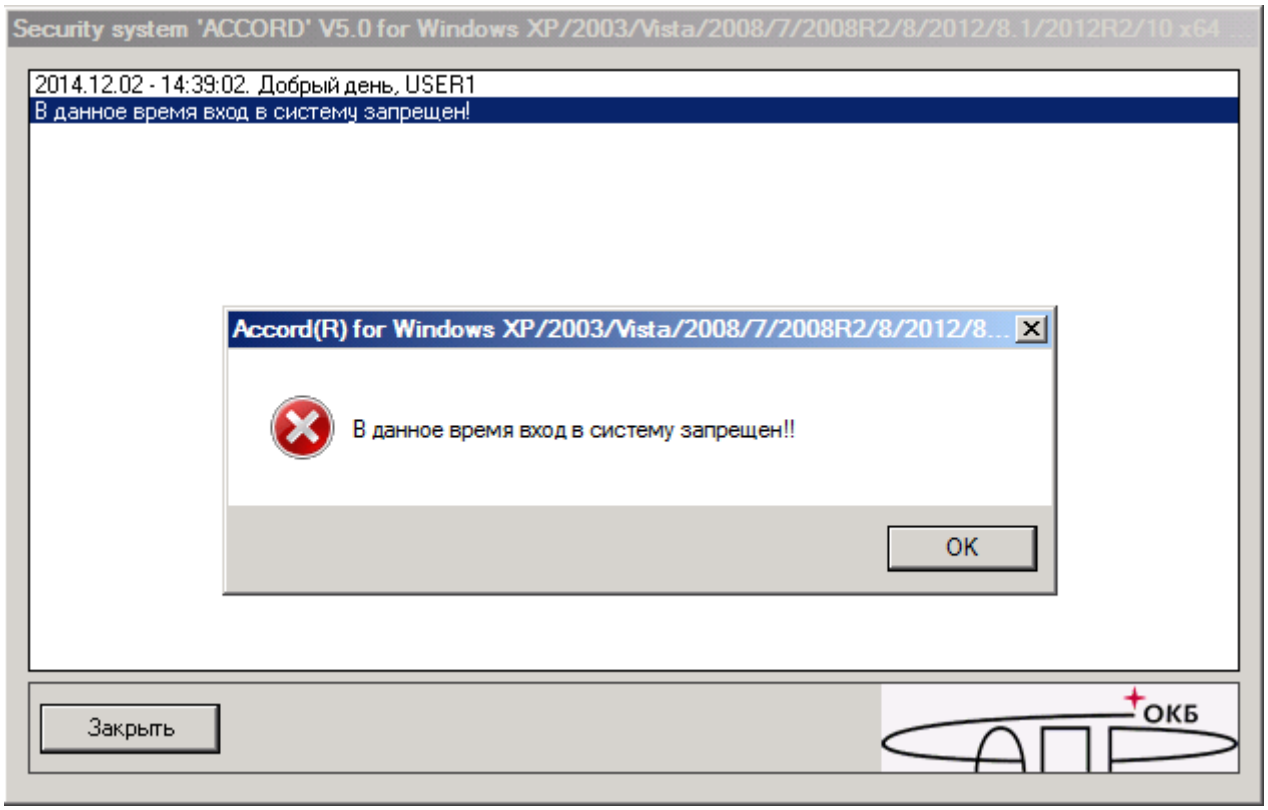

Рисунок 6 – Ограничение доступа по времени

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.

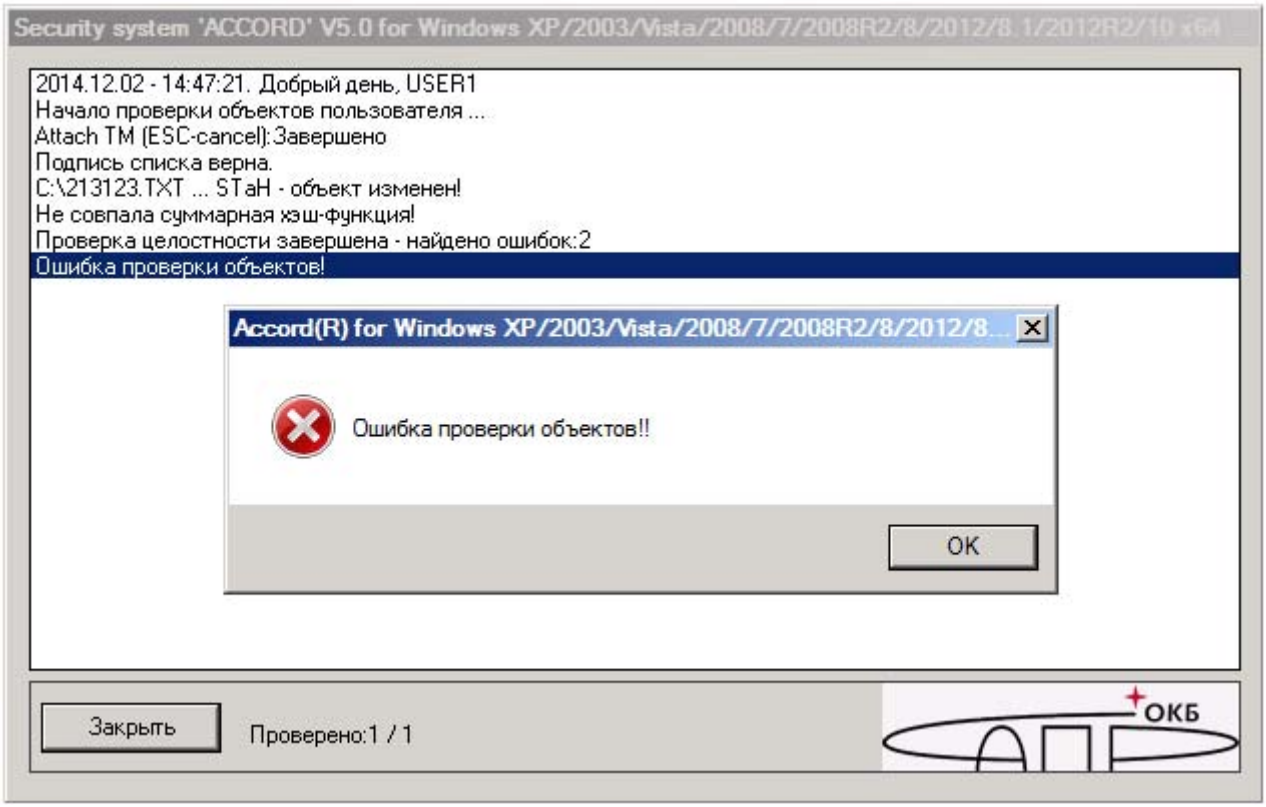

Рисунок 7 – Сообщение о нарушении целостности защищаемых объектов

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

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 СПО 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.

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 специфический окон или сообщений «Аккорд-Win64 K» 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.

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

При работе на СВТ, оснащенном 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 времени 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
«Незарегистрированный пользователь»	Незарегистрированные 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[2], 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
«Такую комбинацию символов недопустимо	Это сообщение появляется в случае,	Ввести более сложную комбинацию символов

[2)] Режим контроля целостности с подтверждением

Сообщение на экране	Причины появления сообщения	Порядок действий
использовать в качестве пароля»	если пользователь вводит комбинацию символов, которую легко подобрать (например, qwerty)	
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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Содержание изменения (обновления)	Дата	Примечание
1			
2			
3			
4			
5			
6			