



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

**Программно-аппаратный комплекс защищенного
хранения информации «Личный Секрет»
(версия 1.1)**

**Руководство пользователя
(оператора)**

11443195.4012.031-34

Листов 19

**Москва
2012**

АННОТАЦИЯ

Настоящий документ является руководством пользователя (оператора) программно-аппаратного комплекса «Личный Секрет» v.1.1 (далее по тексту – ПАК «Личный Секрет», либо «Личный Секрет», либо «Секрет»), предназначенного для защищенного хранения данных на отчуждаемом USB-носителе и исключающего возможность применения этого носителя на каких-либо иных компьютерах, кроме разрешенных владельцем.

В документе приведено описание использования основных целевых функций ПАК «Личный Секрет».

Особенности установки и управления комплексом приведены в документе «Руководство администратора» (11443195.4012.031-90).

В случае личного использования ПАК «Личный секрет» и Администратором, и Пользователем (оператором) «Секрета» является его владелец.

Перед установкой и эксплуатацией ПАК «Личный Секрет» рекомендуется внимательно ознакомиться с настоящим руководством.

Применение ПАК «Личный Секрет» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ (РС).

СОДЕРЖАНИЕ

1 Общие сведения	4
1.1 Состав и назначение ПАК «Личный Секрет»	4
1.2 Технические условия применения комплекса	4
1.3 Комплектность поставки ПАК «Личный Секрет»	5
2 Установка и настройка ПАК «Личный Секрет»	5
2.1 Установка ПО ПАК «Личный Секрет»	5
2.2 Удаление ПО ПАК «Личный Секрет»	5
2.3 Подключение СН	5
2.4 Установка системного драйвера СН	5
2.5 Начало работы	6
3 Управление ПАК «Личный Секрет»	6
3.1 Регистрация компьютера	6
3.2 Регистрация СН	6
3.3 Регистрация СН на другом компьютере	7
3.4 Аннулирование регистрации СН	7
3.5 Смена PIN-кода СН	8
3.6 Разблокирование СН	9
4 Применение ПАК «Личный Секрет»	10
4.1 Получение доступа к данным СН	10
4.2 Журнал регистрации событий	14
4.3 Контроль целостности ПО с помощью «Секретного Агента»	17
5 Перечень принятых сокращений и обозначений	19

1 Общие сведения

1.1 Состав и назначение ПАК «Личный Секрет»

Программно-аппаратный комплекс «Личный Секрет» включает:

- 1) специальный носитель «Личный Секрет» (СН, или «Секрет»);
- 2) программное обеспечение (ПО) рабочей станции (РС) «Секретный Агент»:
 - драйвер USB-устройства для работы в составе операционной системы (ОС);
 - драйвер-фильтр USB-устройств (запрещает доступ ко всем устройствам USB Mass Storage, кроме USB Mass Storage СН «Личный Секрет»);
 - приложение для управления доступом к данным СН.

Специальный носитель «Личный Секрет» представляет собой аппаратный модуль, выполненный в форм-факторе флеш-диска с интерфейсом USB, предназначенный для защищенного хранения информации Пользователя.

Программное обеспечение «Секретный Агент» предназначено для аутентификации (опознавания) «Секрета» на данной РС и передачи аутентификационных данных Пользователя в «Секрет» для получения доступа к внутренней памяти флеш-диска со стороны РС.

ПО «Секретный Агент» устанавливается на жесткий диск персонального компьютера и требует для установки примерно 20 Мб дискового пространства.

ПАК «Личный Секрет» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64).

ПАК «Личный Секрет» предназначен для обеспечения недоступности информации, размещенной на СН, в случае его кражи, потери или применения на компьютере, не входящем в число разрешенных владельцем. Доступ к защищаемой информации предоставляется только на тех компьютерах, на которых конкретный «Секрет» был зарегистрирован его владельцем, и только после ввода PIN-кода, известного владельцу. Незарегистрированный СН не обнаруживается операционной системой компьютера как устройство типа mass-storage и его PIN-код не запрашивается.

1.2 Технические условия применения комплекса

Для работы с ПАК «Личный Секрет» необходим следующий минимальный набор технических и программных средств:

- установленная ОС Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64);
- свободный разъем USB;
- объем дискового пространства для размещения программного обеспечения на жестком диске РС – 20 Мбайт.

1.3 Комплектность поставки ПАК «Личный Секрет»

ПАК «Личный Секрет» поставляется в составе:

- специальный носитель «Личный Секрет»;
- CD со специальным ПО «Личный Секрет», руководствами пользователя и администратора;
- гарантийный талон;
- комплект упаковки.

2 Установка и настройка ПАК «Личный Секрет»

2.1 Установка ПО ПАК «Личный Секрет»

До начала использования СН на жесткий диск РС Администратором должно быть установлено программное обеспечение «Секретный Агент». В случае личного использования «Секрета» Пользователь осуществляет данную процедуру самостоятельно (см. подраздел «Установка ПО ПАК «Личный Секрет» «Руководства администратора» (11443195.4012.031-90).

2.2 Удаление ПО ПАК «Личный Секрет»

При необходимости ПО ПАК «Личный Секрет» можно удалить. Процедура удаления ПО ПАК «Личный Секрет» осуществляется Администратором. В случае личного использования «Секрета» Пользователь осуществляет данную процедуру самостоятельно (см. подраздел «Удаление ПО ПАК «Личный Секрет» «Руководства администратора» (11443195.4012.031-90).

2.3 Подключение СН

Подключение осуществляется установкой СН в свободный USB-разъем системного блока РС¹.

2.4 Установка системного драйвера СН

После установки на жесткий диск ПО ПАК «Личный Секрет» при первом подключении устройства «Личный Секрет» к USB-порту необходимо выполнить установку системного драйвера СН. Установка системного драйвера СН выполняется Администратором. В случае личного использования «Секрета» Пользователь осуществляет данную процедуру самостоятельно (см. подраздел «Установка системного драйвера СН» «Руководства администратора» (11443195.4012.031-90).

¹ В случае неудобного расположения USB-порта на системном блоке компьютера рекомендуется использовать удлинительный кабель USB, это предохранит «Секрет» (а также и все другие применяемые USB-устройства) от поломок и облегчит его подключение и отключение.

2.5 Начало работы

До начала использования «Секрета» на РС должно быть установлено и запущено ПО ПАК «Личный Секрет» (см. подраздел 2.1), выполнено подключение СН (см. подраздел 2.3), произведена установка системного драйвера СН (см. подраздел 2.4) и выполнена регистрация компьютера (см. подраздел 3.1).

Следующий шаг – процедура первичной регистрации СН, в результате которой формируется PIN-код СН (подробнее об этом см. в разделе 3.2). Эта процедура выполняется один раз, при применении «Секрета» в обычном режиме повторять ее не требуется.

PIN-код требуется для получения доступа к данным, хранящимся в СН.

После выполнения процедуры первичной регистрации данный «Секрет» связывается с данным компьютером, который становится для него «первичным».

Следует запомнить или надежно сохранить PIN-код СН. В случае необходимости (например, при компрометации PIN-кода) PIN-код может быть изменен. Для выполнения этой операции потребуется знание старого значения PIN-кода (подробнее см. 3.5).

В случае трех последовательных неудачных попыток ввода PIN-кода СН блокируется. Процедура разблокирования проводится Администратором (см. 3.6). В результате выполнения операции разблокирования формируется новый PIN-код.

После успешной регистрации по предъявлению корректного PIN-кода может быть получен доступ к данным СН (содержимому флеш-диска). Подробнее об этом см. раздел 4.

3 Управление ПАК «Личный Секрет»

3.1 Регистрация компьютера

Регистрация компьютера в «Секретном Агенте» производится Администратором при первом запуске ПО ПАК «Личный Секрет».

В случае личного использования ПАК «Личный Секрет» Пользователь самостоятельно осуществляет регистрацию компьютера в соответствии с информацией подраздела «Регистрация компьютера» «Руководства администратора» (11443195.4012.031-90).

После успешного выполнения процедуры регистрации компьютера можно начать регистрацию СН «Личный Секрет».

3.2 Регистрация СН

Регистрация «Секрета» производится Администратором, который выдает Пользователю уже зарегистрированный «Секрет» и PIN-код к нему.

После этого Пользователь должен сменить PIN-код на тот, что неизвестен Администратору (см. п. 3.5).

PIN-код Секрета задается опционально. При желании, PIN-код Секрету можно не назначать (не рекомендуется).

ВНИМАНИЕ! Настройка политики использования PIN-кода Секрета может быть выполнена только при проведении процедуры первичной регистрации СН. В рамках выполнения иных операций изменить политику использования PIN-кода невозможно.

В случае личного использования ПАК «Личный Секрет» Пользователь самостоятельно осуществляет регистрацию «Секрета» в соответствии с информацией подраздела «Регистрация СН» «Руководства администратора» (11443195.4012.031-90).

ВНИМАНИЕ! Пользователь должен запомнить или надежно сохранить PIN-код и код регистрации СН, знание которых позволяет получить доступ к соответствующим функциям ПАК «Личный Секрет».

Пользователь должен помнить о необходимости сохранения этих данных недоступными третьим лицам!

3.3 Регистрация СН на другом компьютере

Возможна ситуация, когда требуется доступ к защищенным данным СН «Личный Секрет» на других РС (отличных от РС, на которой выполнена первичная регистрация). Для расширения множества доверенных РС предусмотрена процедура повторной регистрации СН. Выполнение процедуры повторной регистрации выполняется Администратором.

В случае личного использования ПАК «Личный Секрет» Пользователь самостоятельно осуществляет повторную регистрацию «Секрета» в соответствии с информацией подраздела «Регистрация СН на другом компьютере» «Руководства администратора» (11443195.4012.031-90).

3.4 Аннулирование регистрации СН

Процедура аннулирования регистрации СН предназначена для исключения РС из списка тех, на которых возможен доступ к данным, хранящимся в «Секрете». Использование этого механизма позволяет контролировать список РС, на которых может быть осуществлен доступ к содержимому «Секрета».

После выполнения процедуры аннулирования регистрации доступ к данному «Секрету» на данном ПК станет невозможен до выполнения процедуры регистрации заново.

Необходимо своевременно выполнять процедуру аннулирования регистрации СН на РС, на которых не требуется доступ к содержимому СН.

Процедуру аннулирования регистрации выполняет Администратор. В случае личного использования ПАК «Личный Секрет» Пользователь самостоятельно осуществляет аннулирование регистрации «Секрета» в

соответствии с информацией подраздела «Аннулирование регистрации СН» «Руководства администратора» (11443195.4012.031-90).

3.5 Смена PIN-кода СН

Если Пользователь СН считает PIN-код скомпрометированным, он может сменить действующий PIN-код на новый. При этом СН должен быть подключен к компьютеру. Для смены PIN-кода нужно в основном окне «Секретного Агента» выбрать из списка нужный СН и нажать кнопку <Сменить PIN-код>.

В случае если при выполнении процедуры первичной регистрации СН установлена политика, в соответствии с которой PIN-код Секрета не используется, кнопка <Сменить PIN-код> недоступна. Политика использования PIN-кода Секрета может быть изменена только в рамках проведения процедуры первичной регистрации СН (см. также подраздел 3.2).

ВНИМАНИЕ! Во время выполнения операции смены PIN-кода не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

В появившемся окне следует ввести старый PIN-код, полученный Пользователем при регистрации данного СН.

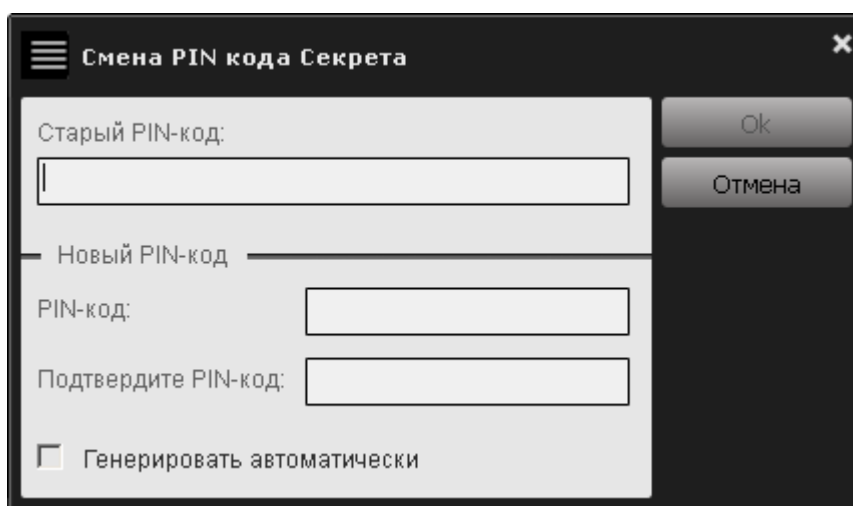


Рисунок 1 - Окно для смены PIN-кода

Пользователь может задать новый PIN-код самостоятельно или сгенерировать его автоматически с помощью установки флага <Генерировать> (рисунок 1).

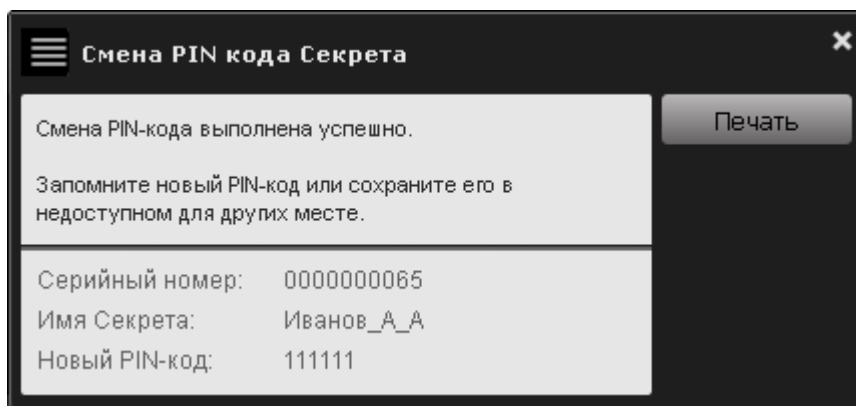


Рисунок 2 - Сообщение об успешной смене PIN-кода

Далее в информационном окне выводится сообщение об успешной смене PIN-кода (рисунок 2).

ВНИМАНИЕ! Пользователь должен запомнить или надежно сохранить PIN-код СН, знание которого позволяет получить доступ к соответствующим функциям ПАК «Личный Секрет».

В случае ввода неправильного старого или неверного подтверждения нового PIN-кода на экран выводится окно, показанное на рисунке 3.

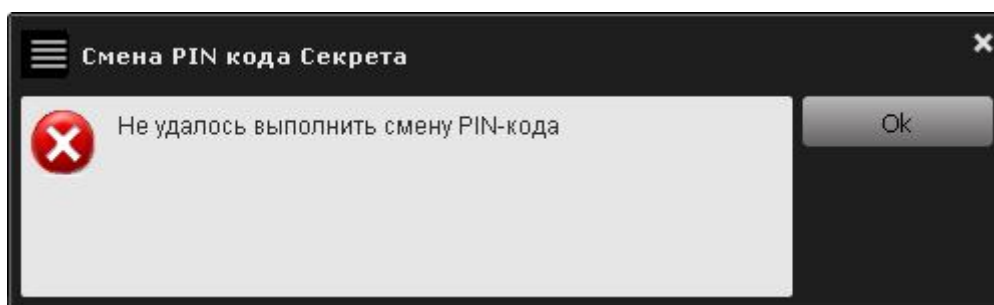


Рисунок 3 - Оповещение об ошибке в ходе смены PIN-кода

3.6 Разблокирование СН

В случае трех последовательных неудачных попыток ввода PIN-кода СН блокируется и на экран выводится соответствующее сообщение (рисунок 4).

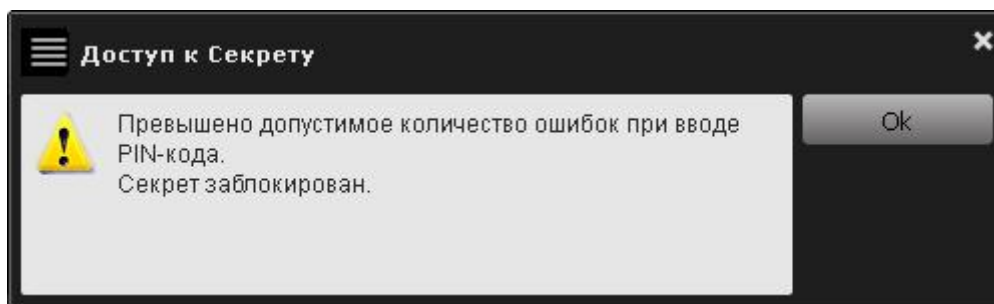


Рисунок 4 - Оповещение о блокировке СН

При этом статус СН в главном окне «Секретного Агента» изменяется на <Заблокирован> и единственной доступной операцией становится <Разблокировать> (рисунок 5).

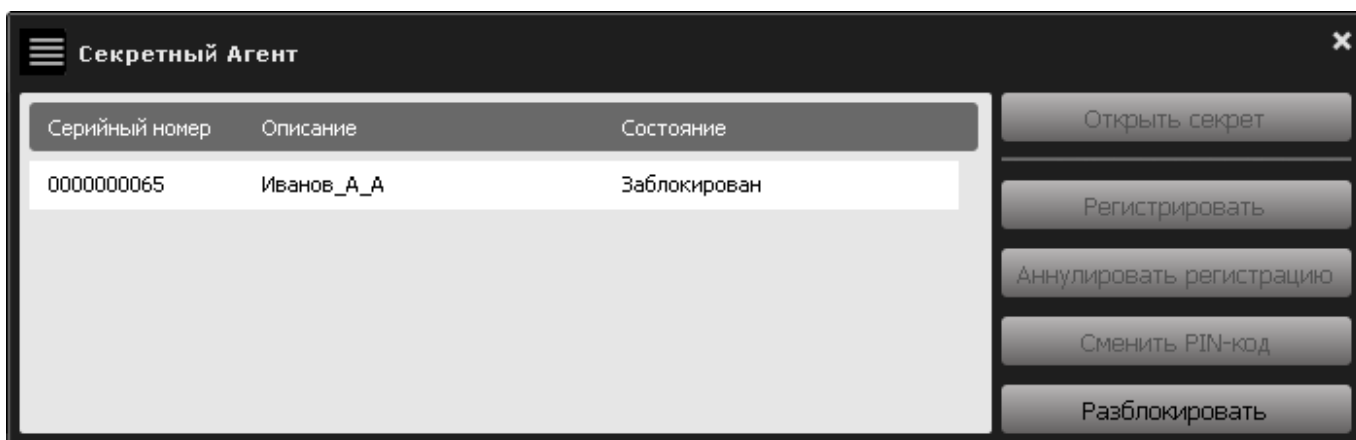


Рисунок 5 - Главное окно приложения «Секретный Агент». Изменение статуса после блокировки СН

Процедура разблокирования «Секрета» описана в подразделе «Разблокирование СН» «Руководства администратора» (11443195.4012.031-90). В случае корпоративного применения разблокирование «Секрета» может быть выполнено только с привлечением Администратора.

4 Применение ПАК «Личный Секрет»

«Секрет» используется точно так же, как и обыкновенный USB-накопитель. Отличие состоит только в процедуре получения доступа к данным, хранящимся в «Секрете».

4.1 Получение доступа к данным СН

После установки комплекта ПО ПАК «Личный Секрет» (см. раздел 2) при загрузке ОС производится автоматический запуск приложения «Секретный Агент», предназначенного для управления доступом к данным СН. При этом в трее появляется соответствующий значок (рисунок 6). «Секретный Агент» также может быть запущен вручную (например, если он был по каким-либо причинам закрыт) посредством выбора пункта меню Пуск→Программы→Личный Секрет→Секретный Агент.

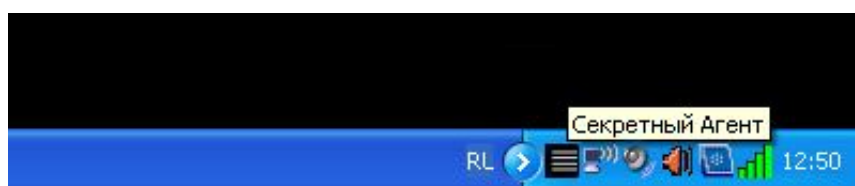


Рисунок 6 - Значок приложения «Секретный Агент» в трее

При первом запуске ПО ПАК «Личный Секрет» следует выполнить процедуру регистрации компьютера (см. «Руководство администратора» (11443195.4012.031-90)).

Для получения доступа к данным, хранящимся в «Секрете», необходимо убедиться в том, что приложение «Секретный Агент» запущено. СН необходимо подключить к USB-порту компьютера – так же, как любое USB-устройство. Если «Секрет» ранее был зарегистрирован на этом компьютере, после его подключения на экран автоматически выводится окно с запросом PIN-кода (рисунок 7). В появившемся окне следует ввести PIN-код, сформированный на этапе первичной регистрации СН (см. подраздел 3.2), выданный Администратором или полученный в результате смены PIN-кода (см. подраздел 3.5).

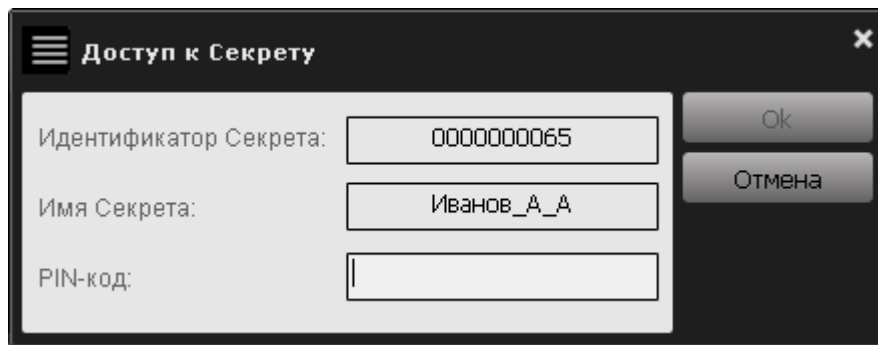


Рисунок 7 - Окно приложения «Секретный Агент» для ввода PIN-кода

При нажатии кнопки <OK> СН производит проверку введенного PIN-кода и в зависимости от ее результата предоставляет доступ к данным СН или отказывает в доступе.

ВНИМАНИЕ! Во время выполнения операции получения доступа не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

В случае если PIN-код введен правильно, на экран выводится информационное сообщение (рисунок 8) и СН предоставляет доступ к данным. Работать с данными при этом можно точно так же, как в случае с обычным USB флеш-накопителем («флешкой»).

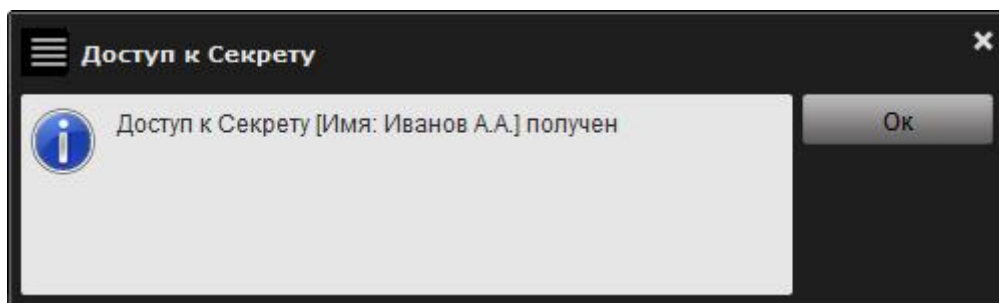


Рисунок 8 - Сообщение об успешном завершении процедуры получения доступа

В противном случае на экран выводится сообщение об отказе в получении доступа (рисунок 9).

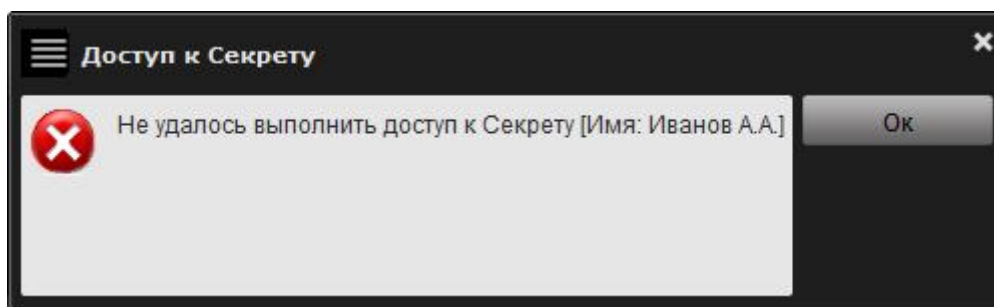


Рисунок 9 - Сообщение об отказе в получении доступа

ВНИМАНИЕ! В случае трех подряд неудачных попыток ввода PIN-кода СН блокируется. Для разблокирования СН необходимо знание кода регистрации (см. «Руководство администратора» (11443195.4012.031-90)), при корпоративном использовании в случае блокировки «Секрета» необходимо обратиться к Администратору.

Если по каким-то причинам уже после подключения «Секрета» к компьютеру необходимо отложить процедуру получения доступа к его данным, можно нажать кнопку <Отмена> (рисунок 7) и выполнить ее позднее описанным ниже образом.

Главное окно приложения «Секретный Агент» может быть активировано по двойному щелчку левой кнопкой мыши на значке в трее (рисунок 6). Внешний вид главного окна приведен на рисунке 10.

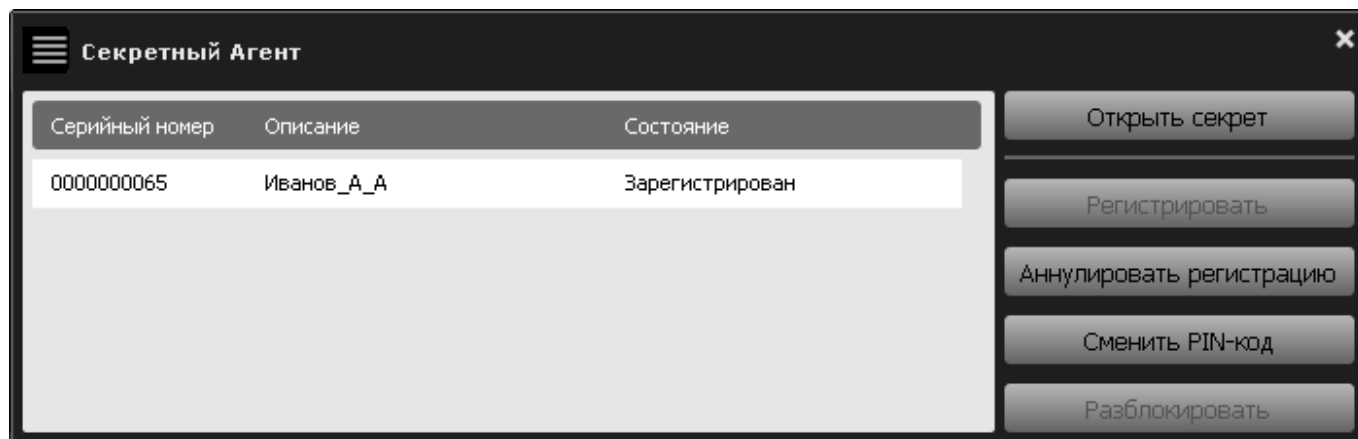


Рисунок 10 - Главное окно приложения «Секретный Агент»

Главное окно «Секретного Агента» содержит список подключенных СН с указанием имени, серийного номера и статуса. Доступ к данным в «Секрете» можно получить, выбрав соответствующий «Секрет» в списке и нажав кнопку <Открыть Секрет>.

Кнопка <Открыть Секрет> неактивна (и, следовательно, невозможен доступ к данным в «Секрете») в том случае, если СН не зарегистрирован на данной РС (на это указывает статус «Не зарегистрирован»). Подробнее о процедуре регистрации СН см. «Руководство администратора» (11443195.4012.031-90).

После нажатия кнопки <Открыть Секрет> появляется окно с предложением ввода PIN-кода, показанное на рисунке 7. Главное окно «Секретного Агента» может быть скрыто посредством нажатия кнопки <Заккрыть>.

ВНИМАНИЕ! После завершения работы с Секретом во избежание возможной потери данных необходимо выполнять процедуру «Безопасного извлечения устройства»!

Оперативное выполнение функций «Секретного Агента» может быть осуществлено из контекстного меню приложения, вызываемого по щелчку правой кнопки мыши на значке в трее (рисунок 11).

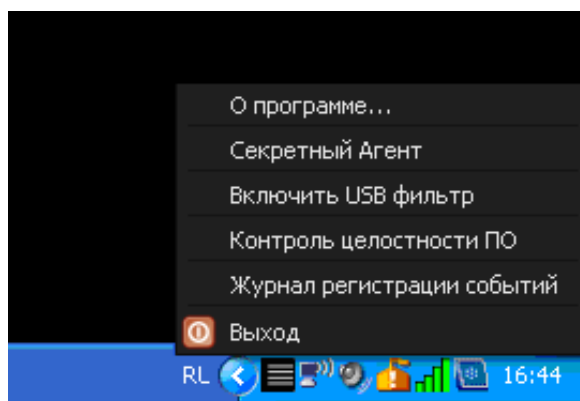


Рисунок 11 - Контекстное меню приложения «Секретный Агент»

ВНИМАНИЕ! При работе в ОС Windows 7 для того, чтобы контекстное меню «Секретного Агента» было доступно полностью, необходимо запускать «Секретный Агент» с правами администратора («Run as Administrator»).

Контекстное меню «Секретного Агента» содержит:

- пункт для вызова окна, содержащего информацию о «Секретном Агенте»;
- пункт для вызова главного окна «Секретного Агента»;
- пункт включения/выключения фильтра USB устройств (если «Секретный Агент» запущен под учетной записью Пользователя, входящего в группу «Администраторы»);
- пункт контроля целостности ПО (подробнее о контроле целостности ПО см. в подразделе 4.3);
- пункт для вызова журнала регистрации событий (подробнее о журнале регистрации событий см. в подразделе 4.2);
- пункт для завершения работы приложения «Секретный Агент».

При выборе в контекстном меню пункта <О программе...> на экран выводится информационное окно приложения «Секретный Агент», содержащее сведения об используемой версии ПАК «Личный Секрет», а также контактные данные службы технической поддержки.

При выборе в контекстном меню пункта <Секретный Агент> на экране отображается главное окно приложения «Секретный Агент».

При выборе в контекстном меню пункта <Включить USB фильтр> запрещается использование в системе всех устройств USB Mass Storage за исключением устройств «Секрет». Следует отметить, что при включенном USB-фильтре в перечне устройств системы могут отображаться записи о подключенных устройствах USB Mass Storage, не являющихся устройствами «Секрет»; при этом запуск таких устройств и получение доступа к хранящимся на них данных невозможен. Фильтр можно отключить, выбрав в контекстном меню пункт <Выключить USB фильтр>.

ВНИМАНИЕ! После включения USB фильтра на PC уже подключенные устройства USB Mass Storage, не относящиеся к устройствам «Секрет», остаются доступными. Доступ к этим устройствам будет запрещен после их переподключения на PC.

Работа приложения «Секретный Агент» может быть завершена посредством выбора в контекстном меню пункта <Выход>.

4.2 Журнал регистрации событий

Для отслеживания процесса работы с «Секретами» все производимые действия с СН, зарегистрированными на данной PC, записываются в журнал регистрации событий, окно просмотра которого показано на рисунке 12.

Работа с журналом может быть начата посредством выбора пункта «Журнал регистрации событий» из контекстного меню приложения «Секретный Агент», вызываемого по щелчку правой кнопки мыши на значке в трее (рисунок 11).

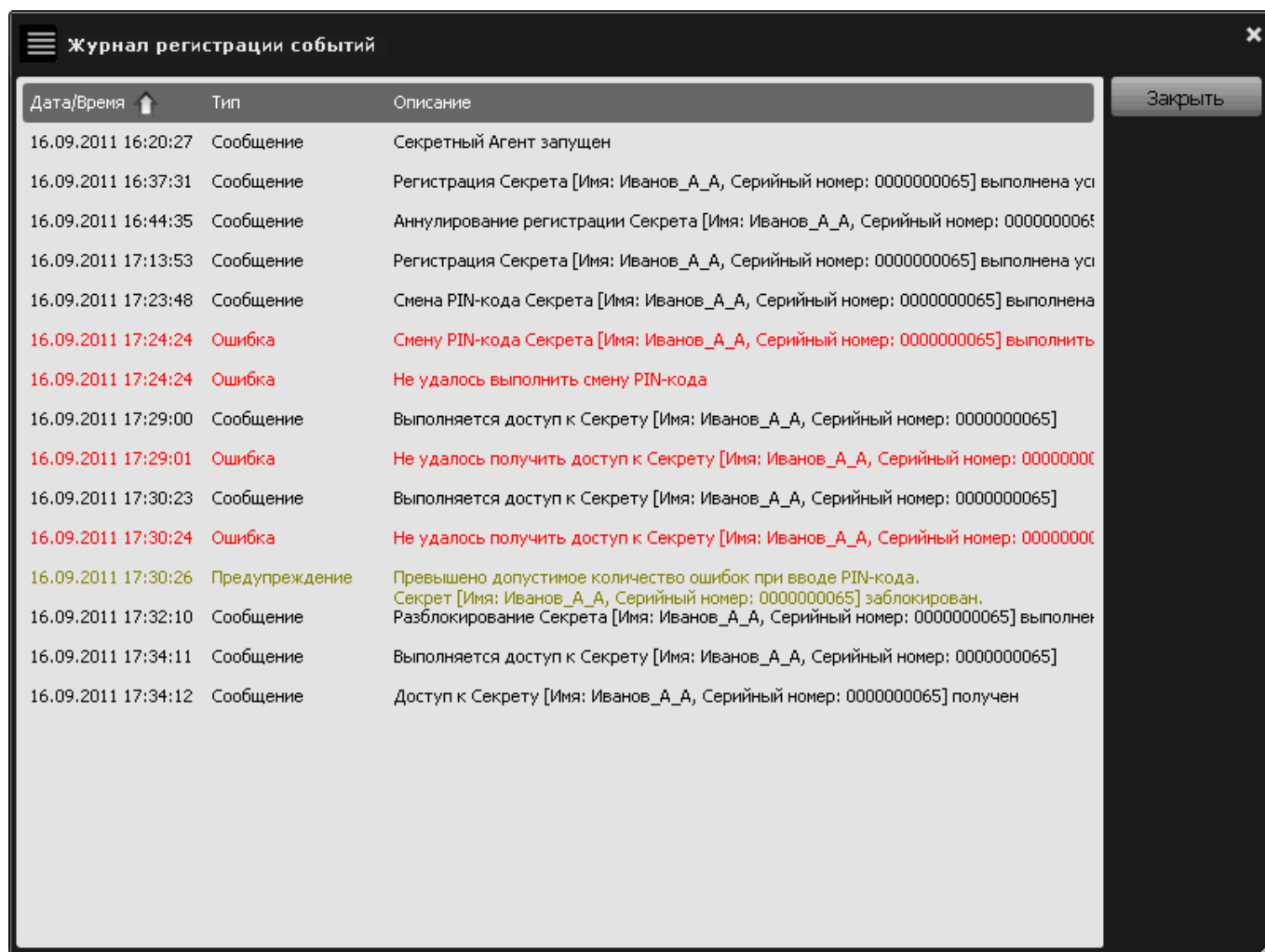


Рисунок 12 – Окно просмотра журнала регистрации событий

Окно просмотра журнала регистрации событий содержит информацию о событиях, зафиксированных в процессе работы пользователя с СН «Личный Секрет» на данной РС.

Имеется возможность упорядочения списка для упрощения поиска необходимых событий. Упорядочение списка может быть выполнено по следующим параметрам:

1) «Дата/Время» – параметр для упорядочения событий по дате/времени (рисунок 12);

2) «Тип» – параметр для упорядочения по типу событий, зафиксированных при работе с СН. Фиксируемые события могут принадлежать одной из следующих категорий: сообщение, ошибка, предупреждение (рисунок 13);

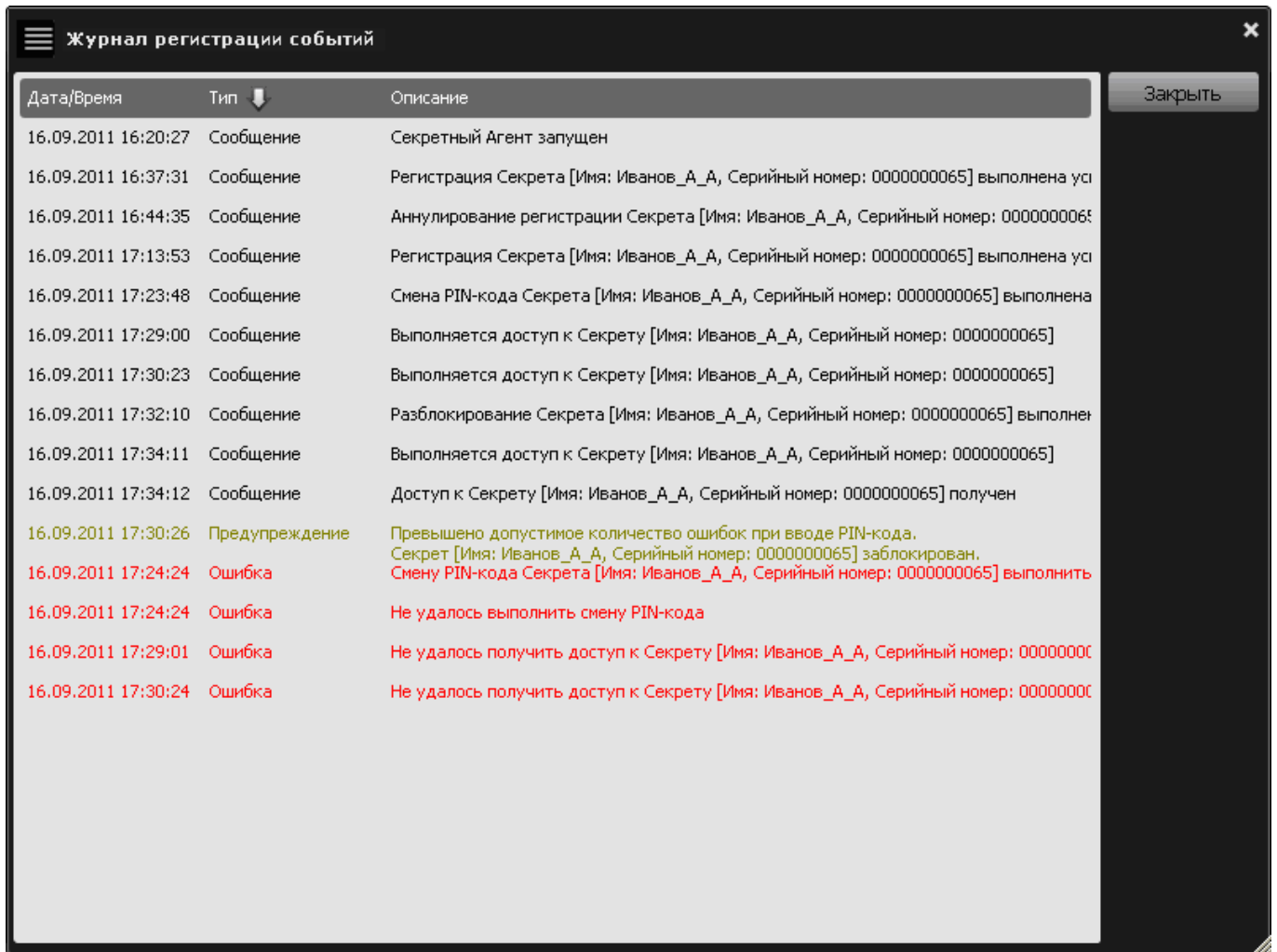


Рисунок 13 - Окно просмотра журнала регистрации событий со списком событий, упорядоченных по типу

3) «Описание» – данный параметр позволяет упорядочить список событий по их описанию в алфавитной последовательности (рисунок 14).

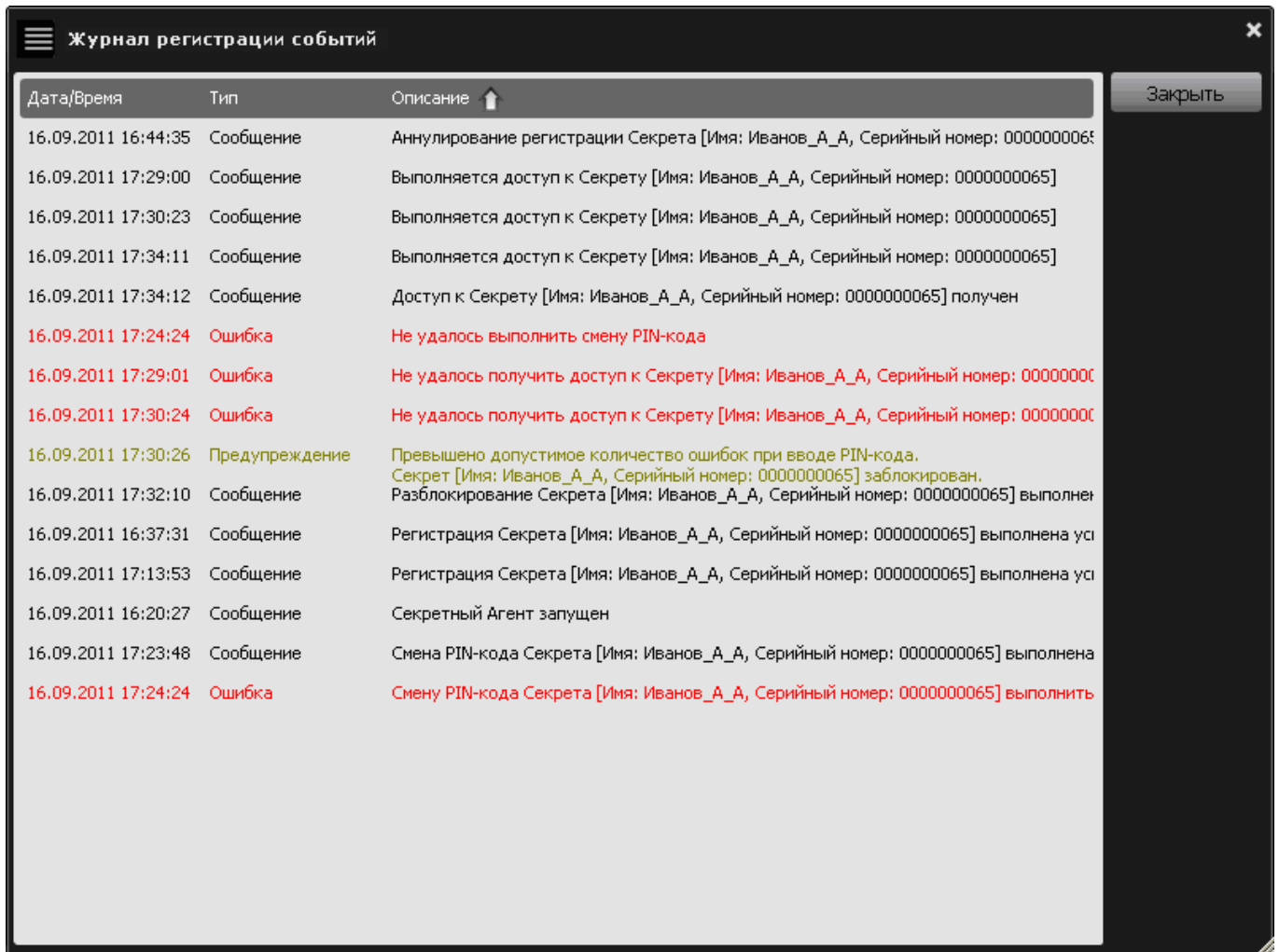


Рисунок 14 - Окно просмотра журнала регистрации событий со списком событий, отсортированных по описанию

4.3 Контроль целостности ПО с помощью «Секретного Агента»

Для отслеживания возможного вмешательства в логику работы ПО ПАК «Личный Секрет» предусмотрена процедура контроля целостности ПО.

Процедура контроля целостности ПО ПАК «Личный Секрет» может быть запущена посредством выбора пункта «Контроль целостности ПО» из контекстного меню приложения «Секретный Агент», вызываемого по щелчку правой кнопки мыши на значке в трее (рисунок 15).

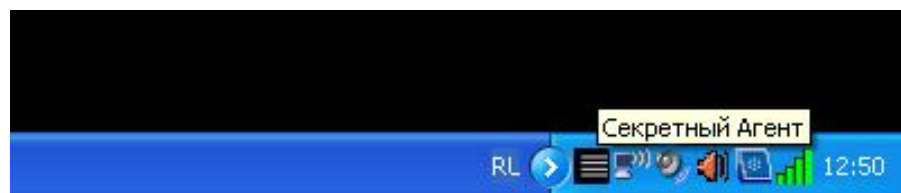


Рисунок 15 - Значок приложения «Секретный Агент» в трее

Начнется проверка целостности установленного ПО ПАК «Личный Секрет», в процессе которой происходит сравнение контрольных сумм установленных файлов с эталонными контрольными суммами.

После завершения процедуры контроля целостности ПО на экран выводится сообщение о завершении проверки контрольных сумм файлов ПО ПАК «Личный Секрет» (рисунок 16).

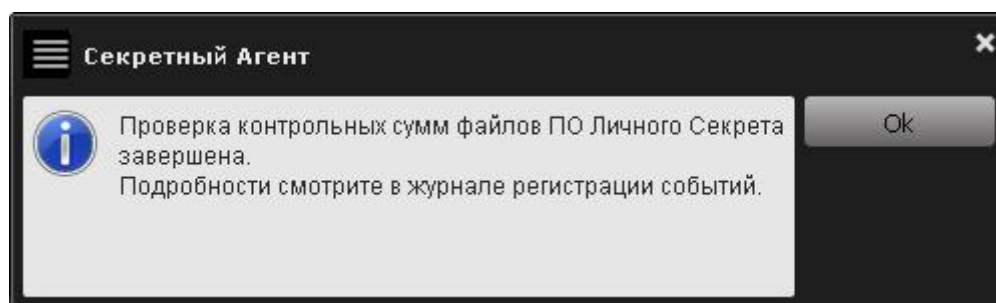


Рисунок 16 – Сообщение о завершении проверки целостности ПО ПАК «Личный Секрет»

Результаты проверки фиксируются в журнале регистрации событий, окно которого представлено на рисунке 17.

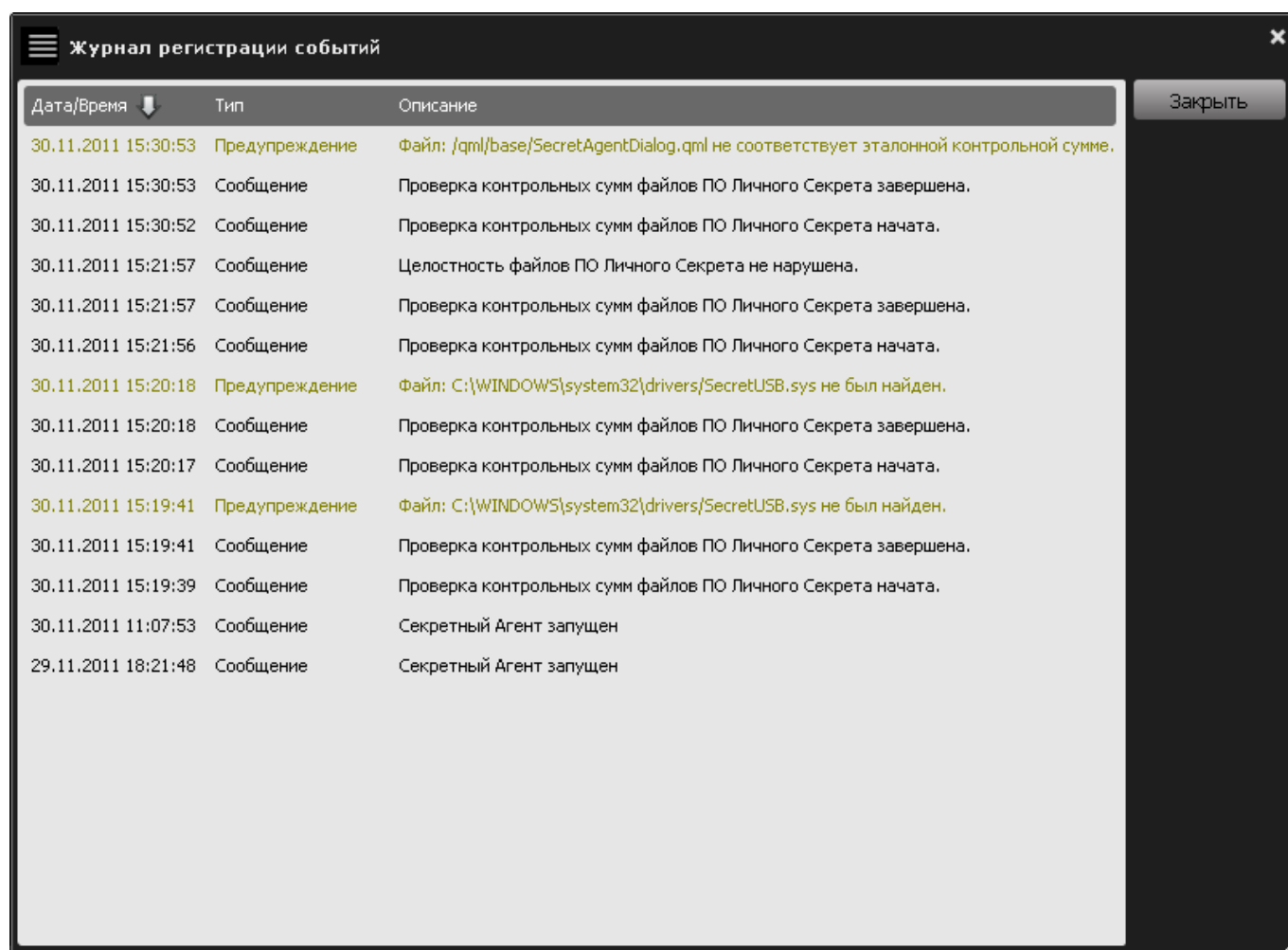


Рисунок 17 - Окно просмотра журнала регистрации событий со списком событий, связанных с контролем целостности ПО

Если в процессе проверки все контрольные суммы файлов ПО совпали с эталонными, то в окно просмотра журнала регистрации событий выводится сообщение о том, что целостность файлов ПО не нарушена. Если контрольная сумма какого-либо файла ПО не совпала с эталонной, то в журнал регистрации событий выводится предупреждение о несоответствии этого файла эталонной контрольной сумме. Если в процессе проверки какой-либо файл не был найден, в окно просмотра журнала регистрации событий выводится соответствующее сообщение (рисунок 17).

В случае нарушения целостности файлов ПО следует обратиться к Администратору Секрета.

5 Перечень принятых сокращений и обозначений

ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СН	Специальный носитель