

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

11443195.4012.031-90

Листов 35

Москва 2012

аннотация

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

ПАК «Личный секрет» предназначен для личного использования, и в этом случае его владелец одновременно является и Пользователем (оператором), и Администратором «Секрета». При корпоративном же использовании функции Администратора ПАК «Секрет» должны выполняться специально назначенным должностным лицом, имеющим необходимые знания и полномочия.

В документе приведены особенности установки, настройки и те из функций, которые связаны с администрированием ПАК «Личный Секрет».

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.

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»	11
	2.3 Контроль целостности ПО ПАК «Личный Секрет»	11
	2.4 Подключение СН	14
	2.5 Установка системного драйвера СН	14
	2.6 Начало работы	17
3	Управление ПАК «Личный Секрет»	18
	3.1 Регистрация компьютера	18
	3.2 Регистрация СН	19
	3.3 Регистрация СН на другом компьютере	24
	3.4 Аннулирование регистрации СН	26
	3.5 Смена PIN-кода CH	27
	3.6 Разблокирование СН	29
4	Рекомендации по организации безопасного применения ПАК	
	«Личный Секрет»	31
	4.1 Общие сведения	31
	4.2 Установка входа пользователя в систему с обязательным вводом пароля	31
	4.3 Включение режима автоматической блокировки экрана	32
5	Рекомендации по применению «Личного Секрета» в	
	корпоративной среде	34
6	Перечень принятых сокращений и обозначений	35

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 (OC);

– драйвер-фильтр USB-устройств (запрещает доступ ко всем устройствам USB Mass Storage, кроме USB Mass Storage CH «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 Мb дискового пространства.

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

ПАК «Личный Секрет» предназначен для обеспечения недоступности информации, размещенной на CH, 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 CH не обнаруживается операционной системой компьютера как устройство типа massstorage 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 OC Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64);

свободный разъем USB;

– объем дискового пространства для размещения программного обеспечения на жестком диске PC – 20 Мбайт.

1.3 Комплектность поставки ПАК «Личный Секрет»

ПАК «Личный Секрет» поставляется в составе:

- специальный носитель «Личный Секрет»;

СD 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 должно быть установлено программное обеспечение «Секретный Агент».

ВНИМАНИЕ! Если у Вас установлено ПО ПАК «Личный Секрет» предыдущей версии, то перед установкой нового ПО обязательно выполните удаление ПО старой версии и перезагрузите компьютер!

Для этого следует запустить с CD, входящего в комплект поставки (см. подраздел 1.3), исполняемый файл SetupSecretPersonal_v1.1.exe. В настоящий момент поддерживается вариант установки (и дальнейшей работы всех программных компонентов) на русском языке.

После запуска исполняемого файла выполняется процедура подготовки к установке и на экран выводится стартовое окно с общей информацией, в котором необходимо выбрать пункт «Установка ПО Личного Секрета» (рисунок 1).



Рисунок 1 – Стартовое окно процедуры установки ПО ПАК «Личный Секрет»

Для продолжения процедуры необходимо нажать кнопку <Далее>. Для прекращения процесса установки следует нажать кнопку <Отмена>.

В следующем окне следует выбрать компоненты ПО (рисунок 2), которые необходимо установить. Полный список устанавливаемых компонентов содержит следующие составляющие:

– «Личный Секрет» – комплект ПО ПАК «Личный Секрет». Устанавливается по умолчанию;

– «Документация» – руководства пользователя и администратора ПАК «Личный Секрет»;

– Фильтр USB-устройств, с помощью которого на данном компьютере запрещается использование любых USB-накопителей, кроме устройств ПАК «Личный Секрет».

Имеется возможность установить полный набор компонентов ПО (полная установка) или выбрать отдельные его составляющие (установка по выбору).

😽 Установка ПО Личного (Секрета	
Компоненты устанавливае Выберите компоненты ПО Ли	е мой программы ічного Секрета, которые вы хотите установить.	
Выберите компоненты прогр. 'Далее' для продолжения.	аммы, которые вы хотите установить. Нажмите кн	юпку
вырерите тип установки:	Полная установка	<u> </u>
или выберите дополнительные	Инный Секрет	
компоненты для установки:	У руководство администратора	
yeranookn	 Руководство пользователя Фильтр USB устройств 	
	Описание	
Требуется на диске: 25.1 Мбайт	Наведите курсор мыши на название компонента чтобы прочесть его описание,	a,
	< <u>Н</u> азад Далее >	Отмена

Рисунок 2 - Окно выбора компонентов устанавливаемого ПО

В следующем окне необходимо указать путь к каталогу установки (рисунок 3). По умолчанию установка всех программных компонентов выполняется в каталог \Program Files\OKB SAPR\Secret\Personal. Каталог, предлагаемый по умолчанию, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <Обзор...>. Если указанный каталог не существует, он будет создан программой установки автоматически.

😽 Установка ПО Личного Секрета	
Выбор папки установки Выберите папку для установки ПО Личного Секрета.	
Программа установит ПО Личного Секрета в указанную папку. Чтобы установ приложение в другую папку, нажмите кнопку 'Обзор' и укажите ее. Нажмите 'Далее' для продолжения.	зить кнопку
Папка установки <u>C:\Program Files\OKB SAPR JSC\Secret\Personal</u> <u>Of</u> sop .	
Требуется на диске: 25.1 Мбайт Доступно на диске: 37.5 Гбайт	
< Назад Далее >	Отмена

Рисунок 3 - Выбор каталога установки ПАК «Личный Секрет»

После выбора каталога установки следует нажать кнопку <Далее>, в появившемся далее окне выбрать место размещения ярлыков программы в меню «Пуск» (папка, предлагаемая по умолчанию, может быть изменена посредством ручного редактирования) и нажать кнопку <Установить>. Далее начинается процесс копирования файлов на жесткий диск (рисунок 4). В число устанавливаемых компонентов ПО ПАК «Личный Секрет» входят: драйвер USB-устройства, драйвер-фильтр USB-устройств, приложение для управления доступом к данным CH «Секретный Агент».

😽 Установка ПО Личного Секрета	
Копирование Файлов Выполняется копирование файлов ПО Личного Секрета. Пожалуйста, подождите Извлечение: OtXmlPatterns4.dll 100%	
Выпоняется установка модулей ПО Личного Секрета Папка установки: C:\DOCUME~1\DASHA~1.PEN\LOCALS~1\Temp\Personal Извлечение: QtCore4.dl 100% Извлечение: QtSql4.dl 100% Извлечение: QtSql4.dl 100% Извлечение: QtNetwork4.dl 100% Извлечение: QtDeclarative4.dl 100% Извлечение: QtXmlPatterns4.dl 100%	
< <u>Н</u> азад Далее >	Отмена

Рисунок 4 - Установка программных компонентов ПАК «Личный Секрет»

При установке программных компонентов АРМ Администратора выводятся сообщения об отсутствии теста на совместимость с ОС (рисунок 5). Необходимо выбрать пункт <Все равно продолжить>.

Software Installation	Hardware Installation
The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (<u>Tell me why this testing is important.</u>) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the software vendor for software that has passed Windows Logo testing.	The software you are installing for this hardware: Universal Serial Bus controllers has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway	Continue Anyway

Рисунок 5 – Предупреждающие сообщения

После завершения процесса копирования файлов следует нажать кнопку <Далее> (рисунок 6).

😽 Установка ПО Личного Секрета	
Установка завершена Установка успешно завершена.	
Готово	
/Driver/DPInst.exe целостность не нарушена /SecretAgent.exe целостность не нарушена /QtScript4.dll целостность не нарушена /QtXmlPatterns4.dll целостность не нарушена /QtDeclarative4.dll целостность не нарушена /QtNetwork4.dll целостность не нарушена /QtSql4.dll целостность не нарушена /QtGui4.dll целостность не нарушена /QtCore4.dll целостность не нарушена Удаление файла: C:\DOCUME~1\DASHA~1.PEN\LOCALS~1\Temp\crc_results.in Установка ПО Личного Секрета успешно завершена. Готово	ń
< Назад Далее >	Отмена

Рисунок 6 - Установка программных компонентов ПАК «Личный Секрет»

Далее в появившемся на экране окне выводится сообщение об окончании процесса установки (рисунок 7). Выход из программы установки выполняется посредством нажатия кнопки <Готово>.



Рисунок 7 - Окно завершения установки ПО ПАК «Личный Секрет»

После успешного завершения процесса установки можно начать регистрацию «Секрета» (см. 3.2).

2.2 Удаление ПО ПАК «Личный Секрет»

ПО ПАК «Личный Секрет» При необходимости можно удалить С способами: компьютера посредством двумя выбора пункта меню Пуск \rightarrow Программы \rightarrow Личный Секрет \rightarrow Удалить (рисунок 8) или с помощью стандартного механизма удаления программ Windows: Пуск→Панель управления → Установка и удаление программ.



Рисунок 8 – Удаление ПО ПАК «Личный Секрет» через меню Пуск

ВНИМАНИЕ! Для полного завершения процесса удаления ПО ПАК «Личный Секрет» необходимо перезагрузить компьютер!

2.3 Контроль целостности ПО ПАК «Личный Секрет»

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

В процессе первой установки ПО «Личный Секрет» проверка целостности ПО производится автоматически (рисунок 6).

Для того чтобы проверить целостность уже установленного Секрет», ПО ПАК «Личный следует запустить исполняемый файл SetupSecretPersonal_v1.1.exe и в появившемся стартовом окне выбрать пункт «Проверка целостности файлов ПО Личного Секрета» и нажать кнопку <Далее> (рисунок 9).



Рисунок 9 - Стартовое окно процедуры установки ПО ПАК «Личный Секрет»

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

На экране появится окно, в котором фиксируются детали проверки (рисунок 10). Детали проверки содержат имена файлов и информацию о состоянии их целостности. Поэтому, если какой-либо файл был изменен, то это легко обнаружить.

😽 Установка ПО Личного Секрета	
Проверка завершена Проверка целостности файлов ПО Личного Секрета завершена. Подробности смотрите ниже, в деталях проверки.	
Готово	
/qml/base/PlainWindowBase.qml целостность не нарушена /qml/base/MessageBoxWarning.qml целостность не нарушена /qml/base/MessageBoxQuestion.qml целостность не нарушена /qml/base/MessageBoxInformation.qml целостность не нарушена /qml/base/MessageBoxError.qml целостность не нарушена /qml/base/LogViewDialog.qml целостность нарушена /qml/base/Log0.qml целостность не нарушена /qml/base/Log0.qml целостность не нарушена /qml/base/InformationBase.qml целостность не нарушена /qml/base/Images/warning.png целостность не нарушена /qml/base/Images/tr.png целостность не нарушена /qml/base/Images/tl.png целостность не нарушена /qml/base/Images/tl.png целостность не нарушена	
< Назад Далее >	Отмена

Рисунок 10 – Контроль целостности ПО ПАК «Личный Секрет»

По нажатии кнопки <Далее> после выполнения процедуры проверки целостности ПО, на экран выводится окно, показанное на рисунке 11.



Рисунок 11 – Окно завершения процесса контроля целостности ПО ПАК «Личный Секрет»

В случае нарушения целостности файлов ПО следует установить возможные причины нарушения и при необходимости выполнить переустановку ПО ПАК «Личный Секрет» (см. 2.1).

2.4 Подключение СН

Подключение осуществляется установкой СН в свободный USB-разъем системного блока PC¹.

2.5 Установка системного драйвера СН

ВНИМАНИЕ! Для корректной установки драйвера необходимо идентифицироваться в системе в качестве пользователя с правами администратора.

После установки на жесткий диск ПО ПАК «Личный Секрет» (см. раздел 2.1) при первом подключении устройства «Личный Секрет» к USB-порту операционная система обнаруживает новое устройство (рисунок 12).



Рисунок 12 – Оповещение об обнаружении СН

Далее происходит автоматический запуск системной программы «Мастер нового оборудования»². Если в настройках ОС включен режим автоматического обновления драйверов, то на экран выводится предложение выполнить поиск подходящего драйвера в сети Интернет (рисунок 13). Необходимо выбрать <Нет, не в этот раз> и нажать кнопку <Далее>.

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 Если автоматического запуска «Мастера нового оборудования» не происходит, его можно инициировать двумя щелчками мыши по значку подключенного устройства, показанному на <u>рисунке</u>12.



Рисунок 13 - Окно поиска текущего и обновленного ПО

В следующем окне программы «Мастер нового оборудования» следует выбрать пункт «Автоматическая установка» и нажать кнопку <Далее> (рисунок 14).



Рисунок 14 – Окно установки нового оборудования

После этого начинается процесс установки драйвера СН (рисунок 15).

Мастер нового оборудования	
Подождите, мастер устанавливает программное обеспечени	16
Secret SpecialMedia	
i i i i i i i i i i i i i i i i i i i	
Создание контрольной точки восстановления систем и резервной копии системных файлов на случай	ы
< <u>Н</u> азад Далее >	Отмена

Рисунок 15 – Установка драйвера СН

При установке драйвера выводится сообщение об отсутствии теста на совместимость с ОС (рисунок 16). Необходимо выбрать пункт <Все равно продолжить>.



Рисунок 16 – Предупреждающее сообщение

После установки драйвера «Секрета» в ОС (он помещается в папку \Windows\System32\Drivers¹) на экран выводится окно завершения работы программы «Мастер нового оборудования» (рисунок 17).



Рисунок 17 – Окно завершения работы Мастера нового оборудования

По нажатии кнопки <Готово> выполняется выход из программы установки драйвера СН.

2.6 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 2.4), произведена установка системного драйвера СН (см. подраздел 2.5) и выполнена регистрация компьютера (см. подраздел 3.1).

Следующий шаг – процедура первичной регистрации СН, в результате которой формируется PIN-код и код регистрации 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 на CH.

Код регистрации необходим для выполнения административных операций над СН (повторная регистрация, аннулирование регистрации, разблокирование. Подробнее см. соответствующие подразделы 3). После выполнения процедуры

¹⁾ В 64-битных ОС драйвер сохраняется также в папку \Windows\SysWOW64\Drivers

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

Следует запомнить или надежно сохранить PIN-код и код регистрации CH. 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 CH блокируется. Разблокировать CH можно с использованием кода регистрации (см. 3.6). В результате выполнения операции разблокирования формируется новый PIN-код.

ВНИМАНИЕ! Код регистрации не подлежит восстановлению! При утере кода регистрации становится невозможным выполнение следующих функций СН:

- повторная регистрация СН;
- аннулирование регистрации CH;
- разблокирование СН.

После успешной регистрации по предъявлении корректного PIN-кода может быть получен доступ к данным СН (содержимому флеш-диска). Процедура получения доступа к данным описана в разделе «Применение ПАК «Личный Секрет» «Руководства пользователя» (11443195.4012.031-34).

З Управление ПАК «Личный Секрет»

3.1 Регистрация компьютера

При первом запуске ПО ПАК «Личный Секрет» следует выполнить процедуру регистрации компьютера.

В ходе выполнения данной процедуры Пользователю предлагается задать имя компьютера, которое позволяет идентифицировать компьютер при взаимодействии с СН (рисунок 18). Регистрационное имя компьютера записывается в СН в рамках выполнения процедуры регистрации СН (процедура регистрации СН описана в 3.2 и 3.3). Регистрация СН на компьютере, который, в свою очередь, регистрируется в СН, является необходимым условием для того, чтобы аутентификация при подключении СН к компьютеру была взаимной.

Далее в СН будет добавляться информация обо всех последующих компьютерах, на которых он будет регистрироваться.

Секретный Агент. Регистрация	×
Имя компьютера	Ok
	Отмена

Рисунок 18 – Окно ввода сетевого имени компьютера

Имя компьютера представляет собой строку, длина которой ограничена 27 символами. В качестве имени целесообразно использовать одно или несколько слов, характеризующих принадлежность компьютера или его назначение. Имя компьютера не связано с защитными функциями и задается только для удобства Пользователя, поэтому не нужно стремиться к тому, чтобы имя было сложным или чтобы о нем было трудно догадаться.

Первоначально в поле «Имя компьютера» подставляется системное имя данного компьютера. Если Пользователя не устраивает данное имя, он может ввести свой вариант.

После ввода имени на экран выводится сообщение об успешной регистрации данного компьютера в «Секретном Агенте» (рисунок 19)



Рисунок 19 - Сообщение об успешной регистрации данного компьютера в «Секретном Агенте»

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

3.2 Регистрация СН

До начала использования СН на РС должно быть установлено ПО ПАК «Личный Секрет» (см. 2), выполнена процедура регистрации компьютера (см. 3.1) и СН.

В результате выполнения процедуры регистрации СН формируется PINкод и код регистрации СН, с использованием которых осуществляются операции получения доступа к данным в «Секрете» и администрирования СН соответственно.

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

Для выполнения регистрации необходимо подключить «Секрет» (см. 2.4). Если подключенный СН еще не зарегистрирован на данной РС, после подключения устройства на экран автоматически выводится сообщение о том, что к РС подключен незарегистрированный Секрет.

После запуска «Секретного Агента» (ручного или автоматического) на экран выводится главное окно приложения, показанное на рисунке 20.

🗮 Секретный Агент			×
Серийный номер	Описание	Состояние	Открыть секрет
000000065		Не зарегистрирован	Регистрировать
			Аннулировать регистрацию
			Сменить PIN-код
			Разблокировать

Рисунок 20 - Главное окно приложения «Секретный Агент». Регистрация СН

Для регистрации СН необходимо выбрать соответствующий элемент списка со статусом <Не зарегистрирован> и нажать кнопку <Регистрировать> (рисунок 20). Если не выбран ни один элемент списка, кнопка <Регистрировать> недоступна.

После этого на экран выводится окно для задания регистрационной информации CH (рисунок 21). Можно также отложить регистрацию CH, нажав в окне кнопку <Отмена> (рисунок 21). Регистрация может быть выполнена позднее через главное окно «Секретного Агента».

🗮 Регистрация Секрета	×
Задайте имя Секрета:	Ok
Иванов_А_А	Отмена
— 🔽 Использовать PIN-код ————————————————————————————————————	
Подтвердите PIN-код:	
Г Генерировать автоматически	

Рисунок 21 - Регистрация СН

Необходимо задать следующие регистрационные параметры СН:

– имя. Имя Секрета задается в обязательном порядке. Представляет собой строку, длина которой ограничена 32 произвольными символами. В

качестве имени целесообразно использовать одно или несколько слов, характеризующих принадлежность СН или его назначение (например, это удобно, если в наличии имеется несколько СН, используемых для различных целей. В этом случае их легко отличить друг от друга). Имя «Секрета» не связано с защитными функциями и задается только для удобства Пользователя, поэтому не нужно стремиться к тому, чтобы имя было сложным или чтобы о нем было трудно догадаться.

– PIN-код. PIN-код Секрета задается опционально. При желании, можно не назначать PIN-код Секрету (не рекомендуется), сняв переключатель <Использовать PIN-код> в окне регистрации Секрета (рисунок 21).

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

PIN-код Секрета должен состоять из 6 цифр. Можно назначить PIN-код самостоятельно или сгенерировать автоматически. При самостоятельном назначении PIN-кода требуется его подтвердить, повторив введенную <Подтверждение последовательность символов в поле PIN-кода>. Для автоматической генерации PIN-кода (рекомендуемый вариант) необходимо установить переключатель <Генерировать автоматически> (рисунок 21). В последнем случае поля для ввода и подтверждения PIN-кода блокируются и PIN-код создается в автоматическом режиме, а Пользователь только ставится о нем в известность.

Кнопка <OK> окна регистрации недоступна, если:

имя «Секрета» не задано;

– установлен переключатель <Использовать PIN-код>, но не заданы значения в полях <PIN-код> и <Подтверждение PIN-кода> и при этом не установлен переключатель <Генерировать автоматически>.

Если PIN-код подтвержден неверно, после нажатия кнопки <OK> на экран выводится соответствующее оповещение (рисунок 22). В этом случае следует корректно подтвердить PIN-код.



Рисунок 22 - Оповещение о некорректном подтверждении PIN-кода

В случае возникновения ошибки в ходе регистрации на экран выводится окно, показанное на рисунке 23.



Рисунок 23 - Оповещение об ошибке в ходе регистрации СН

При успешном выполнении описанной последовательности действий на экран выводится сообщение об успешной регистрации «Секрета» и отображаются PIN-код и код регистрации СН (рисунок 24).

🗮 Регистрация С	екрета	:	×
Регистрация Секрета в	ыполнена успешно.	Печать	
Вы можете распечата Храните данную инфо; месте!			
Серийный номер:	0000002031		
Имя Секрета:	Иванов_А_А		
Код регистрации:	8206875823158836		
PIN-код:	911200		

Рисунок 24 – Окно с регистрационными данными Секрета

В случае если при регистрации Секрета не был установлен переключатель <Использовать PIN-код>, в поле <PIN-код> окна с регистрационными данными Секрета указывается, что PIN-код отсутствует (рисунок 25).



Рисунок 25 – Окно с регистрационными данными Секрета в случае регистрации без использования PIN-кода

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить PIN-код и код регистрации СН, знание которых позволяет получать доступ к соответствующим ПАК «Личный Секрет». Имеется возможность функциям печати кода регистрации и PIN-кода CH (при наличии подключенного принтера). При этом корпоративного использования облегчения «Личный Секрет» для код регистрации и PIN-код печатаются на разных листах.

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

PIN-код используется для получения доступа к данным CH.

Код регистрации используется для выполнения операций:

- регистрации СН на другой РС;
- аннулирования регистрации СН;
- разблокирования СН.

Имеется возможность печати кода регистрации и PIN-кода СН посредством нажатия кнопки <Печать> (при наличии подключенного принтера). При этом для облегчения корпоративного использования «Личный Секрет» код регистрации и PIN-код печатаются на разных листах.

После закрытия окна с регистрационными данными Секрета на экране появляется окно, в котором следует подтвердить знание кода регистрации СН, полученного в процессе текущей регистрации СН (рисунок 26). Данная процедура предусмотрена для того, чтобы убедиться в том, что код регистрации надежно сохранен, поскольку он не подлежит восстановлению (см. подраздел 2.6).

Для этого следует в поле «Код регистрации» ввести код регистрации СН и нажать кнопку <Подтвердить код регистрации> (рисунок 26).

🗮 Подтверждение ко	да регистрации	×
Идентификатор Секрета:	000002018	Подтвердить код регистрации
Имя Секрета:	Иванов_А_А	Аннулировать регистрацию
		Показать код регистрации
Код регистрации:		

Рисунок 26 – Подтверждение кода регистрации

Если по каким-либо причинам код регистрации не был сохранен, следует нажать кнопку «Показать код регистрации». На экране снова появится окно с PIN-кодом и кодом регистрации СН (рисунок 24). Необходимо надежно сохранить эти данные и подтвердить код регистрации, как описано выше.

Если по каким-либо причинам требуется прервать процедуру регистрации СН, то в окне подтверждения кода регистрации следует нажать кнопку <Аннулировать регистрацию> (рисунок 26).

После верного подтверждения кода регистрации на экран выводится сообщение об успешном выполнении регистрации Секрета (рисунок 27).



Рисунок 27 – Сообщение об успешном выполнении регистрации

После успешного завершения процедуры регистрации статус СН в главном окне приложения «Секретный Агент» изменяется на <Зарегистрирован> (рисунок 28), и становится доступным выполнение операций получения доступа, смены PIN-кода и аннулирования регистрации.

🗮 Секретный А	гент		×
Серийный номер	Описание	Состояние	Открыть секрет
000000065	Иванов_А_А	Зарегистрирован	Регистрировать
			Аннулировать регистрацию
			Сменить PIN-код
			Разблокировать

Рисунок 28 - Главное окно приложения «Секретный Агент». Изменение статуса СН после успешной регистрации

После успешного завершения процедуры регистрации СН «Личный Секрет» может применяться на данном компьютере. Для того чтобы иметь возможность применять «Секрет» и на других компьютерах, необходимо выполнить на них его повторную регистрацию.

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 требует знания кода регистрации СН. На компьютере, на котором необходимо произвести повторную регистрацию «Секрета», должно быть установлено ПО ПАК «Личный Секрет» (см. раздел 2)¹.

Процедура регистрации СН на другом компьютере в основном аналогична процедуре первичной регистрации. Отличие состоит в том, что после выбора соответствующего элемента из списка подключенных незарегистрированных СН в главном окне «Секретного Агента» (рисунок 20) и нажатия кнопки <Регистрировать> вместо формы для задания регистрационной информации на экран выводится окно с запросом кода регистрации СН (рисунок 29).

Примечание. Поскольку СН ранее был зарегистрирован на первой РС, колонка «Имя» в списке главного окна «Секретного Агента» содержит имя, назначенное Пользователем СН при первичной регистрации.

🗮 Регистрация Секрет	а	×
Идентификатор Секрета:	000000065	Ok
Имя Секрета:	Иванов_А_А	Отмена
Код регистрации:		

Рисунок 29 - Запрос кода регистрации СН

После ввода кода регистрации СН (сформированного в результате первичной регистрации, см. рисунок 24) и нажатия кнопки <OK> в СН производится его проверка. В случае если введен неверный код регистрации, на экран выводится сообщение об ошибке (рисунок 23).

ВНИМАНИЕ! Во время выполнения операции регистрации СН на другом компьютере не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

Если описанная последовательность действий выполнена верно, то на экран выводится сообщение об успешной регистрации «Секрета» (рисунок 30).

🗮 Регистрация Секрета	×	
Регистрация Секрета выполнена успешно	Ok	

Рисунок 30 – Сообщение об успешной повторной регистрации

¹ ПО «Секретный Агент» можно бесплатно скачать с официального сайта про «СЕКРЕТ» – www.proSecret.ru. Не рекомендуется брать ПО для комплексов «СЕКРЕТ» из случайных или непроверенных источников.

После завершения процедуры повторной регистрации СН «Личный Секрет» может использоваться на РС для защищенного хранения информации.

3.4 Аннулирование регистрации СН

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

Для аннулирования регистрации СН необходимо в основном окне «Секретного Агента» выбрать соответствующий элемент из списка зарегистрированных СН и нажать кнопку <Аннулировать регистрацию> (рисунок 28).

🗮 Аннулирование реги	истрации Секрета	×
Идентификатор Секрета:	000000065	Ok
Имя Секрета:	Иванов_А_А	Отмена
Код регистрации:		

Рисунок 31 - Ввод кода регистрации для аннулирования регистрации

В появившемся окне (рисунок 31) нужно ввести код регистрации, полученный Пользователем при первичной регистрации данного Специального Носителя (рисунок 24).

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



Рисунок 32 - Сообщение об успешном аннулировании регистрации СН

После выполнения всех операций на экран выводится сообщение об успешном выполнении аннулирования регистрации СН (рисунок 32). С этого момента получение доступа к данным в «Секрете» на данной РС становится невозможным (до выполнения процедуры регистрации).

Аннулирование регистрации на первичном компьютере дополнительно влечет за собой удаление из СН информации о регистрации, выполненной на всех других компьютерах. При этом устройство переходит в состояние «до первой регистрации» (см. 3.2).

3.5 Смена PIN-кода СН

Если Пользователь CH считает PIN-код скомпрометированным, он может сменить действующий PIN-код на новый. При этом CH должен быть подключен к компьютеру.

Для смены PIN-кода необходимо в основном окне «Секретного Агента» выбрать из списка нужный СН и нажать кнопку <Сменить PIN-код> (рисунок 28).

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).

В появившемся окне следует ввести старый PIN-код, полученный Пользователем при регистрации данного СН. Пользователь может задать новый PIN-код самостоятельно или сгенерировать его автоматически с помощью установки флага <Генерировать автоматически> (рисунок 33).

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!

🗮 Смена PIN кода Секрета	×
Старый PIN-код:	Ok
	Отмена
— Новый PIN-код	
РІN-код:	
Подтвердите PIN-код:	
Г Генерировать автоматически	

Рисунок 33 - Окно для смены PIN-кода

Далее в информационном окне выводится сообщение об успешной смене PIN-кода (рисунок 34).

🗮 Смена PIN код	ца Секрета	×
Смена PIN-кода выпол	нена успешно.	Печать
Запомните новый PIN- недоступном для друг	код или сохраните его в их месте.	
Серийный номер: Имя Секрета: Новый PIN-код:	000000065 Иванов_А_А 111111	

Рисунок 34 - Сообщение об успешной смене PIN-кода

В случае ввода неправильного старого PIN-кода на экран выводится окно, показанное на рисунке 35.



Рисунок 35 - Оповещение об ошибке в ходе смены PIN-коды

В таком случае следует повторить описанную последовательность действий и ввести PIN-код снова.

3.6 Разблокирование СН

В случае трех последовательных неудачных попыток ввода PIN-кода CH блокируется и на экран выводится соответствующее сообщение (рисунок 36).



Рисунок 36 - Оповещение о блокировке СН

При этом статус СН в главном окне «Секретного Агента» изменяется на <Заблокирован> и единственной доступной операцией становится <Разблокировать> (рисунок 37).

🗮 Секретный А	ыгент		×
Серийный номер	Описание	Состояние	Открыть секрет
000000065	Иванов_А_А	Заблокирован	Регистрировать
			Аннулировать регистрацию
			Сменить PIN-код
			Разблокировать

Рисунок 37 - Главное окно приложения «Секретный Агент». Изменение статуса после блокировки СН

СН может быть разблокирован посредством выбора соответствующего элемента списка и нажатия кнопки <Разблокировать>. В появившемся окне необходимо ввести код регистрации, полученный в результате первичной регистрации СН (рисунок 24), и новое значение PIN-кода.

Разблокирование Секрета	×
Введите Код регистрации:	Ok
	Отмена
— Новый PIN-код —————	
РІN-код:	
Подтвердите PIN-код:	
Г Генерировать автоматически	

Рисунок 38 - Разблокирование СН

Пользователь может задать новый PIN-код самостоятельно или сгенерировать его автоматически с помощью установки флага <Генерировать автоматически> (рисунок 38).

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

После успешного выполнения данной операции на экран выводится окно с новым PIN-кодом CH «Личный Секрет», который необходимо запомнить (рисунок 39).

📕 Разблокирова	ние Секрета	×
Разблокирование выпо	лнено успешно.	Печать
Запомните новый PIN- недоступном для друп	код или сохраните его в их месте.	
Серийный номер: Имя Секрета: Новый PIN-код:	0000000065 Иванов_А_А 111111	

Рисунок 39 – Окно с новым PIN-кодом СН

После успешного разблокирования работа с «Секретом» может быть продолжена.

4 Рекомендации по организации безопасного применения ПАК «Личный Секрет»

4.1 Общие сведения

При применении ПАК «Личный Секрет» следует проявлять осторожность в случае, когда пользователь совершает перерывы в работе на РС: необходимо помнить, что прежде чем встать из-за компьютера, нужно обязательно заблокировать экран (например, нажатием комбинации клавиш <Win>+<L>).

Это позволит защитить данные пользователя от посторонних лиц, когда он отсутствует на рабочем месте, а сеанс работы с ПАК «Личный Секрет» еще не завершен.

Во избежание недоразумений, связанных с ситуациями, когда пользователь забыл заблокировать экран, администратору рекомендуется на рабочих станциях:

- устанавливать вход пользователя в систему с обязательным вводом пароля;
- настраивать автоматическую блокировку экрана РС по истечении заданного периода неактивности.

4.2 Установка входа пользователя в систему с обязательным вводом пароля

Для того чтобы установить вход пользователя в систему с обязательным вводом пароля, необходимо выполнить следующие действия:

1)через Пуск->Выполнить меню запустить команду «control userpasswords2» и в появившемся далее окне «Учетные записи пользователей» поставить галочку «Требовать ввод имени пользователя И пароля» (рисунок 40). Данная операция может быть выполнена для рабочих станций, не включенных в домен.

Учетные записи пользов	ателей 🛛 ? 🔀
Пользователи Дополнител	ьно
Следующий список отказа в доступе к паролей и иных пар Гребовать ввод имени п Пользователи этого компьн	к используется для предоставления или вашему компьютеру, а также для смены раметров. юльзователя и пароля. отера:
Имя пользователя	Группа
Администратор	Администраторы
🛃 Дарья	Администраторы
Иван	Опытные пользователи
До Пароль пользователя Ива Мароль Пользователя Ива Чтобы изменить и кнопку "Сменить	бавить Удалить Свойства ан пароль пользователя "Иван", нажмите пароль". Сменить пароль
(ОК Отмена Применить

Рисунок 40 – Окно настроек учетных записей пользователей

2) если выбранному пользователю еще не задан пароль для входа в систему, следует нажать кнопку <Сменить пароль...> и в появившемся далее окне смены пароля задать и подтвердить новый пароль (рисунок 41).

Смена пароля	
<u>Н</u> овый пароль:	
Подтверждение:	
	ОК Отмена

Рисунок 41 – Окно смены пароля пользователя для входа в ОС

4.3 Включение режима автоматической блокировки экрана

Для включения режима автоматической блокировки экрана по истечении заданного периода неактивности следует выполнить следующие действия:

– при работе в Windows XP: в меню Пуск->Панель управления-> Экран->Заставка следует установить галочку «Начинать с экрана приветствия» и выставить необходимый интервал времени неактивности (рисунок 42).

войства: Экран ?					
Темы	Рабочий стол	Заставка	Оформление	Параметры	
			<u>1</u> 2		
		Window	10		
	_	-	•0		
<u>3</u> ac	тавка ndows XP		🗸 Параметр	ы	
<u>И</u> нт	ервал: 10 🗢	мин. 🔽	Науинать с экр	рана приветствия	
Эне	ргосбережение				
	Дл на	тя изменени жмите кноп	ня параметров і ку "Питание".	питания монитора	
				Питание	
)К От	мена Применить	

Рисунок 42 – Окно настройки заставки экрана в ОС Windows XP

– при работе в Windows 7: в меню Пуск->Панель управления-> Персонализация->Заставка следует установить галочку «Начинать с экрана входа в систему» и выставить необходимый интервал времени неактивности (рисунок 43).

Заставка Объемный текст Параметры Просмотр Интервал: 10 мин. Пачинать с экрана входа в систему Энергосбережение Энергосбережение Энергосбережение Энергосбережение Энергосбережение	аставка		
Заставка Объемный текст Параметры Просмотр Интервал: 10 мин. Иначинать с экрана входа в систему Энергосбережение Энергосбережение Энергосбережение за счет изменения яркости экрана или других параметров электропитания		Eprov	er nut
Объемный текст Параметры Просмотр Интервал: 10 мин. Интервал: 10 мин. Интервал: 10 мин. Энергосбережение Энергосберевосбе			• 0
Интервал: 10 — мин. Интервал: 10 — мин. Интервал: 10 — мин. Интервал: Энергосбережение Энергосбережение Энергосбережение за счет изменения яркости экрана или других параметров электропитания. Изменить параметры электропитания	Заставка		
Энергосбережение Энергосбережение за счет изменения яркости экрана или других параметров электропитания. Изменить параметры электропитания	Заставка Объемный текст	•	Параметры Просмотр
	Заставка Объемный текст Интервал: 10	▼ мин. 🔽 Нач	Параметры Просмотр инать с экрана входа в систему

Рисунок 43 - Окно настройки заставки экрана в ОС Windows 7

5 Рекомендации по применению «Личного Секрета» в корпоративной среде

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

Процедура получения доступа к данным описана в разделе «Применение ПАК «Личный Секрет» «Руководства пользователя» (11443195.4012.031-34).

В случае корпоративного использования ПАК «Личный Секрет» исключить возможность несанкционированного использования СН Пользователем на компьютере, не входящем в список разрешенных, можно только в том случае, если Пользователю не известен код регистрации.

Для этого первичным компьютером для всех «Секретов» должен быть специально выделенный компьютер Администратора, на котором Администратор произведет регистрацию всех «Секретов» (см. 3.2). Компьютер Администратора должен быть защищен от НСД, а распечатки кодов регистрации (либо журнал, в котором записаны Коды регистрации) должны храниться в гарантированно недоступном для Пользователей месте.

После первичной регистрации всех «Секретов» на компьютере Администратора, Администратор должен произвести повторную регистрацию каждого из «Секретов» на тех компьютерах, на которых, в соответствии с политикой безопасности, Пользователю данного «Секрета» разрешено работать с СН (см. 3.3).

После этого каждому Пользователю выдается зарегистрированный для него «Секрет» и сообщается его PIN-код.

ВНИМАНИЕ! Если Пользователю станет известен код регистрации, он сможет зарегистрировать свой «Секрет» на любом компьютере, а также сбросить регистрацию на служебных компьютерах. При этом, сбросив первичную регистрацию (при недостаточной защищенности ОТ НСД компьютера, на котором произведена первичная регистрация данного «Секрета»), он может без потери данных зарегистрировать его на другом компьютере, получив новый код регистрации, который не будет известен Администратору, тем самым, фактически, выведет «Секрет» из корпоративной системы. С помощью ПАК «Личный Секрет» контролировать использование такого «Секрета» в ИС предприятия нельзя. Поэтому необходимо исключить попадание кода регистрации в руки Пользователя.

6 Перечень принятых сокращений и обозначений

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