ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

УТВЕРЖДЕН

11443195.4012.033 31-ЛУ

Программно-аппаратный комплекс защищенного хранения информации «Секрет Особого Назначения»

Описание применения

11443195.4012.033 31

Подп. и дата

Инв. № дубл.

Подп. и дата

Инв. № подл.

АННОТАЦИЯ

Настоящий документ является описанием применения программно-аппаратного комплекса «Секрет Особого Назначения» (далее по тексту – ПАК «Секрет Особого Назначения», либо ПАК), предназначенного для защищенного хранения корпоративной или личной информации конфиденциального характера на отчуждаемом USB-носителе и предоставляет возможность применения этого носителя исключительно на тех компьютерах, которые разрешены владельцем.

В документе приведены общие сведения о ПАК «Секрет Особого Назначения», включая описание основных функций, возможностей, особенностей применения.

Перед установкой и эксплуатацией ПАК «Секрет Особого Назначения» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, указанные в настоящей документации.

Применение ПАК «Секрет Особого Назначения» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ.

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение комплекса

ПАК «Секрет Особого Назначения» – это комплекс программных и аппаратных средств, которые предназначены для применения на ПЭВМ типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP SP3/Vista/7 SP1/8/8.1/10/Server 2012/Server 2012 R2/Server 2016 (x32 или x64), с целью обеспечения безопасного хранения корпоративной или личной информации конфиденциального характера на основе:

– взаимной аутентификации носителя информации и рабочей станции с использованием безопасного криптографического протокола;

– парольной аутентификации пользователя.

1.2 Состав ПАК «Секрет Особого Назначения»

В состав ПАК «Секрет Особого Назначения» входят следующие компоненты:

– специальный носитель «Секрет Особого Назначения» (СН, или «Секрет»);

– программное обеспечение (ПО) рабочей станции (РС), состоящее из двух приложений:

– консоль администратора;

– консоль пользователя.

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

Специальный носитель имеет внутреннюю энергонезависимую память объемом от 64 до 256 Кбайт, предназначенную для хранения внутреннего ПО СН и аутентификационной информации непосредственно в вычислителе, а также дополнительный блок памяти объемом не менее 4 Гбайт[1], который используется для хранения защищаемой информации пользователя.

СН может выпускаться в разных модификациях: с реализацией технологических мер защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля и без реализации данных мер, с внутренними часами и без внутренних часов.

Программное обеспечение рабочей станции предназначено для обнаружения СН, аутентификации (опознавания) СН на РС, передачи аутентификационных данных пользователя в СН для получения доступа к внутренней памяти флеш-диска со стороны РС, а также для поддержки административных и пользовательских функций.

[1)] Объем памяти определяется при заказе комплекса в соответствии с требованиями Заказчика и указывается в формуляре.

2 Условия применения

2.1 Требования к техническим средствам

К техническим и программным средствам рабочей станции, на которой используется ПАК «Секрет Особого Назначения», предъявляются следующие минимальные требования:

– IBM PC совместимая ПЭВМ, работающая под управлением операционной системы Microsoft Windows XP SP3/Vista/7 SP1/8/8.1/10/Server 2012/Server 2012 R2/ Server 2016 (x32 или x64);

– свободный разъем USB.

2.2 Требования и условия организационного, технического и технологического характера

Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов АС необходимо:

– наличие администратора ПАК «Секрет Особого Назначения» – привилегированного пользователя, имеющего особые статус и полномочия. Обязанности администратора по применению комплекса изложены в «Руководстве администратора» (11443195.4012.033 90);

– учет специальных носителей;

– хранение в тайне PUK-кода и кода авторизации (КА) СН.

3 ОПИСАНИЕ ЗАДАЧИ

3.1 Порядок работы

Типовой рабочий цикл ПАК «Секрет Особого Назначения» следующий:

- администрирование СН:
  - запуск консоли администратора администратором безопасности;
  - регистрация администратора;
  - настройка политик использования кода авторизации;
  - настройка политики доступа к РС;
  - настройка политик заполнения журнала;
- регистрация пользователя:
  - запуск консоли пользователя пользователем;
  - установка КА и PUK;
- использование СН:
  - запуск консоли пользователя пользователем;
  - авторизация пользователя;
  - монтирование закрытого диска СН;
  - использование закрытого диска СН для хранения конфиденциальной информации.

Помимо этого при эксплуатации СН выполняется обслуживание СН:

- смена КА (пользователь);
- разблокирование СН (пользователь);
- смена пароля администратора (администратор);
- перенастройка политик СН (администратор);
- просмотр журнала событий СН (администратор);
- экспорт журнала событий СН (администратор);
- очистка журнала событий СН (администратор);
- обновление firmware (администратор);
- аннулирование регистрации пользователя (администратор);
- общий сброс СН (администратор);
- установка внутреннего времени (администратор).

3.2 Запуск ПО РС

ПО РС, состоящее из консоли администратора и консоли пользователя, устанавливается на открытый диск СН при изготовлении. Инсталляция его на РС не требуется. При включении СН в USB-разъем РС автоматически монтируется открытый диск СН. Внутреннее ПО СН разрешает доступ к открытому диску только для чтения. После этого консоль администратора может быть запущена администратором на исполнение. На экране появляется окно консоли

администратора, позволяющее пользователю выбрать необходимые ему действия. Некоторые функции могут быть неактивными в зависимости от состояния СН.

3.3 Регистрация администратора

При запуске консоли администратора с подключенным к РС СН, в котором ранее не зарегистрирован администратор, активна только функция регистрации администратора. В появившемся диалоговом окне администратор должен ввести наименование СН и значение пароля администратора с подтверждением.

После ввода пароль администратора и наименование СН передаются в СН и сохраняется во внутренней памяти.

После регистрации администратора, функция регистрации администратора блокируется и становятся доступными остальные функции администрирования, для активации которых администратор должен авторизоваться вводом своего пароля. В случае трех подряд неудачных попыток авторизации администратора внутреннее ПО СН не реагирует на протоколы ПАК «Секрет Особого Назначения» в течение 30 сек. Это состояние блокирования сбрасывается при повторном включении СН.

3.4 Настройка политик использования кода авторизации

Экран настройки политик КА позволяет администратору выбрать следующие параметры СН:

– минимальную и максимальную длину КА (КА может быть от 6 до 16 алфавитно-цифровых символов в кодировке Windows-1251; администратор может задать конкретные значения в этом диапазоне; по умолчанию используются значения 6 и 16, соответственно);

– максимальное число неудачных попыток авторизации: после достижения этого порога СН блокируется, разблокировка возможна только по предъявлению PUK; по умолчанию установлено значение 3.

Функция настройки политик КА активна только в СН, на котором не зарегистрирован пользователь.

3.5 Настройка политик доступа к РС

Экран настройки политик доступа к РС позволяет администратору выбрать одно из следующих значений:

– разрешить использовать СН на любой РС;

– ограничить использование СН на РС.

При выборе второй опции администратор может указать конкретные домены Active Directory, а также конкретные РС, на которых разрешается использовать данный СН. Предполагается считывать информацию о составе доменов информационной системы из информационных файлов, которые предоставляют контроллеры доменов. Администратор может выбрать отдельные РС домена. Также допустимо указать РС, не включенные в домены.

При авторизации СН получает от ПО РС идентификатор домена и идентификатор РС в домене, что позволяет ему отказать в авторизации пользователю при нарушении политики доступа к РС.

Также комплекс предоставляет возможность временного снятия ограничений на доступ к СН на РС. Администратор может указать начальную и конечную даты, определяющие интервал, в который не требуется ограничивать доступ к СН.

3.6 Настройка политик заполнения журнала СН

Экран настройки политик заполнения журнала событий СН позволяет администратору выбрать одно из следующих значений:

– циклическая перезапись журнала без блокировки;

– блокирование пользователя при переполнении журнала.

В первом случае при достижении журнал событий СН максимального выделенного объема он будет записываться со стиранием самых старых записей. Во втором случае при достижении этой границы внутреннее ПО СН блокирует выполнение всех пользовательских функций СН до тех пор, пока администратор не выполнит очистку журнала событий.

3.7 Регистрация пользователя

При запуске консоли пользователя с подключенным к РС СН, в котором не зарегистрирован пользователь, из доступных функций активна только функция регистрации пользователя.

При регистрации пользователя выполняется следующая последовательность действий:

– пользователь задает имя СН, при условии, что имя СН не было задано ранее при регистрации администратора;

– пользователь вводит значение КА с подтверждением, соответствующее установленной администратором политике;

– КА передается в СН и сохраняется во внутренней памяти микроконтроллера;

– внутреннее ПО СН с помощью физического ДСЧ генерирует PUK;

– внутреннее ПО СН передает значение PUK ПО РС;

– внутреннее ПО СН сохраняет КА и PUK во внутренней памяти микроконтроллера;

– консоль пользователя выводит на экран значение PUK;

– консоль пользователя позволяет напечатать значения КА и PUK.

Пользователь должен запомнить КА и PUK. Если он забудет эти значения, доступ к данным пользователя, записанным на закрытый диск СН будет потерян. При этом для дальнейшего использования СН должен выполнить процедуру аннулирования регистрации пользователя.

Помимо всего этого, при регистрации пользователя внутреннее ПО СН генерирует с помощью внутреннего физического ДСЧ новое значение параметра,

используемого при реализации технологических мер защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля.

3.8 Использование СН на РС

Использование СН для хранения конфиденциальной информации возможно только, если в СН зарегистрирован пользователь.

Для авторизации пользователь должен ввести верное значение КА. После успешного завершения процедуры авторизации автоматически монтируется закрытый диск СН, который становится доступен операционной системе РС.

Если авторизация завершилась неудачей, монтирование закрытого диска не производится. В случае достижения порога неудачных попыток авторизации (определяется политикой КА) СН блокируется. Дальнейшее штатное использование СН возможно только после успешного выполнения операции разблокирования.

3.9 Смена кода авторизации

Регулярно (в соответствии с внутренней политикой безопасности) или экстренно, в случае подозрения о компрометации КА, зарегистрированный пользователь СН может с помощью консоли пользователя заменить действующий КА на новый. При этом пользователь должен авторизоваться, предъявив прежнее значение КА, и ввести новое значение с подтверждением, которое сохранится в СН.

3.10 Разблокирование СН

Регулярно (в соответствии с внутренней политикой безопасности организации) или экстренно, в случае подозрения о компрометации, администратор СН может с помощью консоли администратора заменить действующий пароль администратора на новый. При этом администратор должен авторизоваться, предъявив прежнее значение пароля, и ввести новое значение с подтверждением, которое сохранится в СН.

3.11 Смена пароля администратора

Регулярно (в соответствии с внутренней политикой безопасности организации) или экстренно, в случае подозрения о компрометации, администратор СН может с помощью консоли администратора заменить действующий пароль администратора на новый. При этом администратор должен авторизоваться, предъявив прежнее значение пароля, и ввести новое значение с подтверждением. Новый пароль администратора записывается в СН и выводится на экран для запоминания администратором СН.

3.12 Перенастройка политик СН

Перенастройка политик использования СН выполняется так же, как установка политик (см. п. 3.4, 3.5 и 3.6).

3.13 Просмотр журнала событий СН

Все операции с СН находят отражение во внутреннем журнале событий устройства, в котором обеспечивается регистрация, по крайней мере, следующих событий:

- начало сеанса работы СН с РС;
- установка внутренних часов микроконтроллера СН;
- установка описания РС;
- регистрация администратора;
- смена пароля администратора;
- установка политик КА;
- установка политик доступа к РС;
- установка политик записи журнала СН;
- очистка журнала СН;
- полный сброс СН;
- получение доступа к журналу событий;
- обновление внутреннего ПО СН;
- регистрация пользователя;
- аннулирование регистрации пользователя;
- смена КА;
- блокирование СН;
- разблокирование СН;
- авторизация пользователя.

Структура записи журнала событий содержит:

- дата и время события;
- тип события;
- описание события.

Информация об очередном событии СН всегда записывается в конец журнала событий. В случае достижения предела выделенного объема, внутреннее ПО СН поступает в соответствии с политикой, установленной администратором (см. п. 3.6).

Доступ к содержимому внутреннего журнала событий (просмотр, экспорт и очистка) разрешен с помощью консоли администратора только зарегистрированному администратору после его авторизации. После того, как администратор выбрал функцию просмотра журнала событий, происходят следующие действия:

- раздел памяти, предназначенный для записи журнала событий, становится доступным операционной системе РС на чтение;

- консоль администратора выводит на экран содержимое файлов внутреннего журнала событий, который оно считывает с этого диска.

3.14 Экспорт журнала событий СН

В случае необходимости проведения экспорта журнала событий, администратор, после получения к доступа к СН, может скопировать журнал на любой носитель информации.

3.15 Очистка журнала событий СН

Очистка журнала событий выполняется зарегистрированным администратором СН для того, чтобы освободить место под протоколирование будущей активности, а также для снятия блокировки СН в случае переполнения журнала.

Выбор этой функции приводит к форматированию соответствующего раздела памяти, предназначенного для хранения журнала. После этого информация о предыдущих событиях СН теряется.

3.16 Обновление внутреннего ПО

Обновление внутреннего ПО выполняет зарегистрированный администратор с помощью утилиты fmUploader, при этом он должен указать путь к файлу прошивки. Утилиту fmUploader и новый файл прошивки администратору доставляет производитель СН. Также утилиту fmUploader можно скачать с сайта производителя http://prosecret.ru.

При обновлении внутреннего ПО выполняются следующие действия:

– обновление внутреннего ПО СН во внутренней памяти микроконтроллера;

– обновление СПО РС на открытом диске СН;

– обновление документации расположенной на открытом диске СН.

3.17 Аннулирование регистрации пользователя

Аннулирование регистрации пользователя приводит к очистке содержимого закрытого диска и служебной информации пользователя СН. Операция выполняется зарегистрированным администратором в случае, когда необходимо передать СН другому пользователю, или когда утерян КА и PUK.

Следует иметь в виду, что процесс очистки памяти достаточно длительный, и потеря питания СН до ее завершения не приведет к сбросу, а только к стиранию части закрытого диска. Поэтому администратору следует дождаться окончания процедуры и только после этого извлекать СН из разъема USB.

3.18 Общий сброс СН

Общий сброс СН приводит к аннулированию регистраций администратора и пользователя, очистке содержимого закрытого диска и служебной информации. Операция выполняется администратором в случае, когда пароль администратора утерян.

Следует иметь в виду, что процесс очистки памяти достаточно длительный, и потеря питания СН до ее завершения не приведет к сбросу, а только к стиранию

части закрытого диска. Поэтому администратору следует дождаться окончания процедуры и только после этого извлекать СН из разъема USB.

3.19 Установка внутреннего времени

Установка внутреннего времени выполняется администратором СН, в случае если СН снабжен внутренними часами, и внутренние часы были сброшены, например, вследствие извлечения элемента питания. При установке внутреннего времени администратору необходимо указать подходящие текущие дату и время.

3.20 Идентификация РС

Для идентификации РС используется описание РС, которое включает в себя следующую информацию:

- серийный номер АМДЗ («Аккорд», «Соболь»);
- серийный номер материнской платы компьютера;
- серийный номер дистрибутива ОС;
- идентификатор домена Active Directory;
- идентификатор РС в домене (имя компьютера).

Описание РС собирается ПО РС при запуске и передается каждому СН после установки внутренних часов микроконтроллера. ПО СН записывает описание РС во внутренний журнал событий.

Идентификатор РС в протоколах связи ПО РС имеет длину 32 бита и вычисляется как значение хэш-функции от описания РС.

3.21 Служебная информация СН

Служебная информация СН включает:

– идентификатор СН – серийный номер (32 бита), задаваемый изготовителем;

– наименование СН (64 символа в кодировке Windows-1281), задаваемое администратором;

– параметр обновления (32 байта), используемый для обновления ПО СН;

– параметр, используемый при реализации технологических мер защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля (32 байта);

– пароль администратора (строка длиной от 6 до 16 алфавитно-цифровых символов в кодировке Windows-1281);

– PUK (16 шестнадцатеричных цифр);

– КА (строка от 6 до 16 алфавитно-цифровых символов в кодировке Windows-1281);

– список доменов и РС, в которых разрешено использование СН.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Для работы ПО «Секрет Особого Назначения» не требуется никаких дополнительных служебных данных, хранящихся в ПЭВМ.

СВЕДЕНИЯ О ВНЕСЕННЫХ ИЗМЕНЕНИЯХ И ДОПОЛНЕНИЯХ

Основание (наименование, номер документа и дата)	Дата внесения изменения	Содержание изменений, дополнений	Должность, фамилия и подпись лица ответственного за внесение изменений