УТВЕРЖДЕН

BY.СЮИК.00464-01 34 01-ЛУ

КОМПЛЕКС ПРОГРАММНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОС WINDOWS «БАС-W»

Руководство оператора

BY.СЮИК.00464-01 34 01

Листов 51

2023

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

№ изм.	Подп.	Дата

Литера O_1

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по установке, запуску и эксплуатации «Комплекса программного криптографической защиты информации устройств под управлением ОС Windows «БАС-W» (далее - КП «БАС-W»).

Для понимания изложенного в документе материала необходимы навыки работы в операционных системах (ОС) Windows.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1.1. КП «БАС-W» предназначен для организации защищенного VPN-подключения устройства, работающего под управлением ОС Windows, к «Комплексу программно-аппаратному криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС») или «Комплексу программному виртуальному криптографической защиты информации «БАС-V» BY.СЮИК.00436-01 (далее – КП «БАС-V»).

1.2. КП «БАС-W» обеспечивает криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов путем их шифрования с использованием криптографических алгоритмов на основе протоколов IPsec.

1.3. Область применения КП «БАС-W» – системы обработки информации ограниченного распространения.

1.4. КП «БАС-W» реализует следующие функциональные возможности:

а) защиту информации путем ее шифрования с использованием криптографических алгоритмов на основе протоколов IPsec;

б) шифрование передаваемых данных в соответствие с СТБ 34.101.31;

в) контроль целостности пакетов данных (вычисление имитовставки) в соответствие с СТБ 34.101.31, СТБ 34.101.47;

г) согласование ключей шифрования и аутентификация в соответствии с СТБ 34.101.66;

д) поддержка режимов аутентификации как с использованием сертификатов открытых ключей (протокол BSTS; протокол аутентификации, описанный в RFC 7296, с использованием пары Сертификат/Личный ключ), так и с использованием предустановленного секрета (протокол BPACE);

е) генерацию ключей и синхропосылок в соответствии с СТБ 34.101.47;

ж) выработку открытых ключей в соответствии с СТБ 34.101.45;

и) формирование запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17 и СТБ 34.101.78;

к) обработку сертификатов открытых ключей и списков отозванных сертификатов в соответствии с СТБ 34.101.19 и СТБ 34.101.78;

л) защиту секретных (личных) ключей от несанкционированного раскрытия, модификации и подмены, открытых – от модификации и подмены;

м) проверку работоспособности при включении, по запросу оператора или по расписанию;

н) тестирование следующих параметров;

– тесты криптографических алгоритмов;

– контроль целостности программного обеспечения;

о) статистическое тестирование источников случайности при включении;

п) возможность работы через NAT при помощи протокола NAT Traversal (NAT-T);

р) ведение журнала аудита;

с) автоматическую смену ключей шифрования при достижении заданного «времени жизни» ключа;

т) передача данных аудита на сервер Syslog;

у) получение IP-адреса из пула сервера.

1.5. КП «БАС-W» не ограничивает функциональные возможности устройства, на котором он установлен и работает.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для выполнения КП «БАС-W» необходимо устройство, работающее под управлением ОС Windows версии 7 или выше.

КП «БАС-W» для своей работы не предъявляет дополнительных системных требований, отличных от требований ОС Windows.

КП «БАС-W» обеспечивает защиту данных, передаваемых пользователями ОС Windows, вне зависимости от их прав в самой ОС.

В связи с этим, для КП «БАС-W» существует две роли пользователей:

– Администратор;

– Пользователь (оператор).

Администратор – пользователь, обладающий привилегированными правами в ОС Windows.

Администратору доступны следующие функции КП «БАС-W»: установка, восстановление, обновление, удаление.

Пользователю (оператору ОС Windows) доступны все сервисы, необходимые для организации защищенного канала передачи данных.

Перед началом работы с КП «БАС-W» Администратор ОС Windows должен выполнить настройку средств защиты от вредоносного программного обеспечения, стандартными средствами ОС выполнить работы по регистрации Пользователей в ОС, созданию требований к аутентификационным данным пользователей, таким образом, чтобы каждый Пользователь сменил свои аутентификационные данные (пароль) при следующем входе в ОС, и их прав. В качестве аутентификационных данных необходимо использовать сложные пароли длиной не менее 8 символов. Это исключает возможность их подбора методом «словаря». Администратор не должен допускать возможности работы пользователей с недостаточно стойкими паролями.

Обычно для работы КП «БАС-W» не требуется дополнительных настроек среды, отличных от настроек, определенных в ОС Windows, по умолчанию. Однако КП «БАС-W» не запрещает Администратору изменять как настройки ОС, так и настройки самого КП «БАС-W» (выбор места размещения КП «БАС-W» на диске). При этом необходимо учесть, что Пользователям должен быть ограничен доступ на изменение файлов КП «БАС-W».

КП «БАС-W» в процессе своей работы использует пользовательскую папку («%USERPROFILE%\BAS-W») для хранения конфигурационных файлов Пользователя. По умолчанию доступ к ней разрешен только владельцу и запрещен для других Пользователей. Администратор не должен изменять данные настройки доступа к пользовательской папке.

Организация защищенного канала передачи данных с помощью КП «БАС-W» разрешается под непривилегированной учетной записью Пользователя (оператора).

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Установка

3.1.1. Установка КП «БАС-W» производится Администратором путем запуска программы установки «BasWSetup_x32.exe» или «BasWSetup_x64.exe» в зависимости от разрядности ОС.

3.1.2. КП «БАС-W» предлагает Администратору выбрать язык (рис. 1), который будет использован в процессе установки. Программа установки поддерживает работу трех языков: английский, белорусский и русский. Далее описывается работа программы установки с использованием русского языка.

Чтобы продолжить Администратор должен в выпадающем списке выбрать язык и нажать кнопку «ОК».

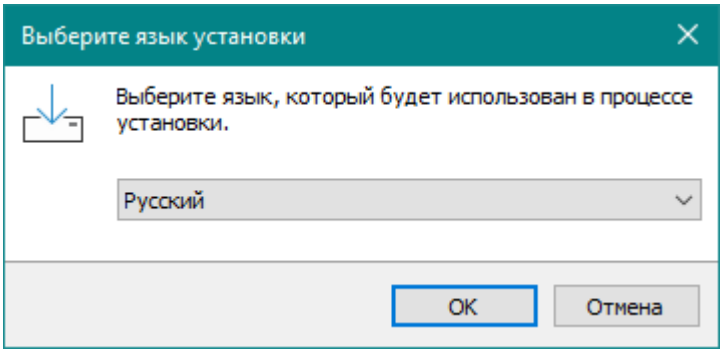

Рис. 1

3.1.3. После выбора языка установки Администратору будет предложено прочитать Лицензионное Соглашение (рис. 2). Соглашаясь с условиями Лицензионного Соглашения, Администратор подтверждает, что он ознакомился с ними, понимает свои права и обязанности.

Чтобы продолжить Администратор должен отметить переключатель «Я принимаю условия соглашения» и нажать кнопку «Далее».

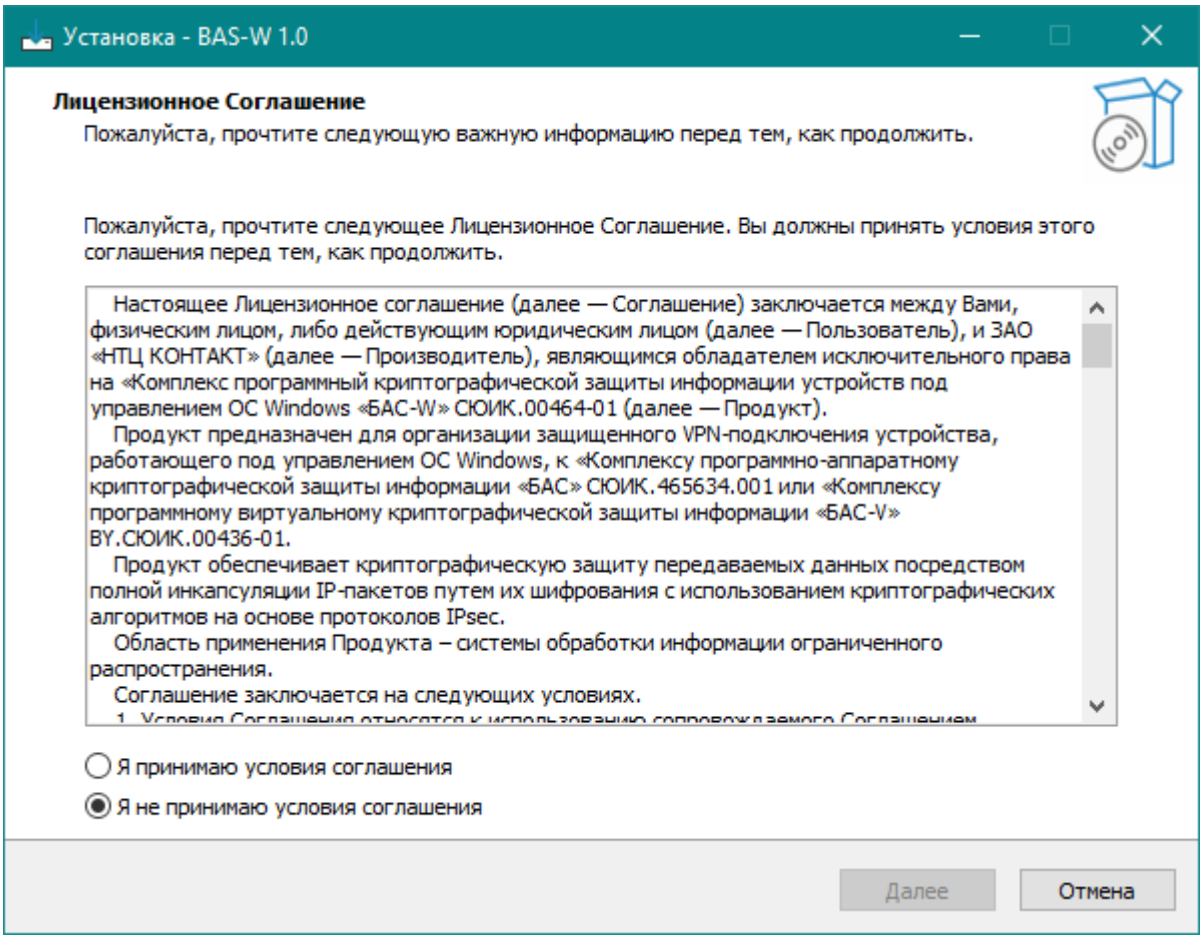

Рис. 2

3.1.4. Затем Администратору будет предложно выбрать место установки КП «БАС-W» (рис. 3). По умолчанию используется папка «%PROGRAMFILES%\NTC CONTACT\BAS-W». Администратор может выбрать другое место установки КП «БАС-W», при этом необходимо убедиться, что были выполнены работы по настройке среды, описанные в Разделе 2 настоящего Руководства.

Чтобы продолжить Администратор должен нажать кнопку «Далее». Чтобы вернуться на предыдущий шаг необходимо нажать кнопку «Назад».

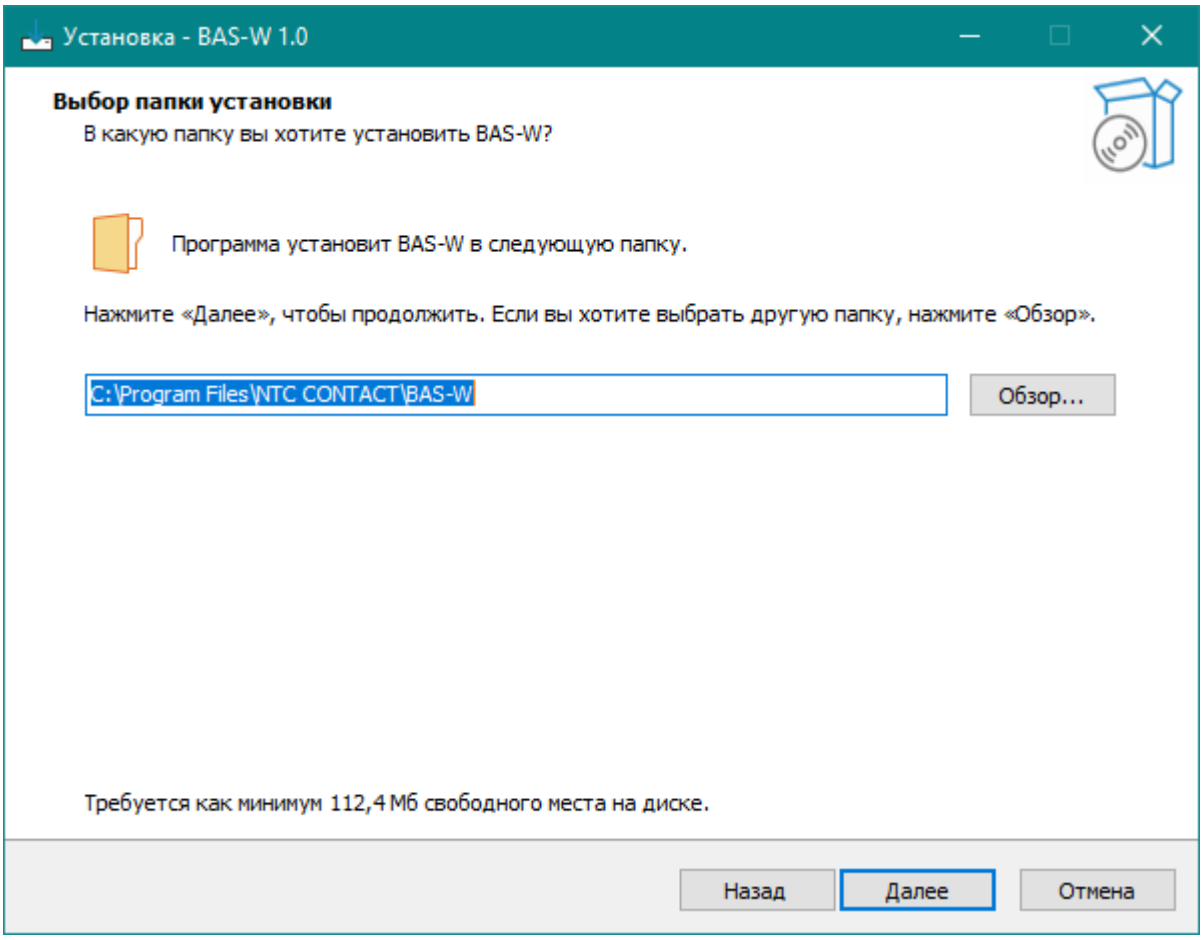

Рис. 3

3.1.5. Далее Администратору необходимо выбрать дополнительные параметры установки (рис. 4). Единственным дополнительным параметром установки является возможность создания значка (ярлыка) на Рабочем столе. При выборе параметра значок будет автоматически создан на Рабочем столе каждого пользователя данной ОС.

Чтобы продолжить Администратор должен нажать кнопку «Далее».

Чтобы вернуться на предыдущий шаг необходимо нажать кнопку «Назад».

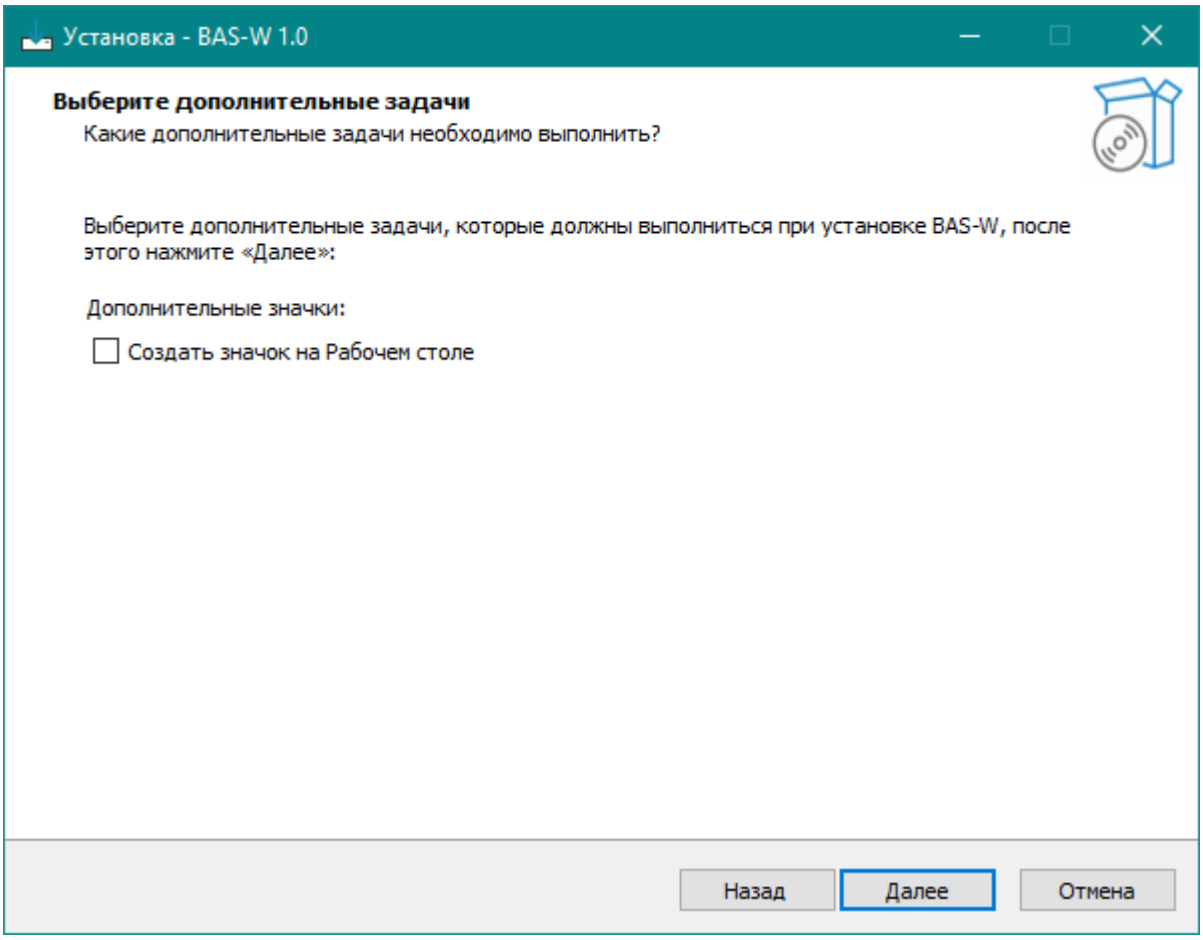

Рис. 4

3.1.6. Далее Администратору будет продемонстрировано окно с выбранными опциями установки (рис. 5). Чтобы начать установку Администратору необходимо нажать кнопку «Установить». Чтобы вернуться на предыдущий шаг необходимо нажать кнопку «Назад».

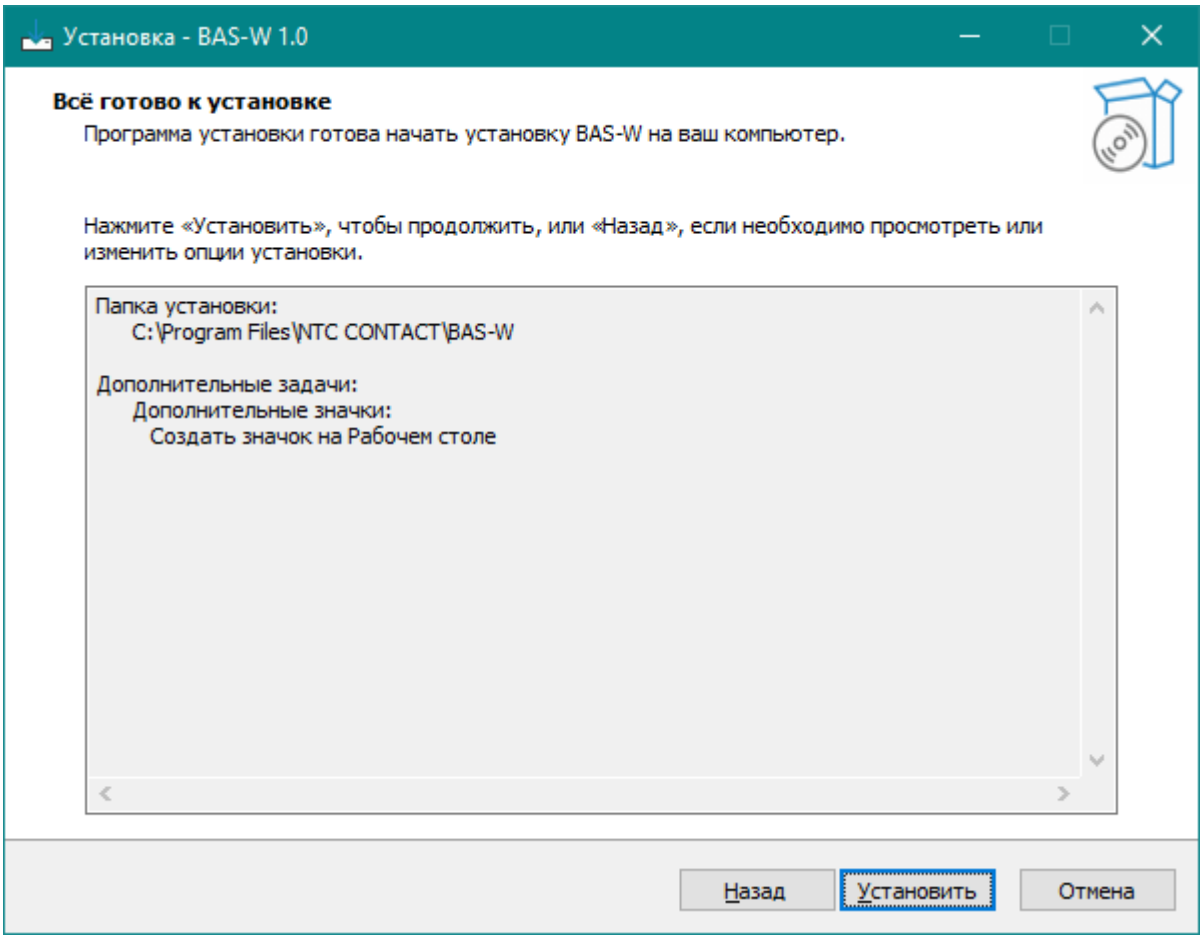

Рис. 5

3.1.7. После нажатия кнопки «Установить», начнется установка файлов КП «БАС-W» на жесткий диск ПЭВМ. В окне, представленном на рис. 6, отображается текущее состояние установки и индикатор выполнения. Сразу после распаковки файлов автоматически выполняется самотестирование КП «БАС-W», в ходе которого проверяются правильность работы криптографических алгоритмов, контроль целостности установленных файлов КП «БАС-W» и статистические параметры генератора случайных чисел.

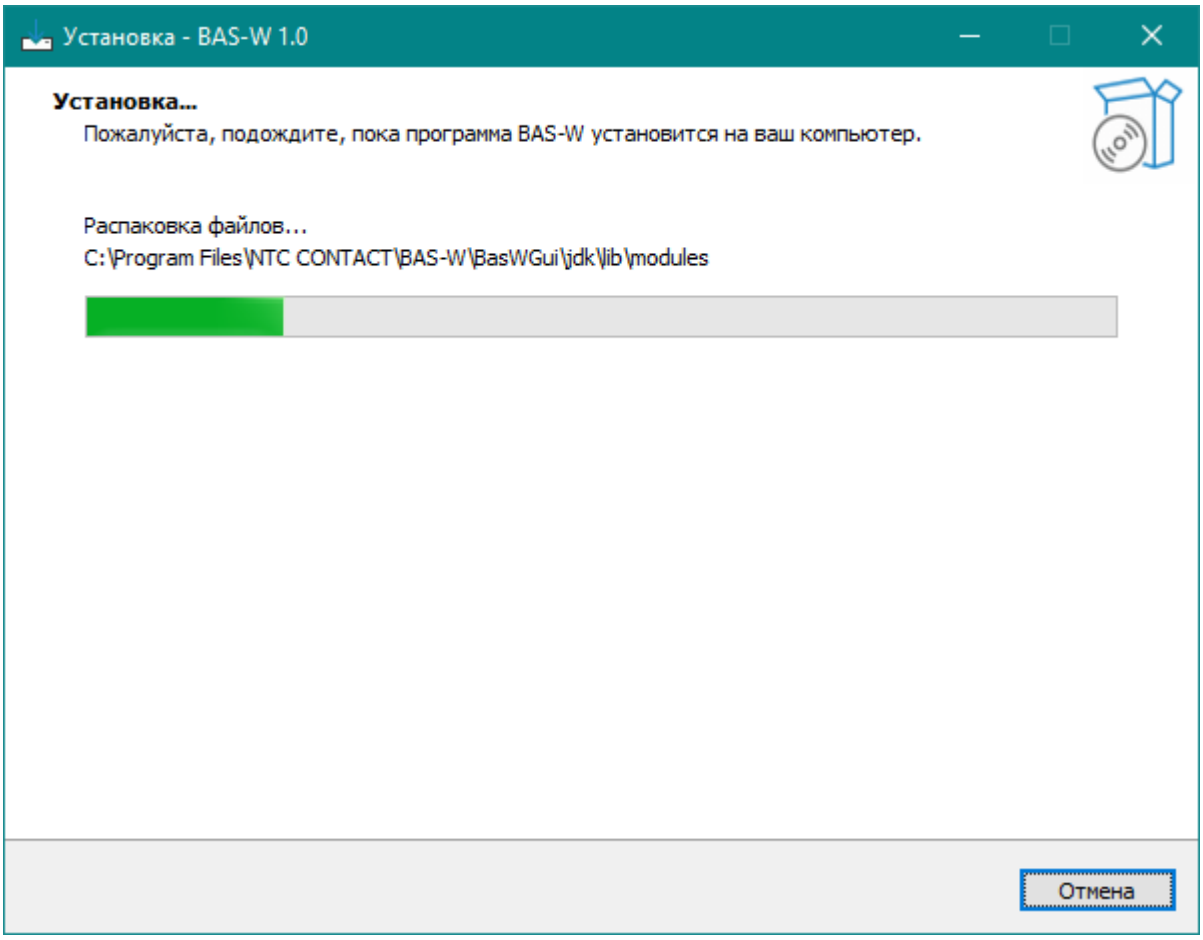

Рис. 6

3.1.9 После успешной установки и самотестирования Администратор получит сообщение о завершении работы мастера установки (рис. 7).

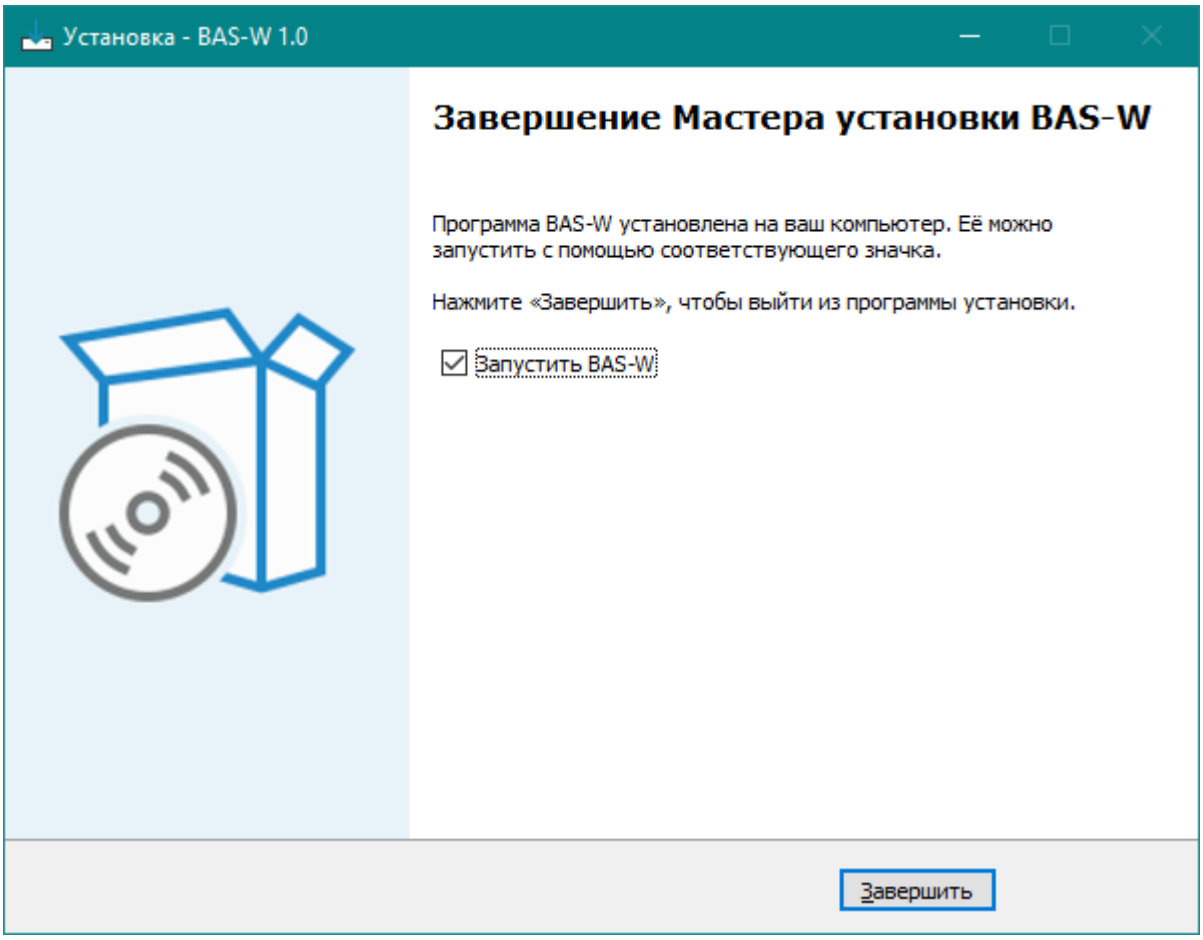

Рис. 7

3.1.10. При возникновении ошибки во время установки или самотестирования Администратор получит соответствующее сообщение и КП «БАС-W» будет удален с жесткого диска ПЭВМ.

3.1.11. Программа установки КП «БАС-W» обеспечивает защиту от создания нескольких копий КП «БАС-W» в системе. При попытке повторной установки КП «БАС-W» автоматически определяется наличие в системе установленного КП «БАС-W» и выполняется восстановление или переустановка (см. п. 3.4.).

3.2. Выполнение

Выполнение КП «БАС-W» доступно Пользователю после успешной аутентификации в ОС. При этом Пользователи должны хранить свои аутентификационные данные (пароль) в тайне.

Запустить КП «БАС-W» можно либо дважды кликнув левой клавишей мыши по иконке на рабочем столе (рис. 8), либо из меню «Пуск» (рис. 9).

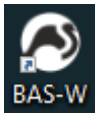

Рис. 8

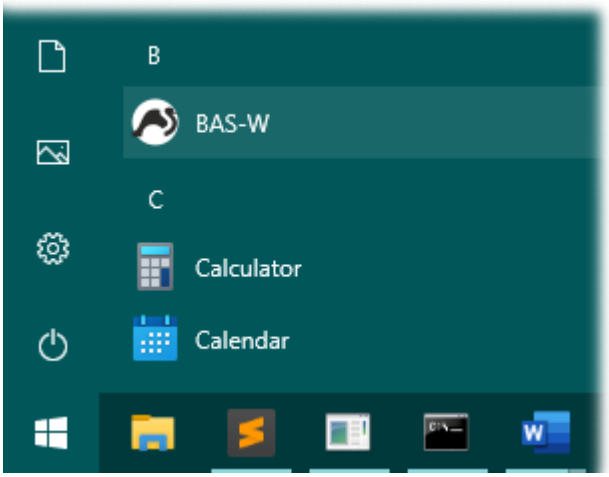

Рис. 9

КП «БАС-W» работает в системном трее панели задач ОС Windows (рис. 10).

Рис. 10

Обращение за функциями КП «БАС-W» осуществляется через контекстное меню (рис. 11), которое вызывается кликом правой клавиши мыши по иконке в системном трее.

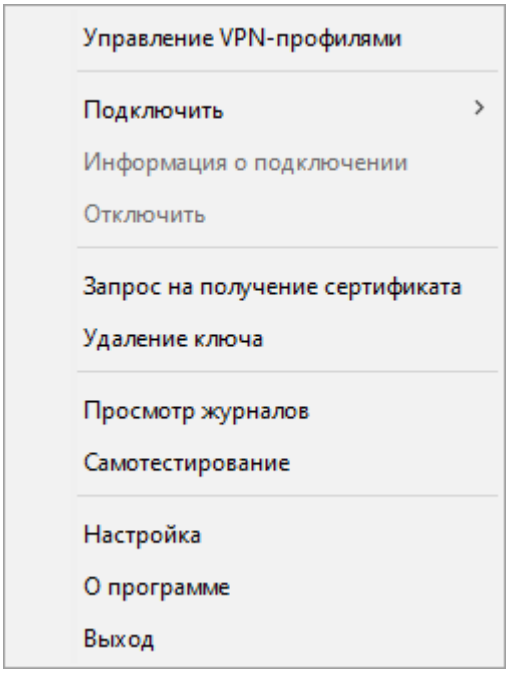

Рис. 11

КП «БАС-W» поддерживает три языка интерфейса: английский, белорусский и русский. Язык интерфейса устанавливается автоматически в зависимости от языка интерфейса ОС Windows. Настоящий документ описывает работу КП «БАС-W» с использованием русского языка.

3.2.1. Формирование запроса на получение сертификата

3.2.1.1. В КП «БАС-W» есть возможность сгенерировать ключевую пару для аутентификации, сформировать контейнер защищенного личного ключа и запрос на получение сертификата открытого ключа. Для этого необходимо в контекстном меню выбрать пункт «Запрос на получение сертификата».

Откроется окно, отображенное на рис. 12.

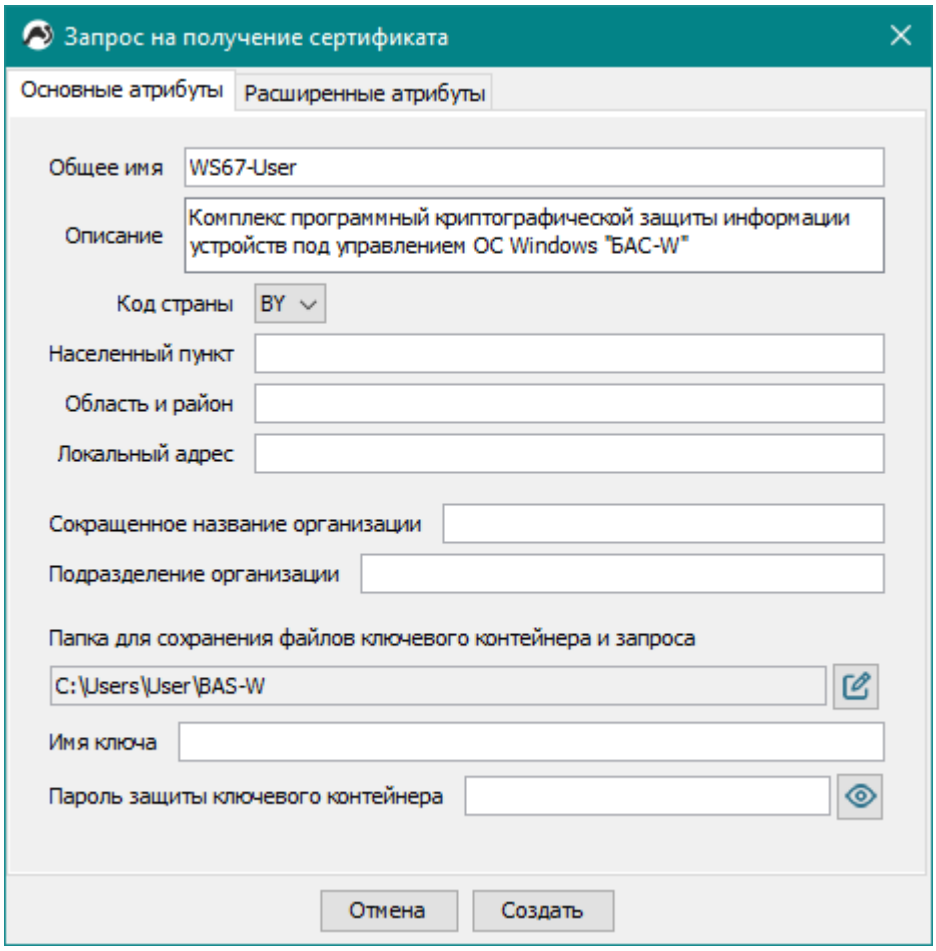

Рис. 12

В окне «Запрос на получение сертификата» есть две вкладки:

– вкладка «Основные атрибуты»;

– вкладка «Расширенные атрибуты».

3.2.1.2. Во вкладке «Основные атрибуты» обязательными полями для заполнения являются «Общее имя», «Населенный пункт», «Сокращенное название организации», «Имя ключа», «Пароль защиты ключевого контейнера».

Поле «Общее имя» по умолчанию заполняется значениями имени хоста и имени текущего пользователя, разделенными символом дефиса. Пользователь может изменить его. При этом необходимо использовать уникальное значение, которое позволяет идентифицировать Пользователя или устройство, на котором он работает (DNS-имя, IP-адрес, ID устройства).

Папка для сохранения файлов ключевого контейнера и запроса на получение сертификата по умолчанию устанавливается равной «%USERPROFILE%\BAS-W».

Значение поля «Имя ключа» будет частью названия файлов ключевых контейнеров и запроса на получение сертификата, а в сам запрос эта информация не будет включена. Имя ключа должно быть уникальным.

Пример заполнения полей представлен на рис. 13.

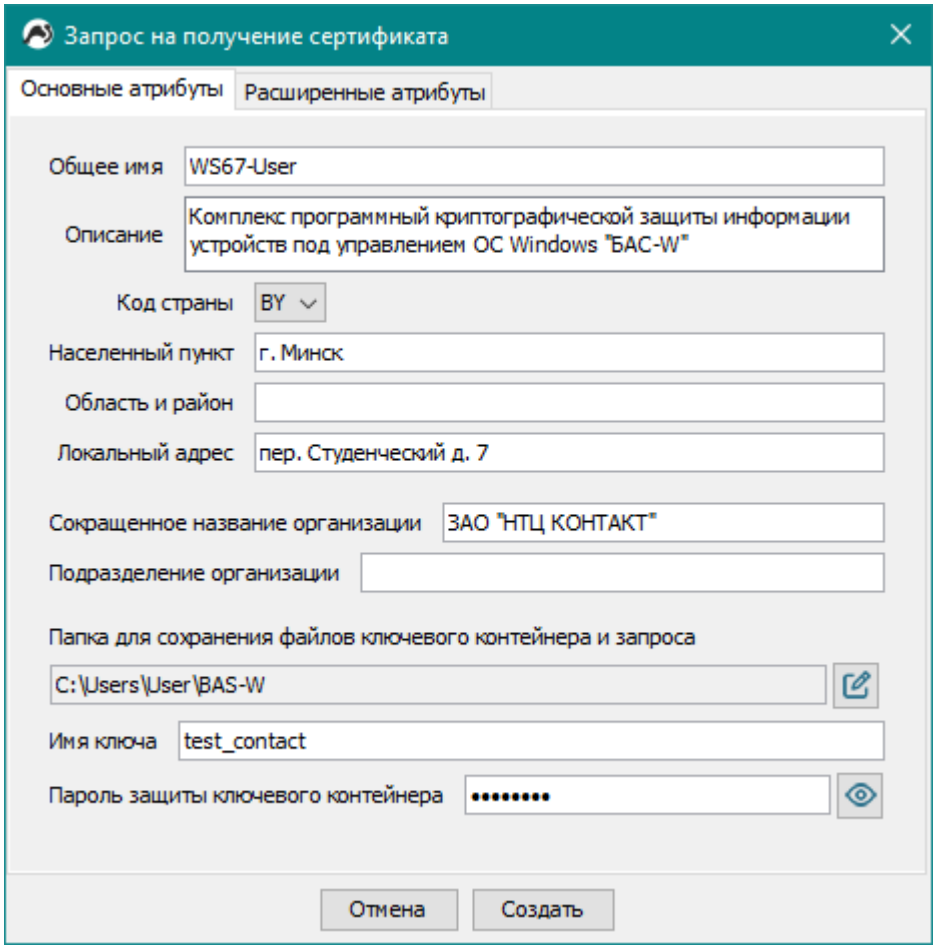

Рис. 13

3.2.1.3. На вкладке «Расширенные атрибуты» представлены дополнительные необязательные для заполнения поля (рис. 14).

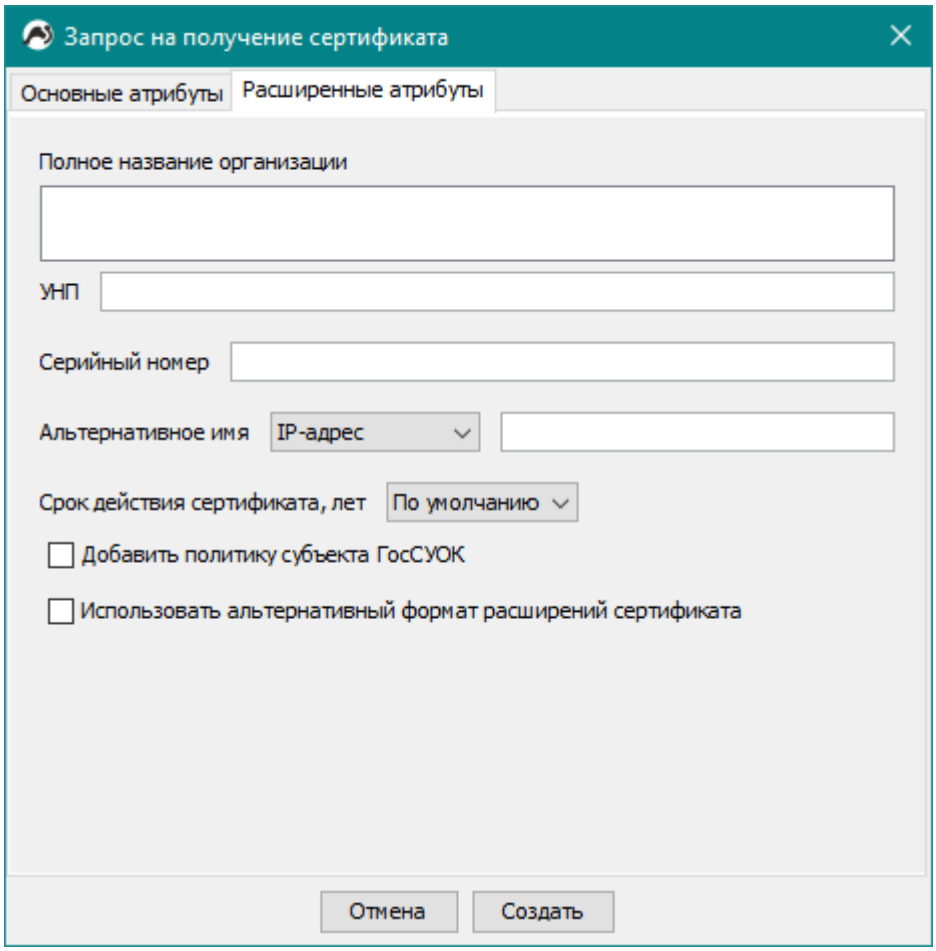

Рис. 14

Расширенные атрибуты могут понадобиться для специфических требований Удостоверяющего центра, который будет выпускать сертификат. Так, например, для Удостоверяющего центра ГосСУОК необходимо установить галочку «Добавить политику субъекта ГосСУОК».

3.2.1.4. Чтобы закрыть окно «Запрос на получение сертификата» без формирования ключевых контейнеров и запроса необходимо нажать либо кнопку закрытия окна в верхнем правом углу, либо кнопку «Отмена» в нижней части окна.

3.2.1.5. Для продолжения формирования ключевых контейнеров и запроса после заполнения полей необходимо нажать на кнопку «Создать» в нижней части окна.

3.2.1.6 Если какие-то из обязательных полей не будут заполнены или заполнены некорректно, то информация об этом отобразится в виде окон с сообщениями (рис. 15, 16).

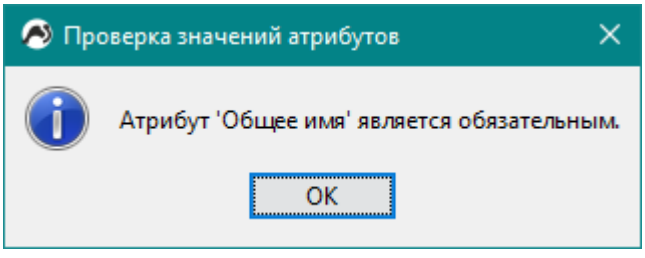

Рис. 15

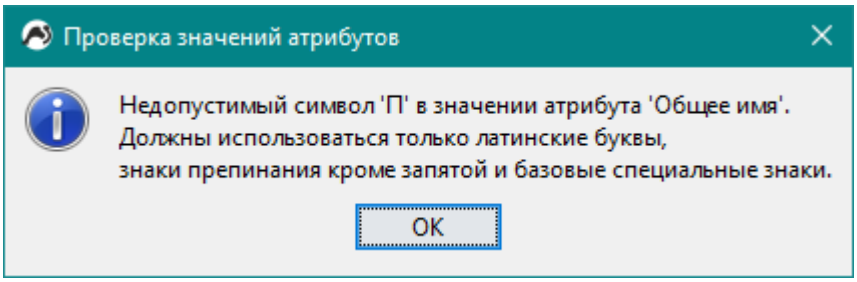

Рис. 16

3.2.1.7. Если поля заполнены корректно, после нажатия на кнопку «Создать» откроется окно «Накопление случайности». В нем необходимо накопить случайности для инициализации криптографического генератора псевдослучайных чисел путем нажатия клавиши клавиатуры. По мере накопления случайности будет заполняться индикатор выполнения (рис. 17).

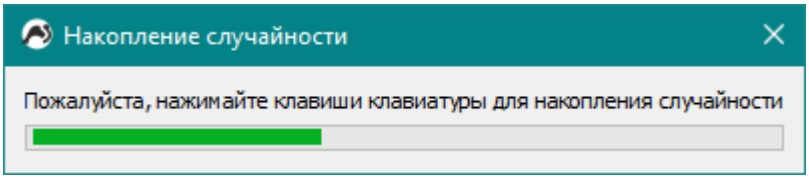

Рис. 17

3.2.1.8. В случае успеха сформируются четыре файла, описанные в табл. 1.

Таблица 1

Содержимое файла	Имя файла	Расположение файла
Запрос на выпуск сертификата	CertReq_*[имя_ключа]*.der	Папка для сохранения файлов ключевого контейнера и запроса на получение сертификата, указанная в окне «Запрос на получение сертификата»
Защищенный контейнер с личным ключом	PrivKey_*[имя_ключа]*.pkc	Системная папка КП «БАС-W»
Защищенный контейнер с первым частичным секретом	ShareKey1_*[имя_ключа]*.ssc	Системная папка КП «БАС-W»
Защищенный контейнер со вторым частичным секретом	KeyContainer_*[имя_ключа]*.ssc	Папка для сохранения файлов ключевого контейнера и запроса на получение сертификата, указанная в окне «Запрос на получение сертификата»

[имя_ключа] – это введенное пользователем значение поля «Имя ключа» в окне «Запрос на получение сертификата».

Для защиты личного ключа используется высокоэнтропийный ключ, сгенерированный с помощью криптографического генератора псевдослучайных чисел. Далее этот ключ делится на два частичных секрета с помощью алгоритма разделения секрета, а они в свою очередь защищаются на пароле, введенном пользователем в окне «Запрос на получение сертификата» в поле «Пароль защиты ключевого контейнера». Защищенный контейнер с личным ключом и

защищенный контейнер с первым частичным секретом сохраняются в системной папке КП «БАС-W», доступ к которой пользователю закрыт.

Пользователи должны хранить пароль защиты ключевого контейнера в тайне.

Если ключевые контейнеры и запрос на получение сертификата успешно сформированы, то отобразится сообщение с путями к файлу защищенного контейнера со вторым частичным секретом и к файлу запроса (рис. 18).

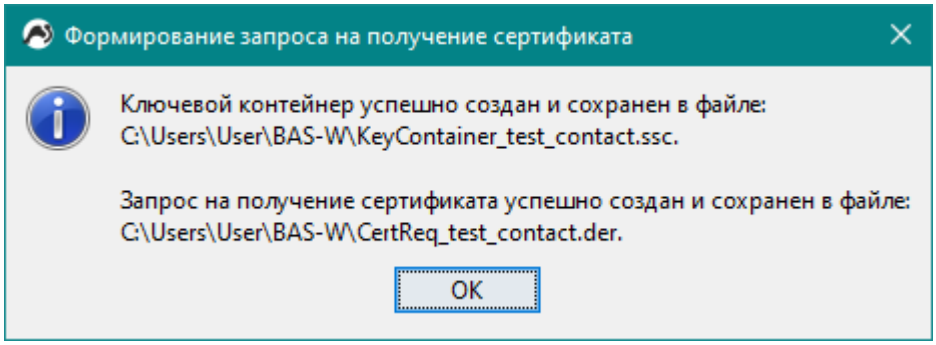

Рис. 18

3.2.1.9. Для безопасного использования ключей Пользователь должен переместить полученный ключевой контейнер с частичным секретом на внешний съемный носитель, удалить все копии ключевого контейнера, кроме внешнего съемного носителя, и ограничить доступ посторонних лиц к съемному.

3.2.1.10. Если во время формирования ключевых контейнеров или запроса на получение сертификата произошла ошибка, то на отобразится окно с сообщением, а подробности можно посмотреть в файле журнала (подробнее см. п. 3.2.4).

3.2.2. Управление VPN-профилями

VPN-профиль – набор параметров и характеристик VPN-подключения, включающий адрес сервера, тип аутентификации, параметры аутентификации, используемые криптографические алгоритмы и др.

Для управления VPN-профилями необходимо в контекстном меню выбрать пункт «Управление VPN-профилями», после чего отобразится окно, представленное на рис. 19.

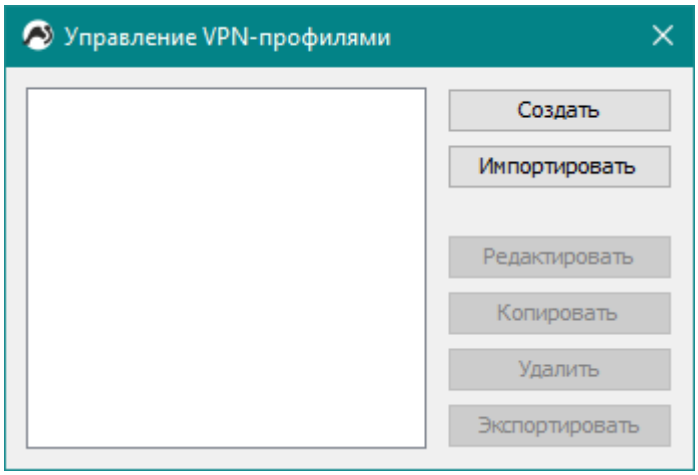

Рис. 19

В окне «Управление VPN-профилями» расположена область со списком уже существующих VPN-профилей и кнопки для управления. С помощью этого окна можно создавать и импортировать новые VPN-профили, а также редактировать, копировать, удалять и экспортировать уже существующие VPN-профили.

3.2.2.1. Создание VPN-профиля

3.2.2.1.1. Для создания нового VPN-профиля в окне «Управление VPN-профилями» необходимо нажать кнопку «Создать». Откроется окно «Создание VPN-профиля» (рис. 20).

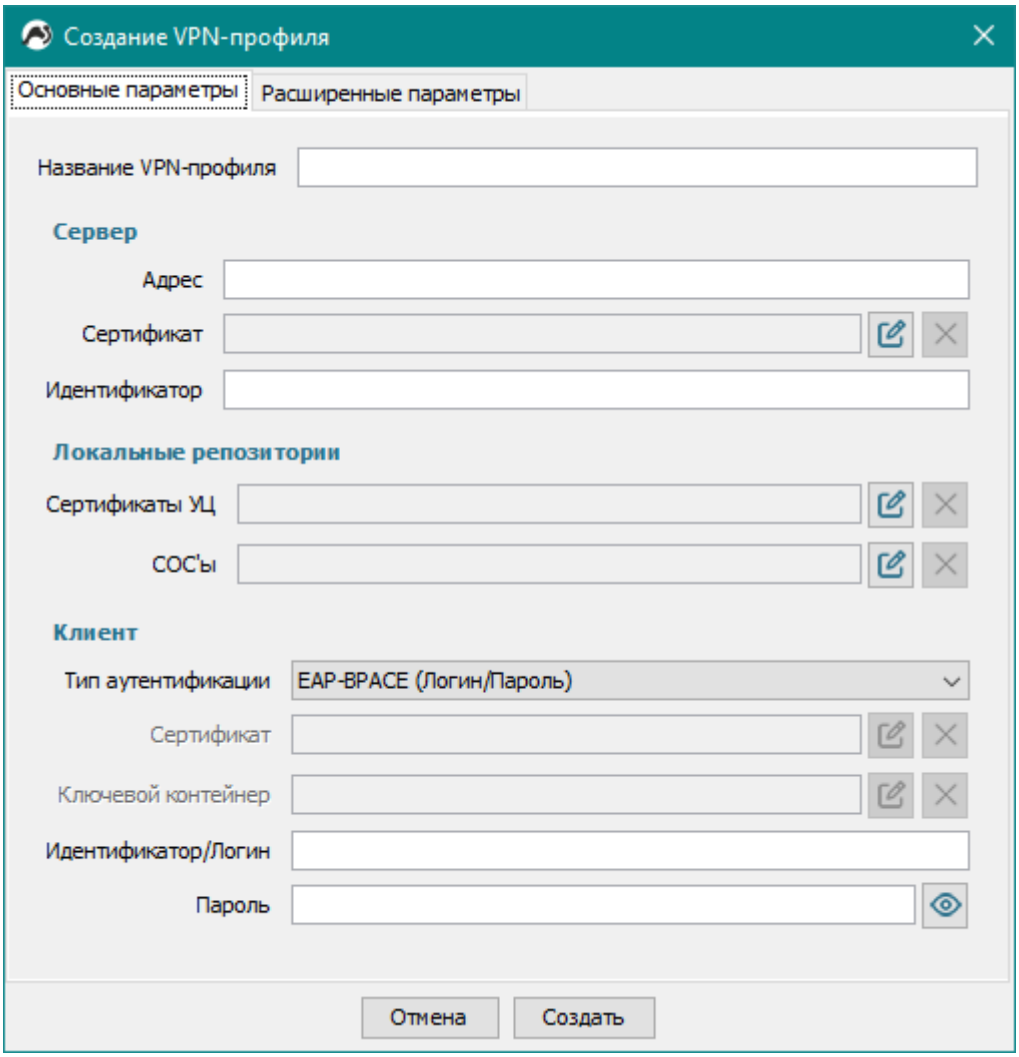

Рис. 20

В окне «Создание VPN-профиля» есть две вкладки:

– вкладка «Основные параметры»;

– вкладка «Расширенные параметры».

3.2.2.1.2. На вкладке «Основные параметры» поле «Название VPN-профиля» является обязательным для заполнения и его значение должно быть уникальным.

3.2.2.1.3. Секция «Сервер» содержит поля с характеристиками сервера. КП «БАС-W» выполняет защищенное VPN-подключение к ПАК «БАС» или КП «БАС-V».

Поле «Адрес» является обязательным для заполнения и должно содержать IP-адрес или имя хоста VPN-сервера.

Поле «Сертификат» секции «Сервер» является необязательным и может содержать сертификат сервера для аутентификации перед клиентом. Для выбора сертификата необходимо нажать кнопку  и в открывшемся окне выбора файла указать файл необходимого сертификата. Для отмены своего выбора необходимо нажать кнопку  справа от поля.

3.2.2.1.4. Локальные репозитории сертификатов удостоверяющих центров (УЦ) и списков отозванных сертификатов (СОС) являются необязательными характеристиками. Если они не заданы в VPN-профиле, то при подключении по умолчанию как репозитории сертификатов УЦ и СОСов обработаются папки «%ALLUSERSPROFILE%\BAS-W\x509ca» и «%ALLUSERSPROFILE%\BAS-W\x509crl» соответственно. Для выбора папки репозитория необходимо нажать кнопку  справа от соответствующего поля и в открывшемся окне выбора указать необходимую папку. Для отмены своего выбора необходимо нажать кнопку  справа от соответствующего поля.

3.2.2.1.5. Для успешной аутентификации сервера КП «БАС-W» должен иметь информацию о доверенном сервере, поэтому ему должен быть известен либо сертификат сервера, либо цепочка корневых сертификатов УЦ, выпустивших сертификат сервера.

3.2.2.1.6. В секции «Клиент» необходимо из выпадающего списка выбрать тип аутентификации:

– EAP-BPACE (Логин/Пароль) – аутентификация EAP протоколом BPACE в соответствии с СТБ 34.101.66, п. 7.6;

– EAP-BSTS (Сертификат/Личный ключ) – аутентификация EAP протоколом BSTS в соответствии с СТБ 34.101.66, п. 7.5;

– Сертификат/Личный ключ – аутентификация IKEv2 в соответствии с RFC 7296 «Internet Key Exchange Protocol Version 2 (IKEv2)» с протоколом Диффи-Хеллмана, описанным в СТБ 34.101.66, Приложение А.

Если выбрать тип аутентификации «EAP-BPACE (Логин/Пароль)», то поле «Идентификатор/Логин» становится обязательным для заполнения.

Если выбрать тип аутентификации «EAP-BSTS (Сертификат/Личный ключ)» или «Сертификат/Личный ключ», то обязательными для заполнения становятся поля «Сертификат» и «Ключевой контейнер».

Для выбора файла сертификата и файла ключевого контейнера необходимо нажать кнопку  справа от соответствующего поля и в открывшемся окне выбора указать необходимый файл. Для отмены своего выбора необходимо нажать кнопку  справа от соответствующего поля.

В поле «Ключевой контейнер» необходимо выбрать файл защищенного контейнера второго частичного секрета. Имя файла должно соответствовать шаблону «KeyContainer_*[имя_ключа]*.ssc», где *[имя_ключа]* – это введенное пользователем значение поля «Имя ключа» в окне «Запрос на получение сертификата» при формировании запроса.

Поле «Пароль» необязательное для заполнения. Может содержать пароль аутентификации для подключения к серверу или пароль снятия защиты с личного ключа. Если поле оставить пустым, то КП «БАС-W» запросит пароль непосредственно во время подключения. Если пароль указан, то он сохраняется в диспетчере учетных данных ОС Windows.

Для просмотра введенного пароля можно нажать кнопку справа от поля. Чтобы снова скрыть пароль необходимо нажать кнопку .

Пользователи должны хранить пароль защиты ключевого контейнера и пароль аутентификации для подключения к серверу в тайне.

3.2.2.1.7. Пример заполнения основных полей профиля с типом аутентификации «EAP-BPACE (Логин/Пароль)» представлен на рис. 21.

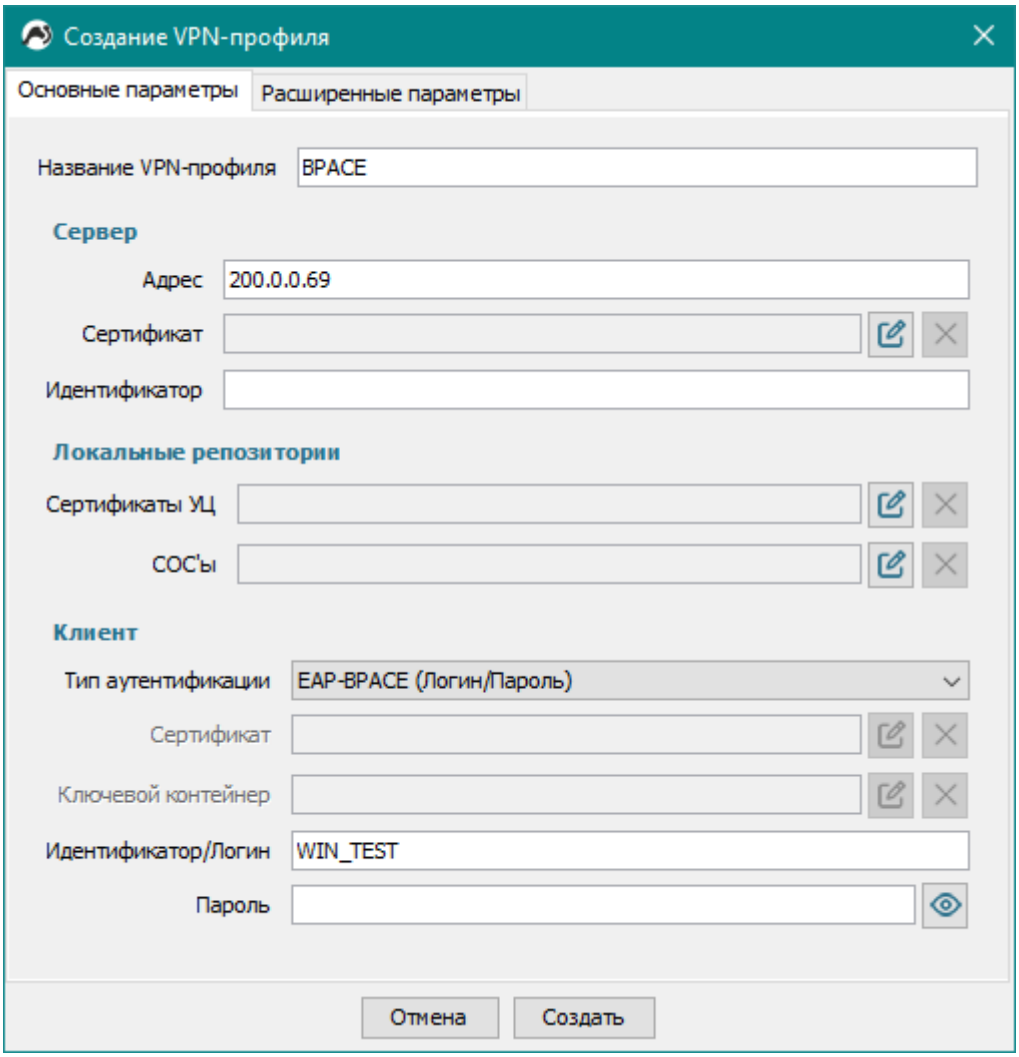

Рис. 21

3.2.2.1.8. Пример заполнения основных полей профиля с типом аутентификации «EAP-BSTS (Сертификат/Личный ключ)» представлен на рис. 22. Для типа аутентификации «Сертификат/Личный ключ» поля заполняются аналогично.

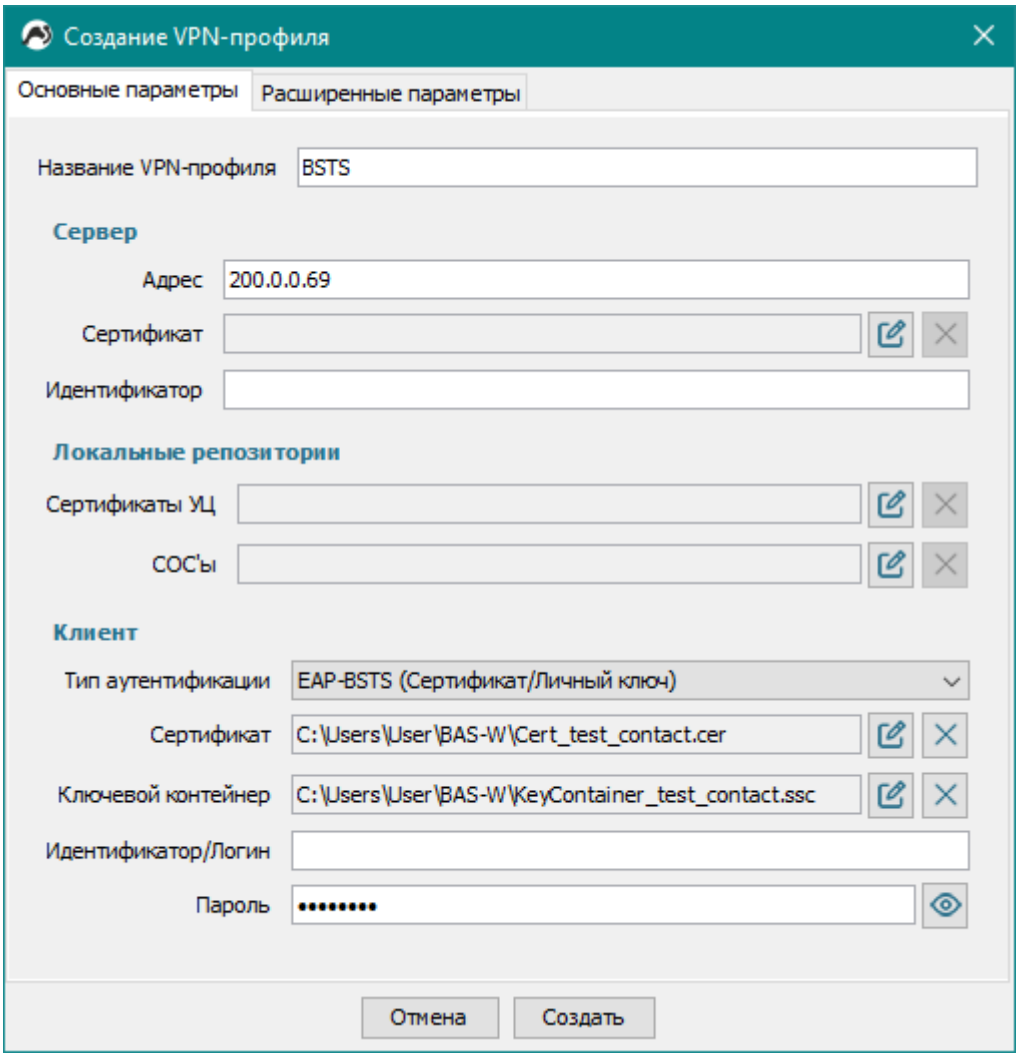

Рис. 22

3.2.2.1.9. На вкладке «Расширенные параметры» (рис. 23) можно указать дополнительные характеристики подключения. Поля расширенных параметров содержат подробное описание. Оно отображается при наведении курсора мыши на поле параметра.

3.2.2.1.10. При установке галочки «Запрос IP адреса» (по умолчанию) в ОС создается виртуальный интерфейс, которому присваивается IP-адрес, полученный из пула сервера, при этом защищаемая информация будет передаваться с этого интерфейса и адреса.

При снятии галочки «Запрос IP адреса» дополнительный IP-адрес не будет запрашиваться у сервера при установке соединения, при этом защищаемая информация будет передаваться с физического интерфейса и адреса.

3.2.2.1.11. Установленная галочка «Строгая проверка статуса сертификата» означает, что аутентификация завершится ошибкой не только, если сертификат сервера был отозван, но и если его статус не удалось установить (например, из-за сбоя OCSP и отсутствия действительного СОС).

Снятая галочка «Строгая проверка статуса сертификата» означает, что в случае, когда не удалось установить статус сертификата сервера, он считается действительным.

ВНИМАНИЕ: Снимая галочку «Строгая проверка статуса сертификата», Пользователь подтверждает, что он осознает, что его действие может привести к снижению безопасности подключения.

3.2.2.1.12. При обращении к сайту по его DNS имени ОС Windows формирует DNS-запрос, который рассылает со всех своих IP-адресов. Таким образом может сложиться ситуация, когда Пользователь защитит данные, передаваемые или получаемые с определенного сайта, но при этом злоумышленник, анализируя трафик DNS-запросов, сможет узнать DNS-имя и IP-адрес сайта, к которому обращается Пользователь.

Установка галочки «Защита от утечки данных через DNS» позволяет заблокировать DNS-запросы в открытом виде. При этом DNS-запросы с виртуального интерфейса и адреса будут отправляться в защищенном виде.

3.2.2.1.13 В поле «Порт сервера» можно задать порт ПАК «БАС» или КП «БАС-V», к которому будет выполняться подключение, отличный от используемого по умолчанию. При этом этот же порт должен быть задан в настройках сервера. По умолчанию используется 500 порт с переходом на 4500.

3.2.2.1.14. В поле «Период DPD» можно задать период протокола обнаружения отказавших узлов (DPD) в секундах. Определяет временной интервал, с которым отправляются сообщения для проверки работоспособности узла IPsec. По умолчанию период равен 30 с.

3.2.2.1.15. Также можно задать пользовательские алгоритмы шифрования, контроля целостности, выработки псевдослучайных чисел, Диффи-Хеллмана, преобразования ключа для IKEv2 и IPsec/ESP. Описание допустимых значений для каждой группы алгоритмов приведен в Приложении А.

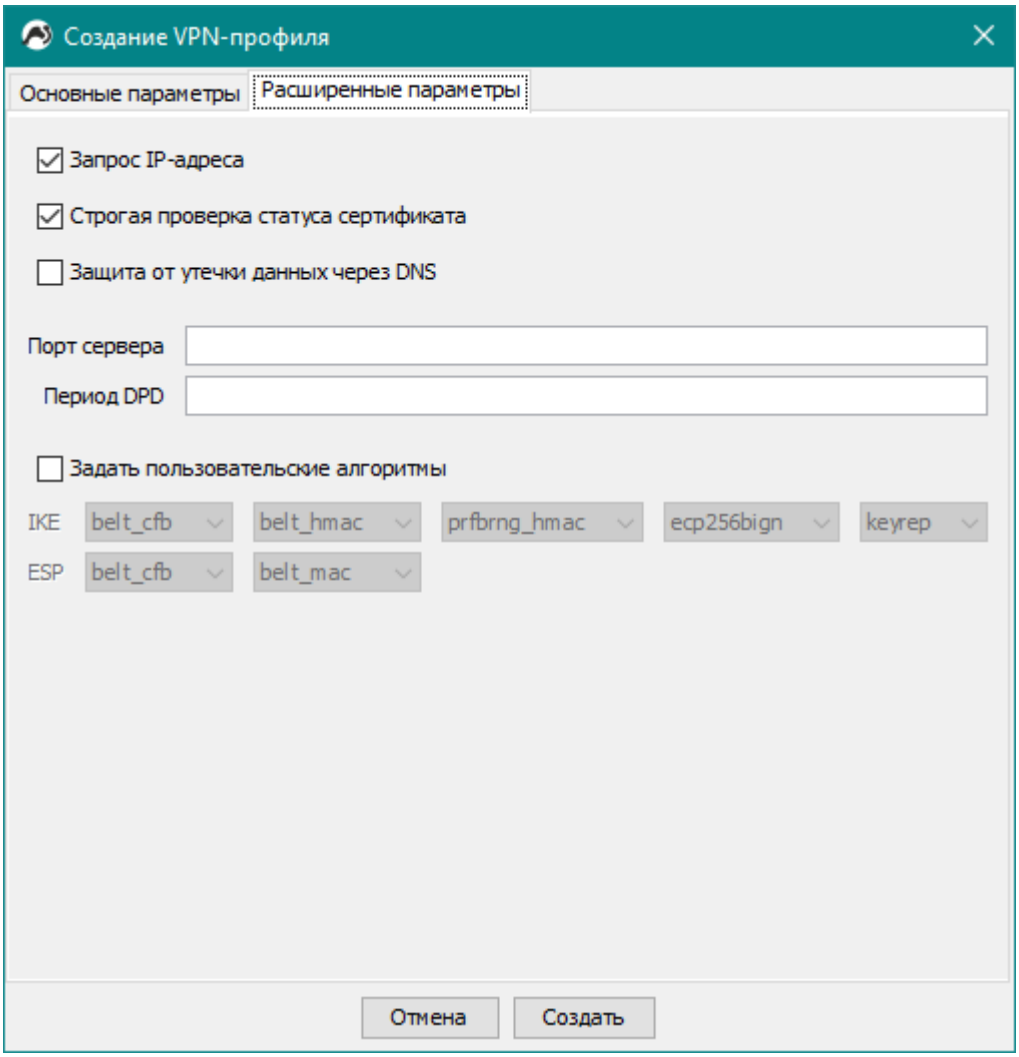

Рис. 23

3.2.2.1.16. Чтобы закрыть окно «Создание VPN-профиля» без сохранения VPN-профиля необходимо нажать либо кнопку закрытия окна в верхнем правом углу, либо кнопку «Отмена» в нижней части окна.

3.2.2.1.17. Для сохранения VPN-профиля нажать на кнопку «Создать» в нижней части окна. Если какие-то из обязательных полей не будут заполнены или заполнены некорректно, то информация об этом отобразится в виде окон с сообщениями (например, рис. 24-26).

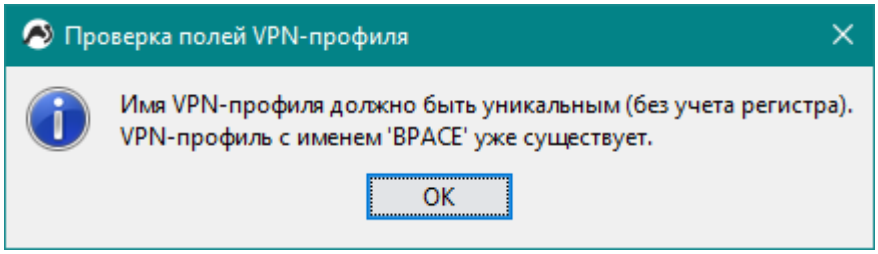

Рис. 24

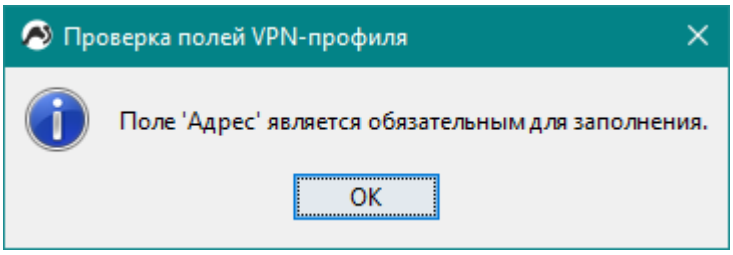

Рис. 25

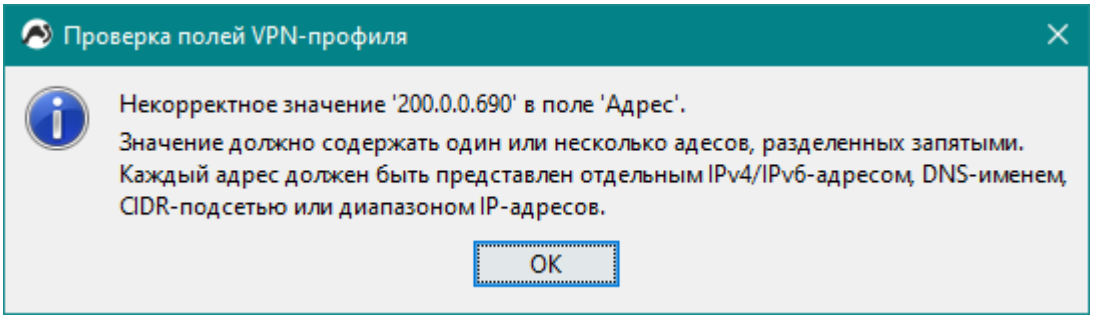

Рис. 26

3.2.2.1.18. Если поля корректно заполнены, после нажатия на кнопку «Создать» VPN-профиль сохраняется файл «%USERPROFILE%\BAS-W\profiles*[название_профиля]*.profile», где *[название_профиля]* – это введенное пользователем значение поля «Название VPN-профиля», окно «Создание VPN-профиля» закрывается, а в окне «Управление VPN-профилями» в списке отображается имя созданного профиля (рис. 27).

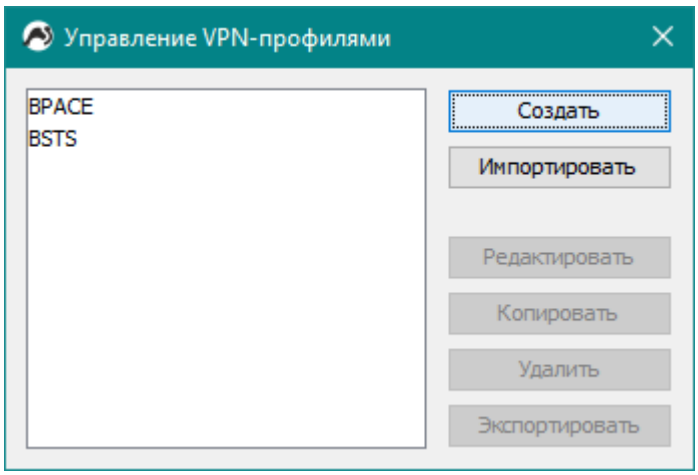

Рис. 27

3.2.2.2. Импорт VPN-профиля

Для импорта VPN-профиля в окне «Управление VPN-профилями» необходимо нажать кнопку «Импортировать». Откроется стандартное окно выбора файла, в котором необходимо указать файл VPN-профиля с расширением «.profile» и нажать кнопку «Импортировать» (рис. 28).

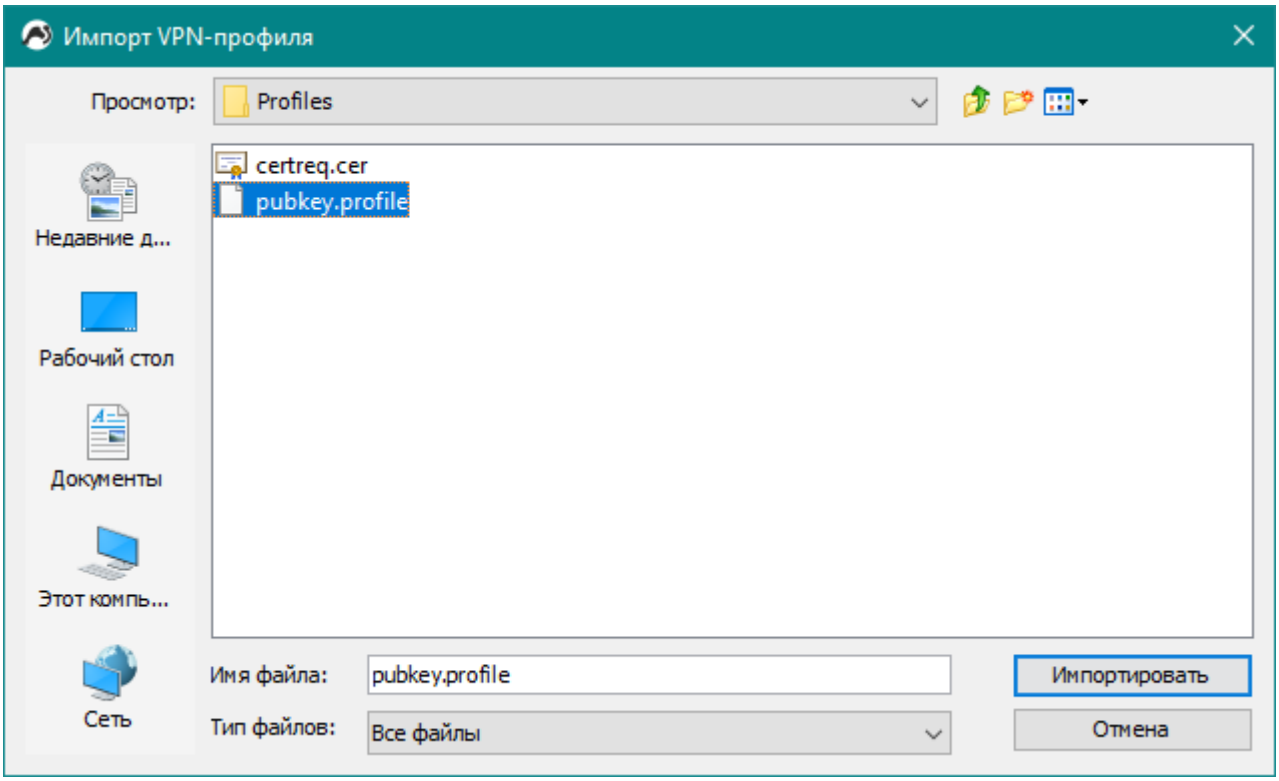

Рис. 28

В случае успешного импорта VPN-профиля отобразится окно с соответствующим сообщением (рис. 29), а в список VPN-профилей в окне «Управление VPN-профилями» добавится имя импортированного VPN-профиля (рис. 30).

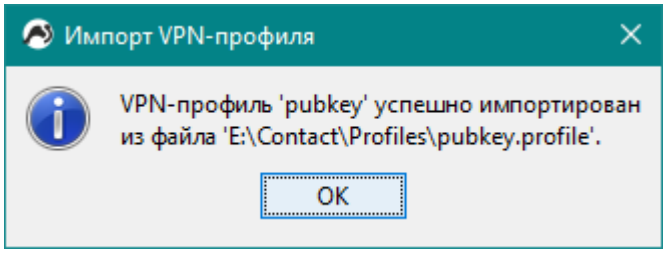

Рис. 29

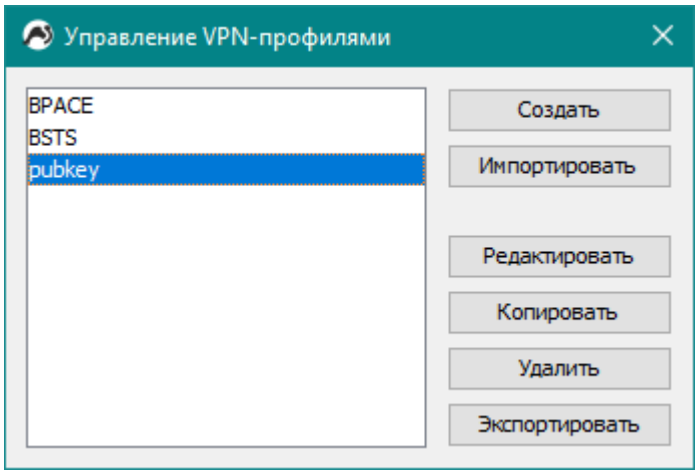

Рис. 30

Если во время импорта произошла ошибка, то отобразится окно с соответствующим сообщением (рис. 31)

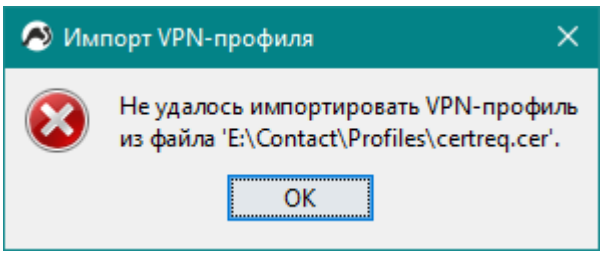

Рис. 31

3.2.2.3. Редактирование VPN-профиля

Для редактирования в окне «Управление VPN-профилями» в списке необходимо выделить VPN-профиль и нажать кнопку «Редактировать». Откроется окно, отображенное на рис. 32.

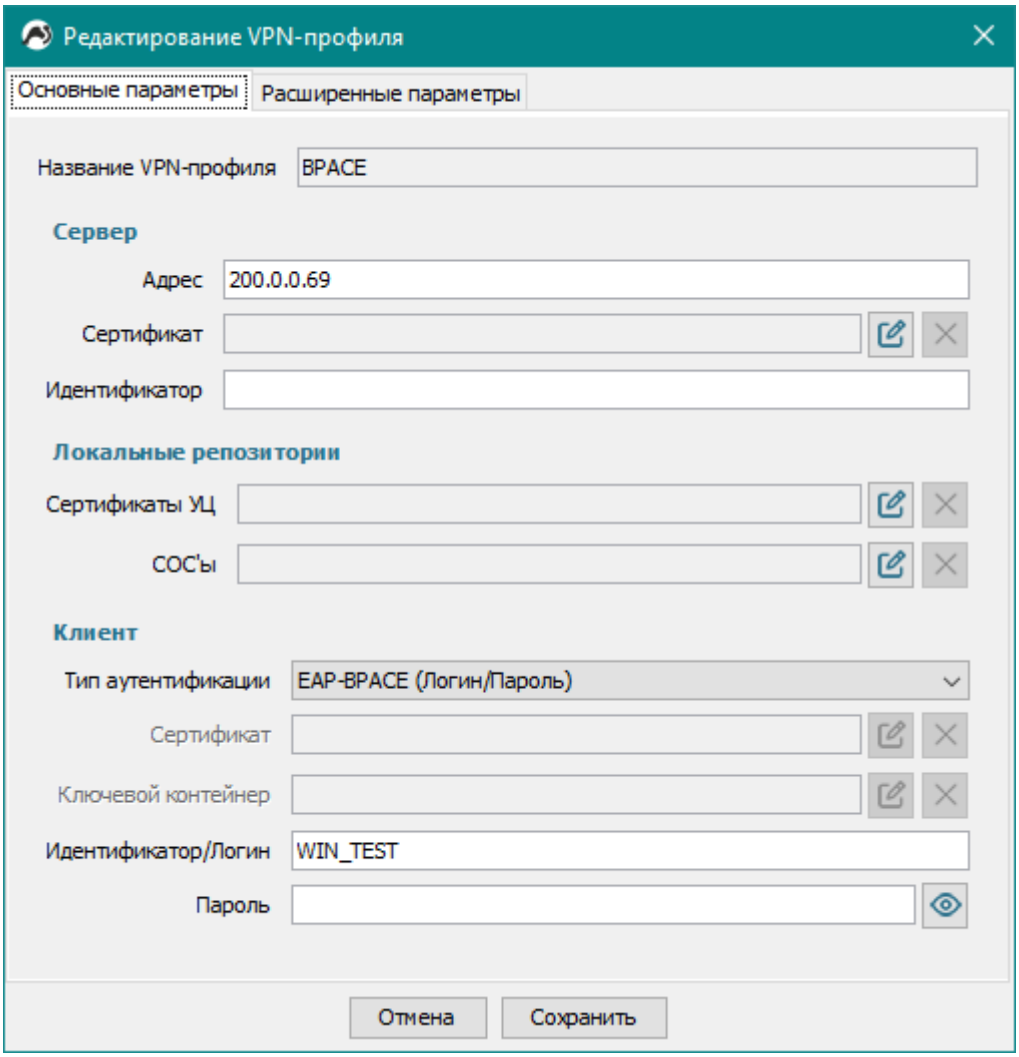

Рис. 32

Окно «Редактирование VPN-профиля» отличается от окна «Создание VPN-профиля» только тем, что при редактировании нельзя изменить название VPN-профиля.

Для сохранения внесенных изменений необходимо нажать кнопку «Сохранить».

Чтобы закрыть окно «Редактирование VPN-профиля» без сохранения внесенных изменений необходимо нажать либо кнопку закрытия окна в верхнем правом углу, либо кнопку «Отмена» в нижней части окна.

3.2.2.4. Копирование VPN-профиля

Для копирования существующего VPN-профиля в окне «Управление VPN-профилями» в списке необходимо выделить VPN-профиль и нажать кнопку «Копировать». Откроется окно с полем для ввода имени нового VPN-профиля (рис. 33).

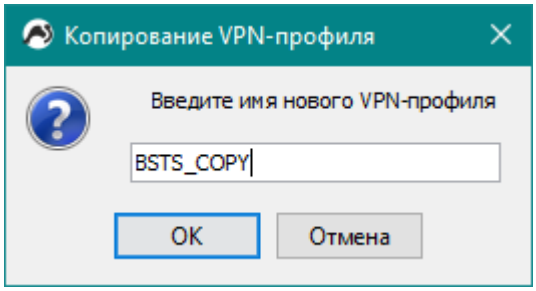

Рис. 33

Если имя нового VPN-профиля корректно, то оно добавится в список VPN-профилей в окне «Управление VPN-профилями» (рис. 34).

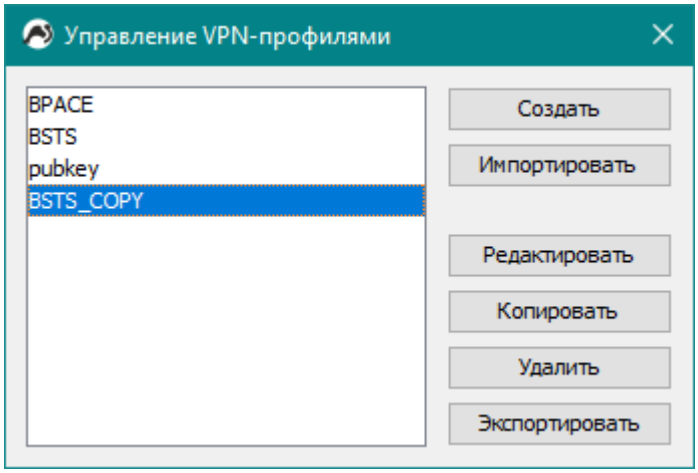

Рис. 34

Если введенное имя содержит недопустимые символы или VPN-профиль с введенным именем уже существует, то отобразится окно с соответствующим сообщением (рис. 35, 36).

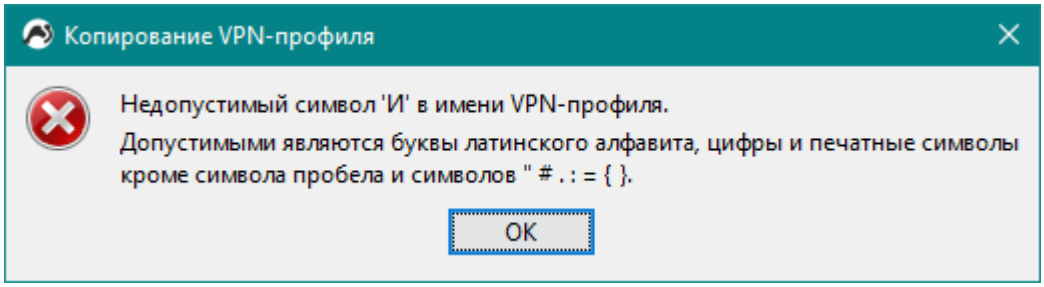

Рис. 35

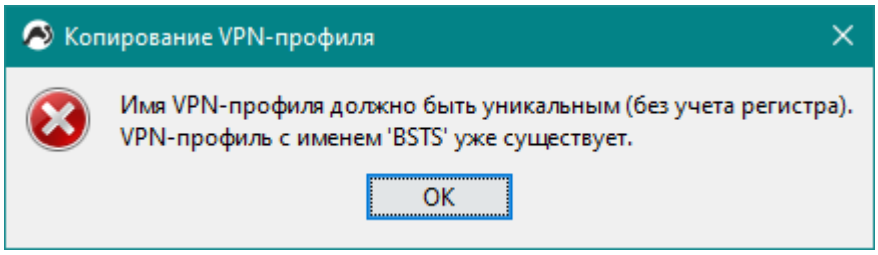

Рис. 36

3.2.2.5. Удаление VPN-профиля

Для удаления существующего VPN-профиля в окне «Управление VPN-профилями» в списке необходимо выделить VPN-профиль и нажать кнопку «Удалить». Откроется окно для подтверждения удаления (рис. 37).

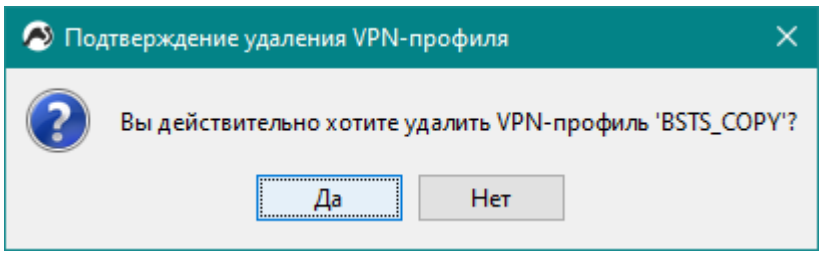

Рис. 37

Для подтверждения удаления необходимо нажать кнопку «Да», после чего выделенный VPN-профиль удалится из списка в окне «Управление VPN-профилями».

Для отмены удаления VPN-профиля необходимо нажать кнопку «Нет».

3.2.2.6. Экспорт VPN-профиля

Экспорт VPN-профиля представляет собой сохранение VPN-профиля в файл в указанное оператором место на диске.

Для экспорта VPN-профиля в файл в окне «Управление VPN-профилями» в списке необходимо выделить VPN-профиль и нажать кнопку «Экспорт». Откроется стандартное окно сохранения файла, в котором необходимо указать место сохранения файл VPN-профиля и возможно имя файла и нажать кнопку «Сохранить» (рис. 38).

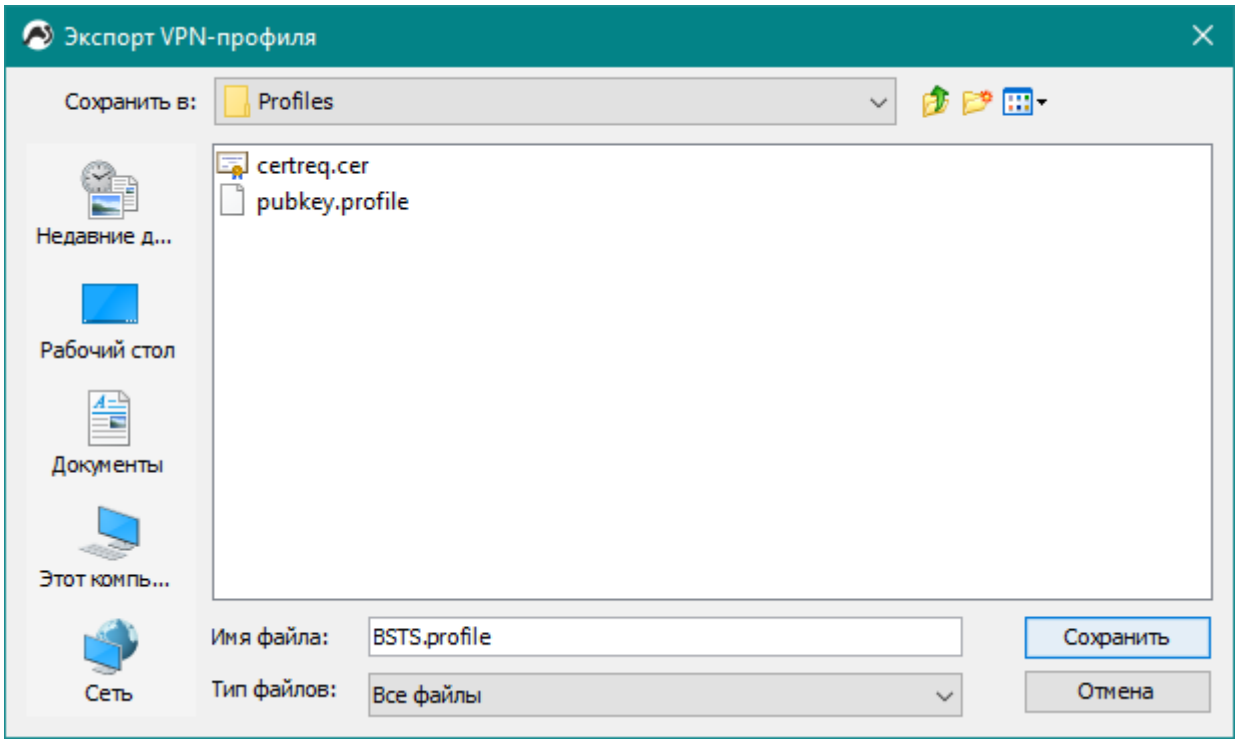

Рис. 38

В случае успешного сохранения файла VPN-профиля отобразится окно с соответствующим сообщением (рис. 39), а в указанном месте создастся файл VPN-профиля.

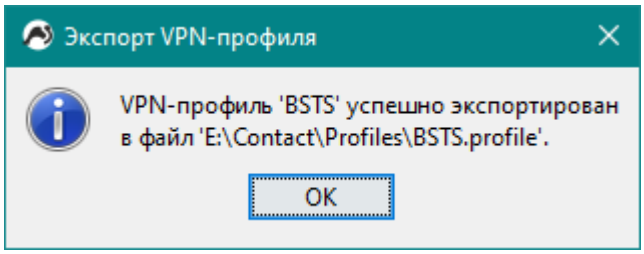

Рис. 39

3.2.3. Управление подключением

При отсутствии действующего VPN-подключения, иконка КП «БАС-W» в системном трее имеет белый фон, а при наведении курсора мыши на нее всплывает текстовое сообщение, представленное на рис. 40.

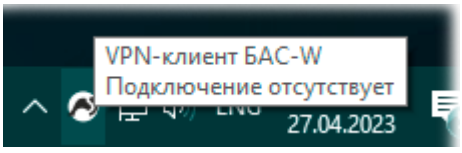

Рис. 40

3.2.3.1. Подключение VPN-профиля

Для того чтобы установить подключение к VPN-серверу необходимо вызвать контекстное меню КП «БАС-W», навести курсор мыши на пункт «Подключить» и в появившемся списке подменю выбрать нужный VPN-профиль (рис. 41).

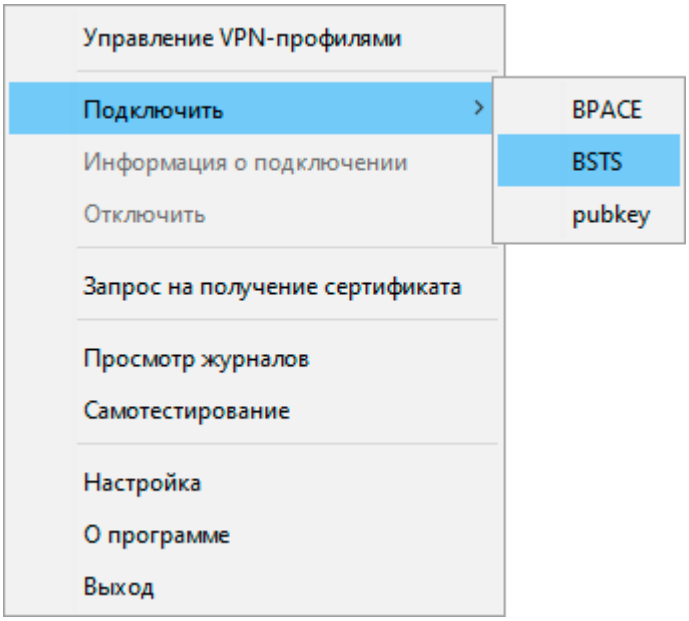

Рис. 41

Если при создании VPN-профиля не был указан пароль аутентификации, то перед подключением он запрашивается с помощью окна с полем для ввода (рис. 42).

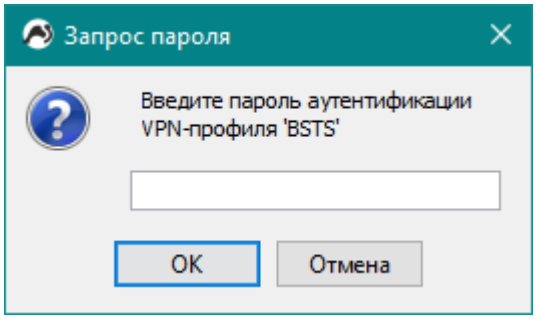

Рис. 42

При выполнении подключение VPN-профиля иконка КП «БАС-W» в системном трее меняет цвет фона на желтый, а при наведении курсора мыши на нее всплывает текстовое сообщение, представленное на рис. 43.

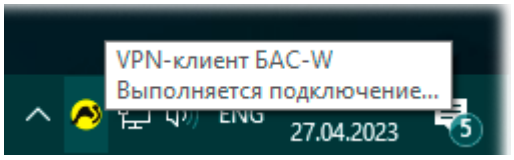

Рис. 43

При успешном подключении VPN-профиля отображается всплывающее сообщение (рис. 44), фон иконки КП «БАС-W» в системном трее становится зеленого цвета, а при наведении

курсора мыши на иконку всплывает текстовое сообщение с информацией о том, какой VPN-профиль сейчас подключен, и какой IP-адрес назначен клиенту (рис. 45).

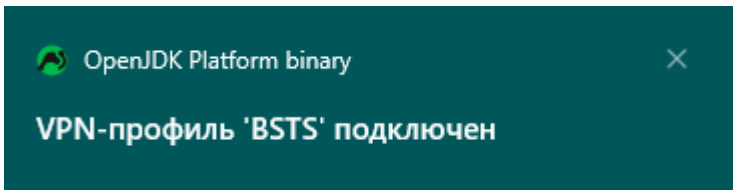

Рис. 44

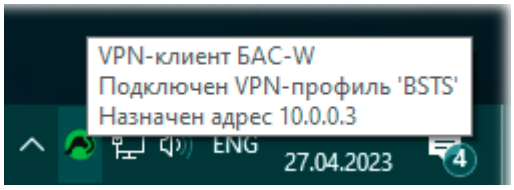

Рис. 45

Если во время подключения VPN-профиля произошла ошибка, то отображается соответствующее всплывающее сообщение (рис. 46). Подробно об ошибке можно узнать, просмотрев журнал сообщений (подробнее см. п. 3.2.4).

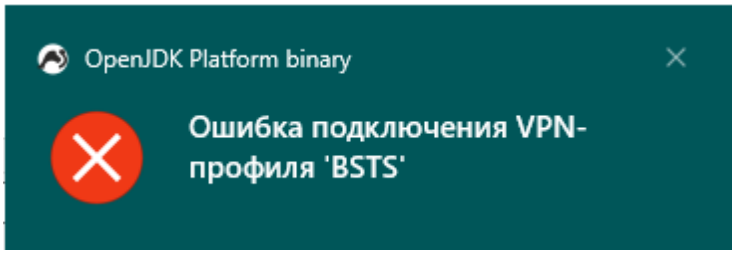

Рис. 46

3.2.3.2. Просмотр информации о подключении

Когда VPN-профиль подключен в контекстном меню КП «БАС-W» становится доступен пункт «Информация о подключении», при выборе которого открывается одноименное окно (рис. 47). В этом окне отображена следующая информация:

– название подключенного VPN-профиля;

– политика защищаемого трафика;

– согласованные алгоритмы IKE и ESP;

– количество отправленных и полученных байтов/пакетов с момента последней смены ключей или переаутентификации;

– время, прошедшее с последней смены ключей и переаутентификации, а также информация о том, когда запланированы следующие смена ключей и переаутентификация.

Информация в окне обновляется каждую секунду.

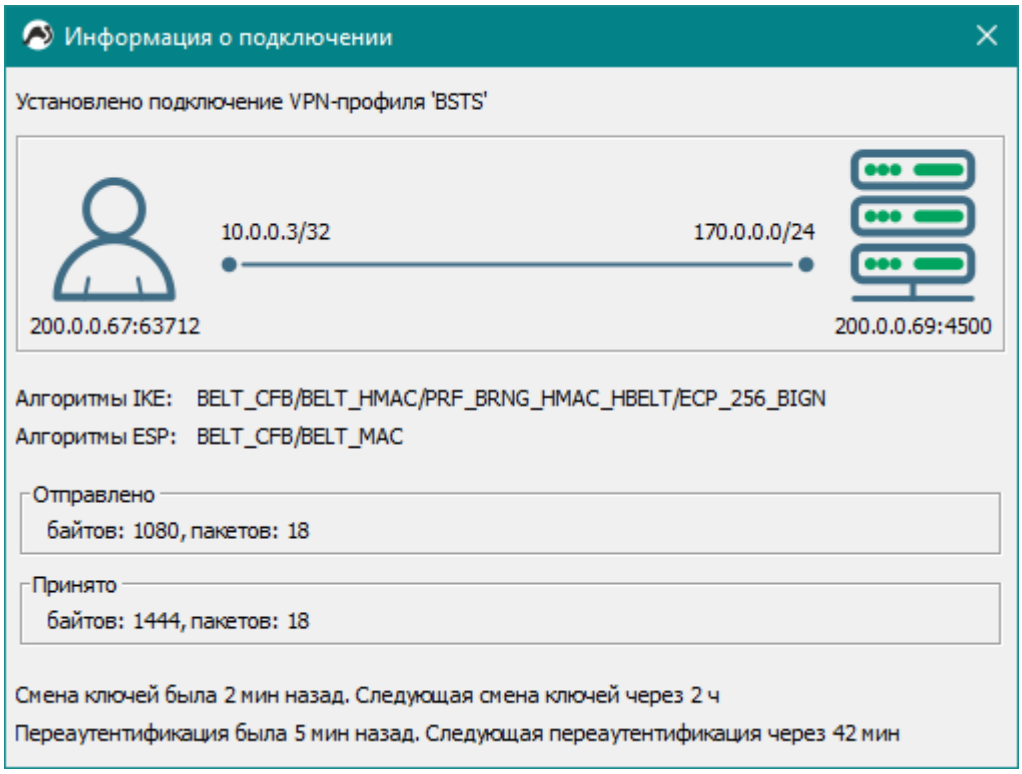

Рис. 47

3.2.3.3. Отключение VPN-профиля

Для отключения подключенного VPN-профиля необходимо вызвать контекстное меню КП «БАС-W» и выбрать пункт «Отключить».

После отключения отображается всплывающее сообщение (рис. 48), а иконка КП «БАС-W» в системном трее снова становится как на рис. 40.

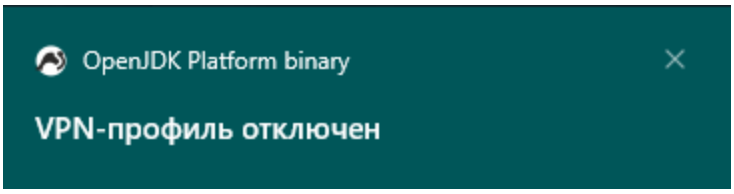

Рис 48

3.2.4. Удаление ключа

3.2.4.1 Для того, чтобы полностью удалить личный ключ, необходимо вызвать контекстное меню и выбрать пункт «Удаление ключа». Откроется окно, представленное на рис. 49.

3.2.4.2. В окне «Удаление ключа» необходимо указать файл защищенного контейнера с частичным секретом, принадлежащий Пользователю, и пароль защиты.

Для выбора файла защищенного контейнера необходимо нажать кнопку  и в открывшемся окне выбора файла указать файл необходимого контейнера.

Для просмотра введенного пароля можно нажать кнопку  справа от поля. Чтобы снова скрыть пароль необходимо нажать кнопку  .

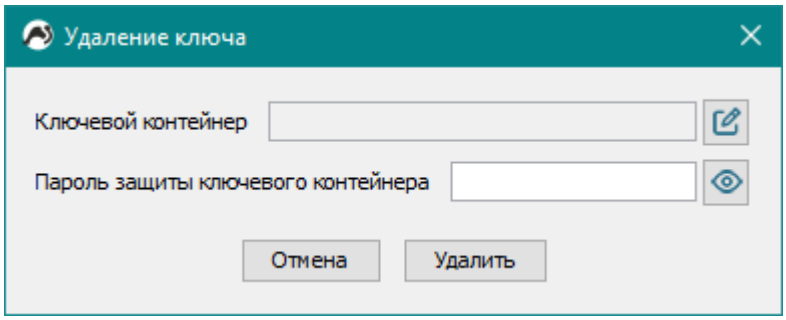

Рис. 49

После заполнения полей (рис. 50) необходимо нажать кнопку «Удалить».

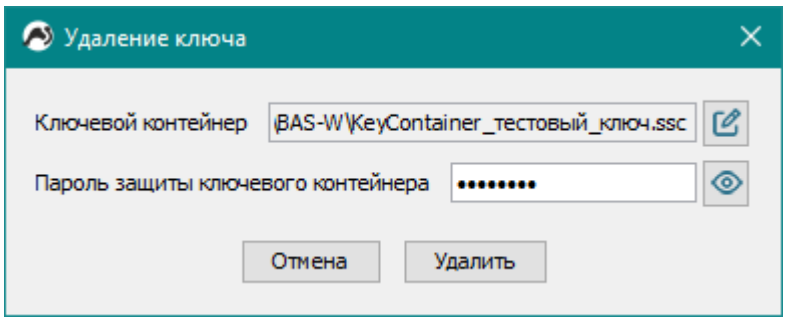

Рис. 50

3.2.4.3. Если поля не были заполнены или заполнены некорректно, то отобразятся соответствующие сообщения (рис. 51, 52).

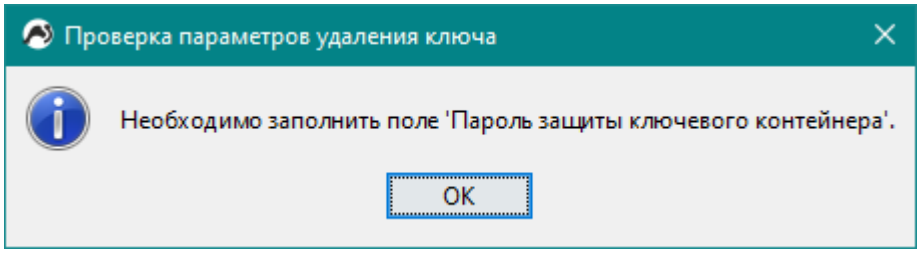

Рис. 51

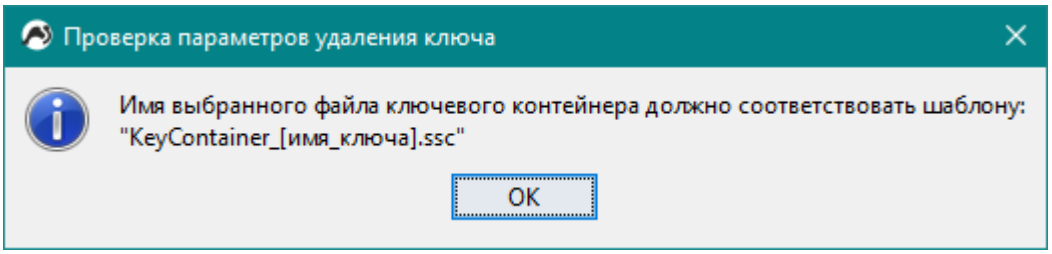

Рис. 52

3.2.4.4. Если заполненные поля прошли необходимые проверки, то отобразится окно с подтверждением удаления ключа (рис. 53).

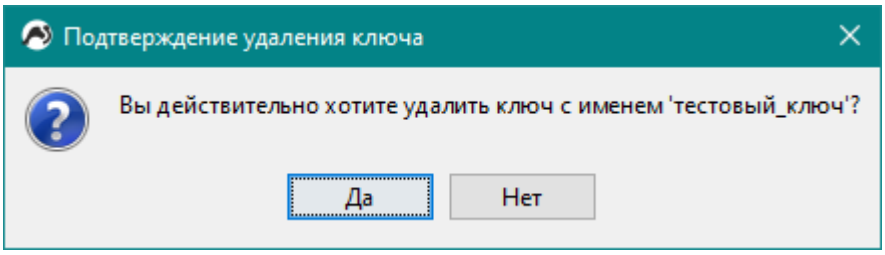

Рис.53

3.2.4.5. Если указанный ключ является секретом аутентификации текущего подключенного VPN-профиля, то отобразится окно с подтверждением, представленное на рис. 54.

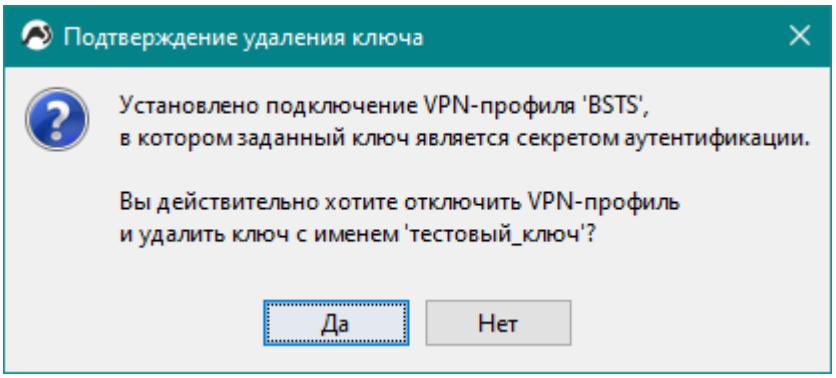

Рис. 54

3.2.4.6. После подтверждения удаления ключа в случае успеха будут удалены файлы защищенного контейнера с личным ключом и защищенного контейнера с первым частичным секретом из системной папки КП «БАС W», а также указанный файл защищенного контейнера со вторым частичным секретом, после чего отобразится окно, представленное на рис. 55.

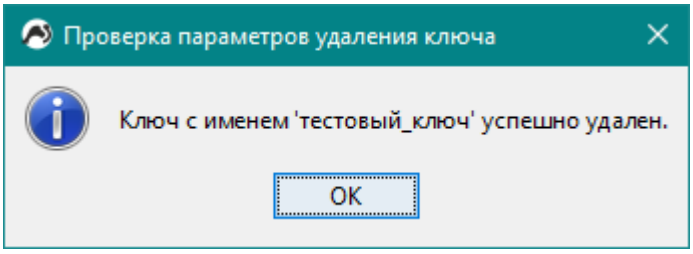

Рис. 55

3.2.4.6. Если удалить ключ не удалось, отобразится окно с сообщением о причине. Например, если ключ не найден, то отобразится окно, представленное на рис. 56.

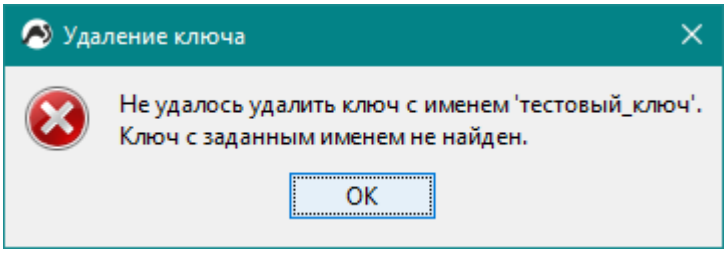

Рис. 56

3.2.4.7. Чтобы закрыть окно «Удаление ключа» без выполнения удаления ключа необходимо нажать либо кнопку закрытия окна в верхнем правом углу, либо кнопку «Отмена» в нижней части окна.

3.2.5. Просмотр журналов

3.2.5.1. Просмотреть журналы сообщений КП «БАС-W» можно вызвав контекстное меню и выбрав пункт «Просмотр журналов». Для просмотра доступны три файла в трех разных вкладках:

– журнал сообщений демона IKE во вкладке «Журнал сервиса charon-svc» (рис. 57);

– локальный журнал КП «БАС-W» во вкладке «Журнал приложения БАС-W» (рис. 58);

– результаты проведения контроля целостности во время последнего самотестирования во вкладке «Контроль целостности» (рис. 59).

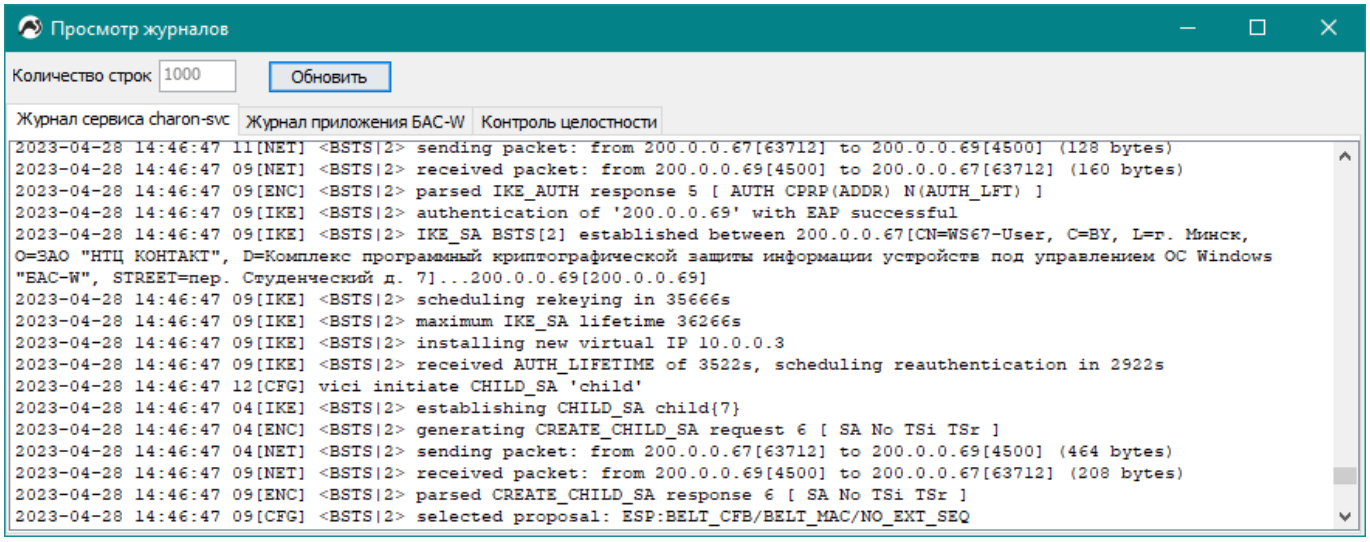

Рис. 57

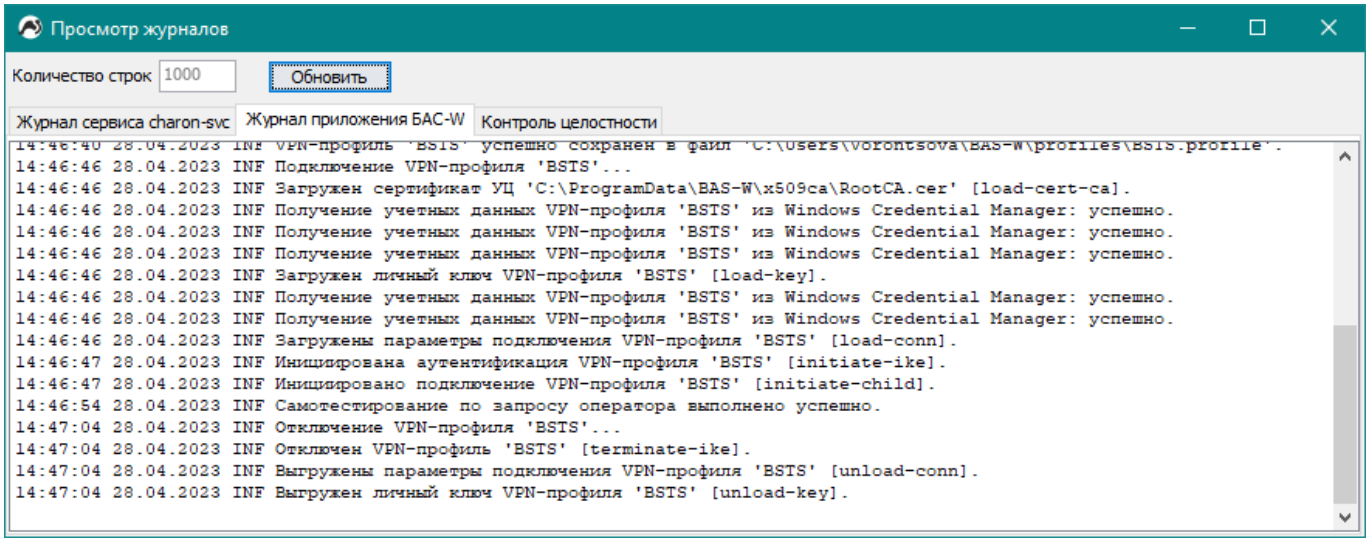

Рис. 58

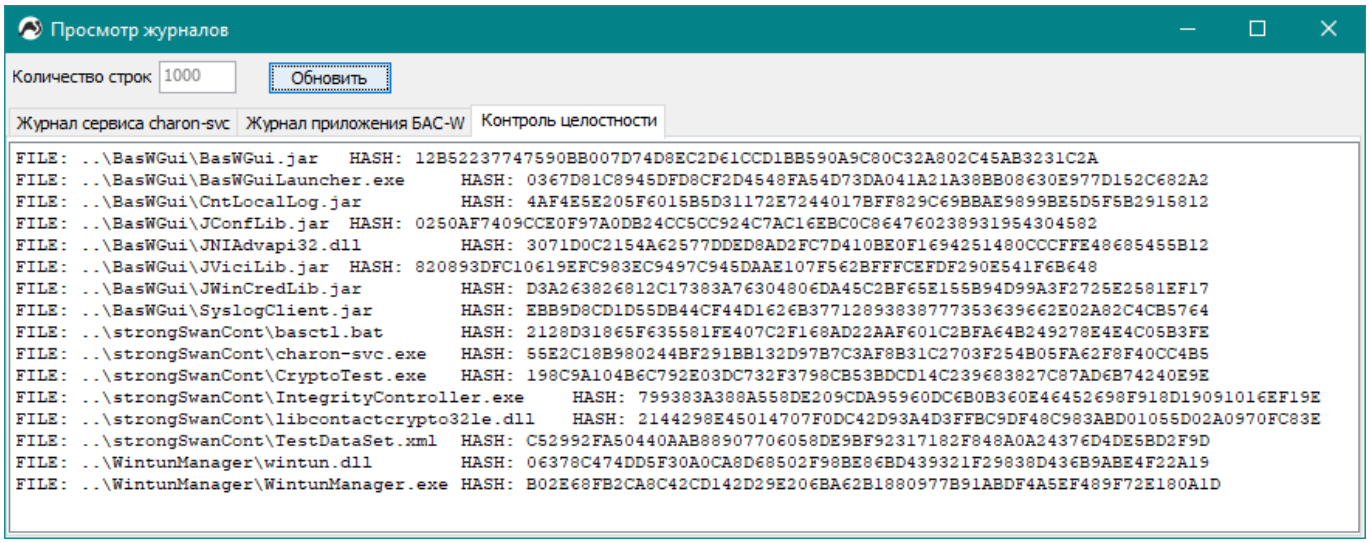

Рис. 59

3.2.5.2. В журнал сообщений демона IKE помещаются сообщения, формируемые при работе VPN-подключения. По сообщениям в этом журнале можно узнать причину ошибки при установке VPN-соединения.

3.2.5.3. В локальный журнал КП «БАС-W» помещаются сообщения о действиях, выполняемых по запросу Пользователя.

3.2.5.4. В журнал «Контроль целостности» помещаются результаты проведения контроля целостности во время последнего самотестирования. Пользователь может сравнить эти значения со значениями, приведенными в Сертификате соответствия, для идентификации соответствия используемой версии КП «БАС-W» сертифицированному образцу.

3.2.6. Выполнение самотестирования

Самотестирование включает в себя тестирование криптографических алгоритмов и контроль целостности файлов КП «БАС-W». Самотестирование выполняется во время установки КП «БАС-W», при включении (при загрузке сервиса charon-svc), по запросу оператора, а также по таймеру в автоматическом режиме.

Дополнительно во время установки КП «БАС-W» и при включении (при загрузке сервиса charon-svc) выполняется статистическое тестирование источников случайности.

3.2.6.1. Самотестирование по запросу оператора

Для того, чтобы запросить выполнение самотестирования, необходимо вызвать контекстное меню КП «БАС-W» и выбрать пункт «Самотестирование».

Если самотестирование выполнилось успешно, отобразится окно с соответствующим сообщением (рис. 60).

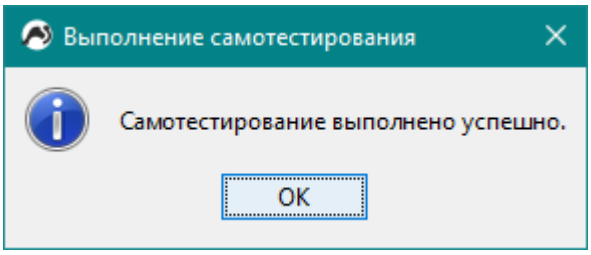

Рис. 60

Если во время выполнения самотестирования по запросу оператора произошла ошибка, то отобразится окно, представленное на рис. 61, и КП «БАС-W» перейдет в состояние блокировки (подробнее см. п. 3.2.6.3).

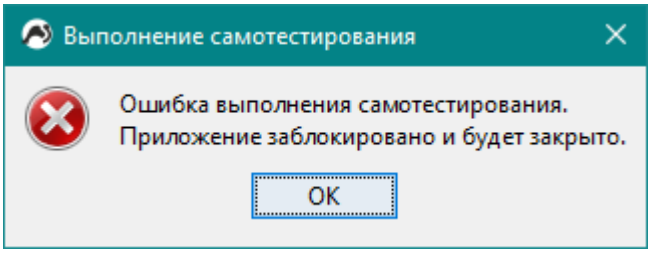

Рис. 61

3.2.6.2. Автоматическое самотестирование

В КП «БАС-W» есть возможность запустить автоматическое самотестирование, которое будет выполняться по таймеру. Настройки автоматического самотестирования описаны в п. 3.2.7.2. Результат автоматического самотестирования записывается в локальный журнал КП «БАС-W» при каждом выполнении.

Если во время выполнения автоматического самотестирования по таймеру произошла ошибка, то отобразится окно, представленное на рис. 61, и КП «БАС-W» перейдет в состояние блокировки (подробнее см. п. 3.2.6.3).

3.2.6.3. Состояние блокировки

Состояние блокировки наступает, когда самотестирование КП «БАС-W» завершается ошибкой. В состоянии блокировки завершается установленное VPN-подключение, если такое имеется, устанавливается флаг блокировки и работа КП «БАС-W» завершается.

Если попытаться запустить заблокированный КП «БАС-W», то отобразится окно, представленное на рис. 62, и КП «БАС-W» не запустится.

Если КП «БАС-W» перешел в состояние блокировки, Пользователь должен сообщить об этом Администратору.

Для выхода из состояния блокировки Администратору необходимо восстановить КП «БАС-W» в соответствии с п. 3.4.

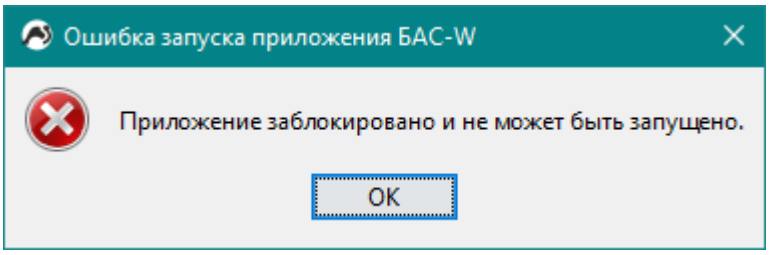

Рис. 62

3.2.7. Локальные настройки

К локальным настройкам КП «БАС-W» относятся настройки клиента Syslog и настройки выполнения автоматического самотестирования. Чтобы изменить локальные настройки необходимо вызвать контекстное меню и выбрать пункт «Настройки». Откроется окно «Настройки программы».

3.2.7.1. Настройки клиента Syslog

Настройки клиента Syslog представлены в одноименной вкладке в окне «Настройки программы» (рис. 63).

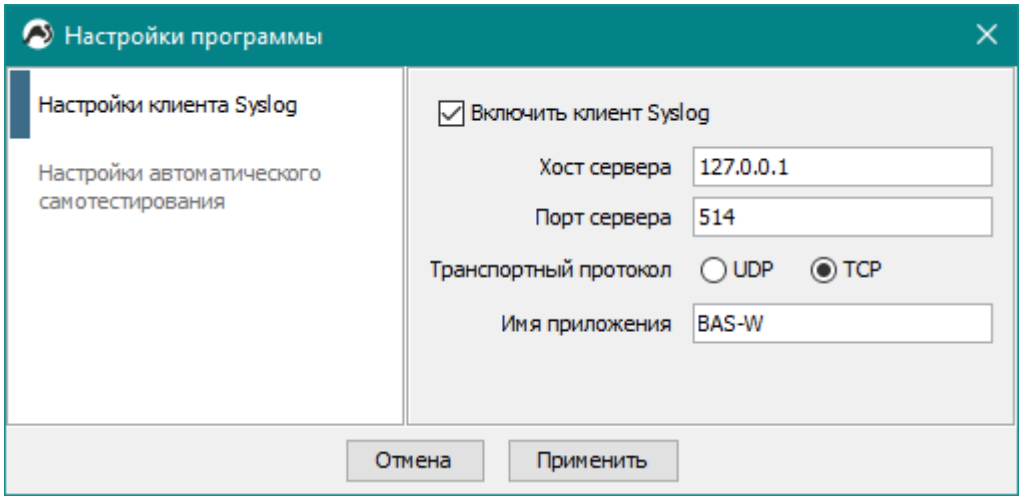

Рис. 63

С помощью клиента Syslog КП «БАС-W» может отправлять сообщения демона IKE на сервер. Чтобы включить клиент Syslog необходимо установить соответствующую галочку и указать необходимые параметры:

– «Хост сервера» – хост, на котором сервер Syslog ожидает приема сообщений. Должен быть представлен IP-адресом или DNS-именем;

– «Порт сервера» – порт, на котором сервер Syslog ожидает приема сообщений. По умолчанию используется порт 514;

– «Транспортный протокол» – протокол транспортного уровня, который используется для передачи сообщений на сервер;

– «Имя приложения» – имя приложения, которое может использоваться для фильтрации сообщений на сервере.

3.2.7.2. Настройки автоматического самотестирования

Настройки автоматического самотестирования представлены в одноименной вкладке в окне «Настройки программы» (рис. 64).

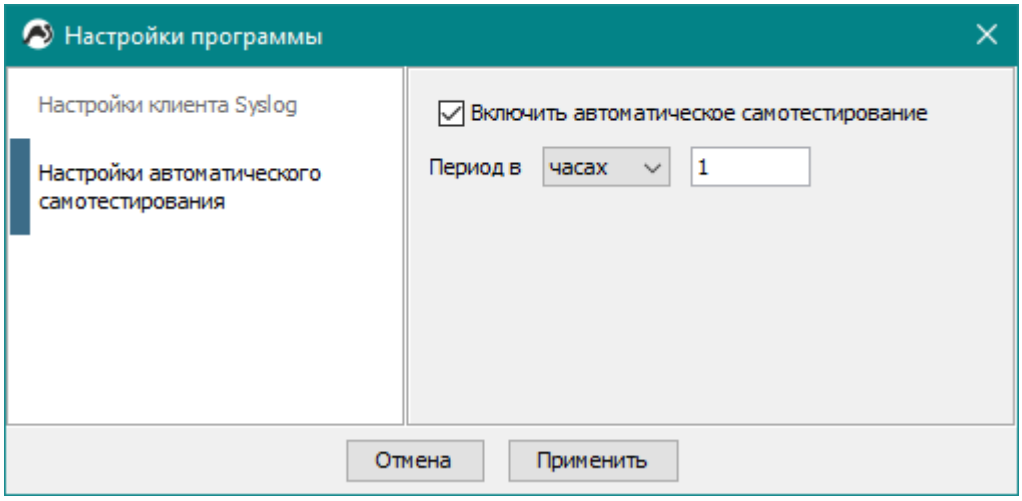

Рис. 64

Чтобы включить автоматическое самотестирование необходимо установить соответствующую галочку и указать период его выполнения. Допустимый диапазон значений от 5 до 1440 при использовании периода в минутах или от 1 до 24 при использовании периода в часах.

3.2.8. Просмотр версии

Для просмотра версии КП «БАС-W» необходимо вызвать контекстное меню и выбрать пункт «О программе». В открывшемся окне (рис. 65) представлено полное название КП «БАС-W», его версия, год разработки и наименование производителя.

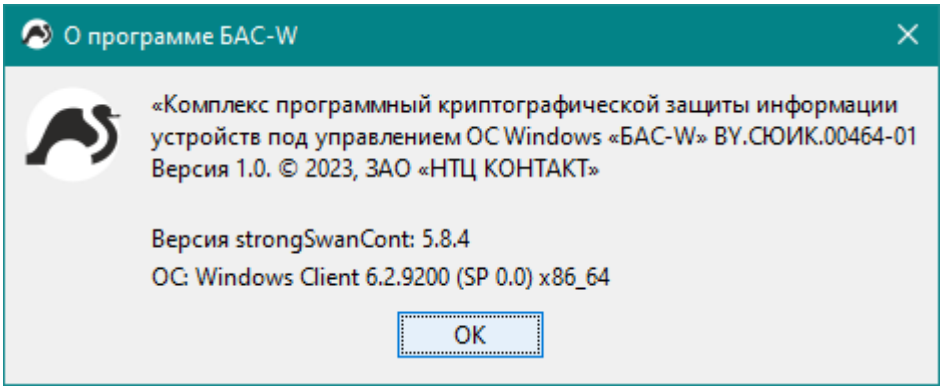

Рис. 65

3.2.9. Завершение работы

Для завершения работы КП «БАС-W» необходимо вызвать контекстное меню и выбрать пункт «Выход».

Если во время завершения работы КП «БАС-W» установлено подключение VPN-профиля, то отобразится окно с подтверждением выхода (рис. 66).

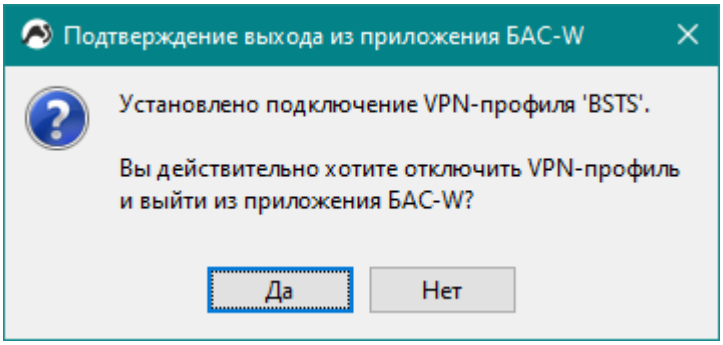

Рис. 66

Для отключения VPN-профиля и завершения работы КП «БАС-W» необходимо нажать кнопку «Да». Для отмены завершения работы КП «БАС-W» необходимо нажать кнопку «Нет».

3.3. Выполнение от имени Администратора

При запуске КП «БАС-W» от имени Администратора добавляется возможность обновления КП «БАС-W».

Чтобы обновить программу необходимо запустить КП «БАС-W» от имени Администратора и в контекстном меню выбрать пункт «Обновление» (рис. 67).

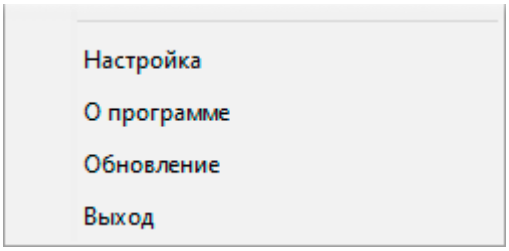

Рис. 67

Если во время обновления КП «БАС-W» установлено подключение VPN-профиля, то отобразится окно с подтверждением выхода (рис. 68).

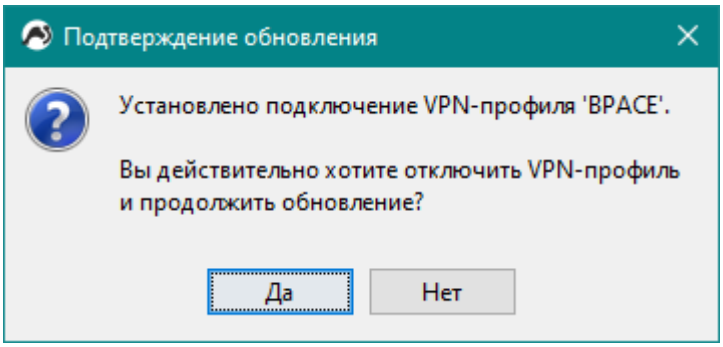

Рис. 68

Для отключения VPN-профиля и продолжения обновления КП «БАС-W» необходимо нажать кнопку «Да». Для отмены обновления необходимо нажать кнопку «Нет».

Если пользователь соглашается продолжить или если подключение не установлено, откроется стандартное окно выбора файла, в котором необходимо указать файл с программой обновления, заранее полученный от производителя КП «БАС-W» и нажать кнопку «Выбрать» (рис. 69). Файл, содержащий ЭЦП, должен находиться в той же папке, что и файл с программой обновления.

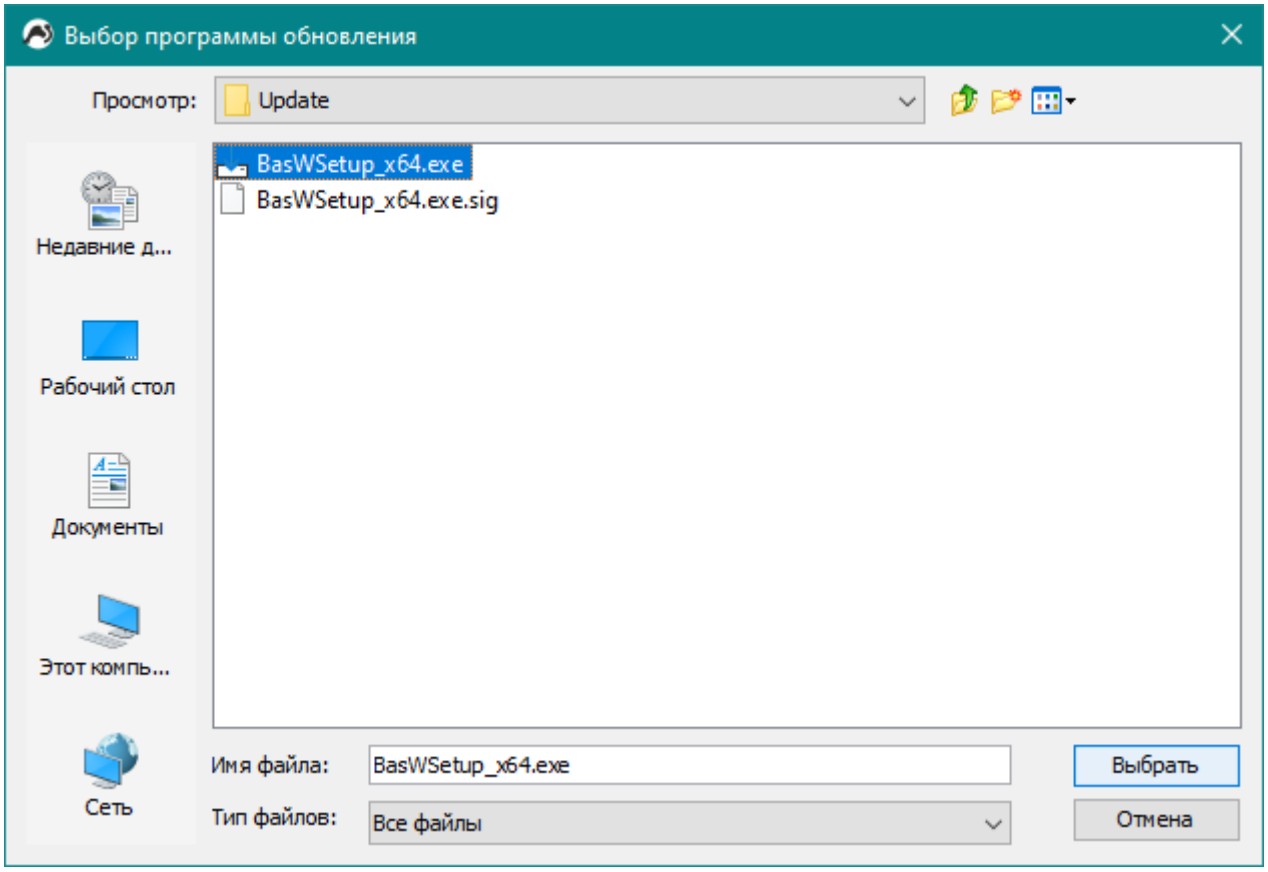

Рис. 69

После этого КП «БАС-W» выполнит проверку ЭЦП для подтверждения целостности и подлинности пакета обновляемых программ. Если ЭЦП отсутствует или недействительна,

отобразится окно с соответствующим сообщением (рис. 70, 71), и обновление программы не будет выполнено.

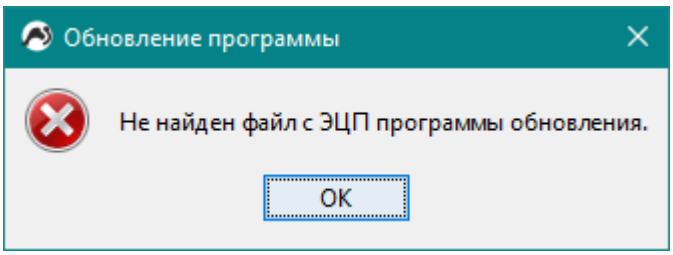

Рис. 70

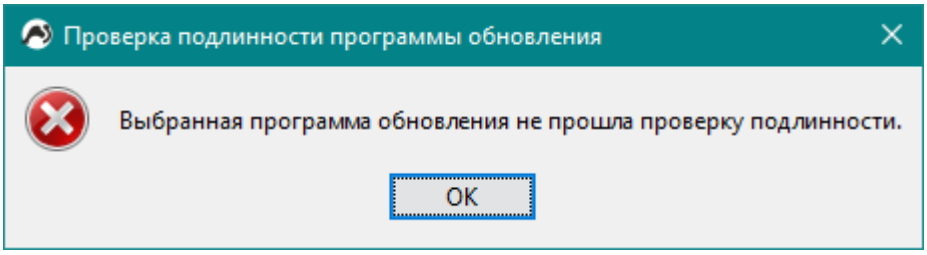

Рис. 71

Если целостность и подлинность пакета обновляемых программ будет подтверждена ЭЦП, , КП «БАС-W» будет закрыт, и будет запущена программы обновления.

3.4. Удаление

Для удаления КП «БАС-W» Администратору необходимо вызвать программу удаления. В ОС Windows это можно сделать разными способами. Например, для ОС Windows 10:

– удаление из меню «Пуск»: выбрать «Пуск», найти в списке «BAS-W», нажать правой кнопкой мыши и выбрать пункт «Удалить» (рис. 72).

– удаление на панели управления: ввести «панель управления» в поле поиска на панели задач, в списке результатов выбрать «Панель управления», в открывшемся окне выбрать «Программы» > «Программы и компоненты», в списке программ выбрать «BAS-W» и нажать кнопку «Удалить» (рис. 73).

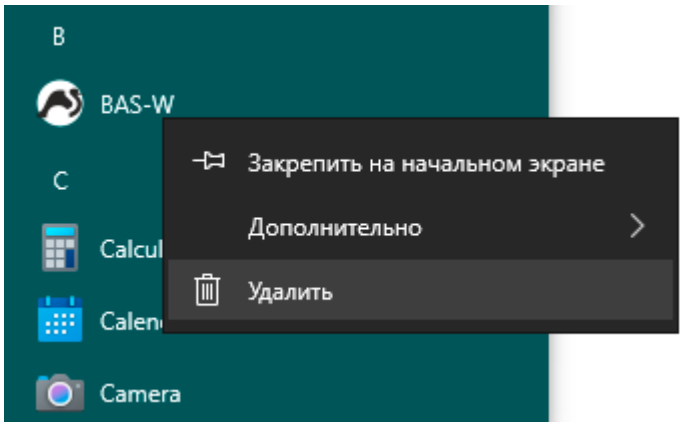

Рис. 72

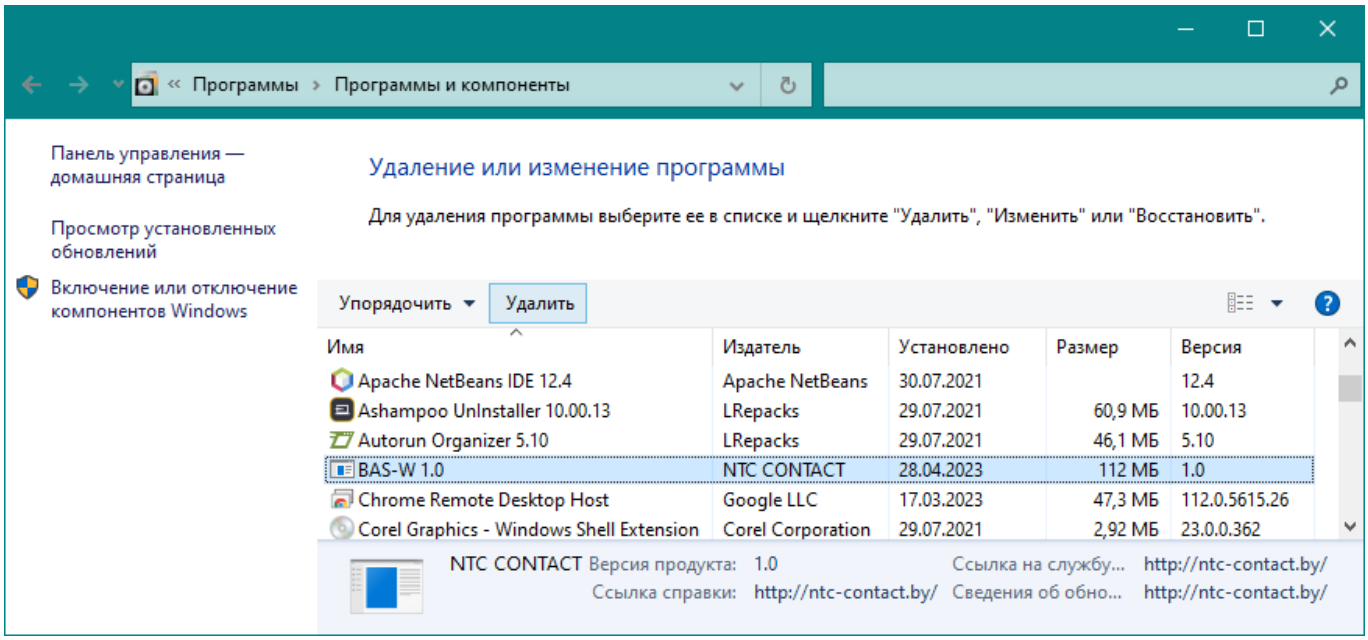

Рис. 73

Вне зависимости от выбранного способа запустится программы удаления КП «БАС-W» и откроется окно с подтверждением удаления (рис. 74).

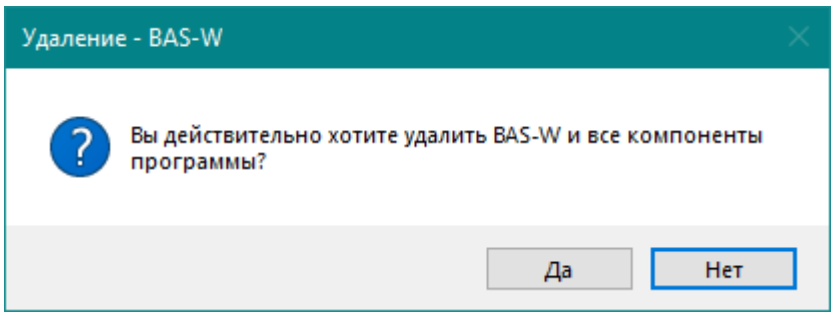

Рис. 74

Чтобы продолжить необходимо нажать кнопку «Да». Для отмены удаления необходимо нажать кнопку «Нет».

После подтверждения удаления откроется окно, в котором отображается состояние удаления (рис. 75).

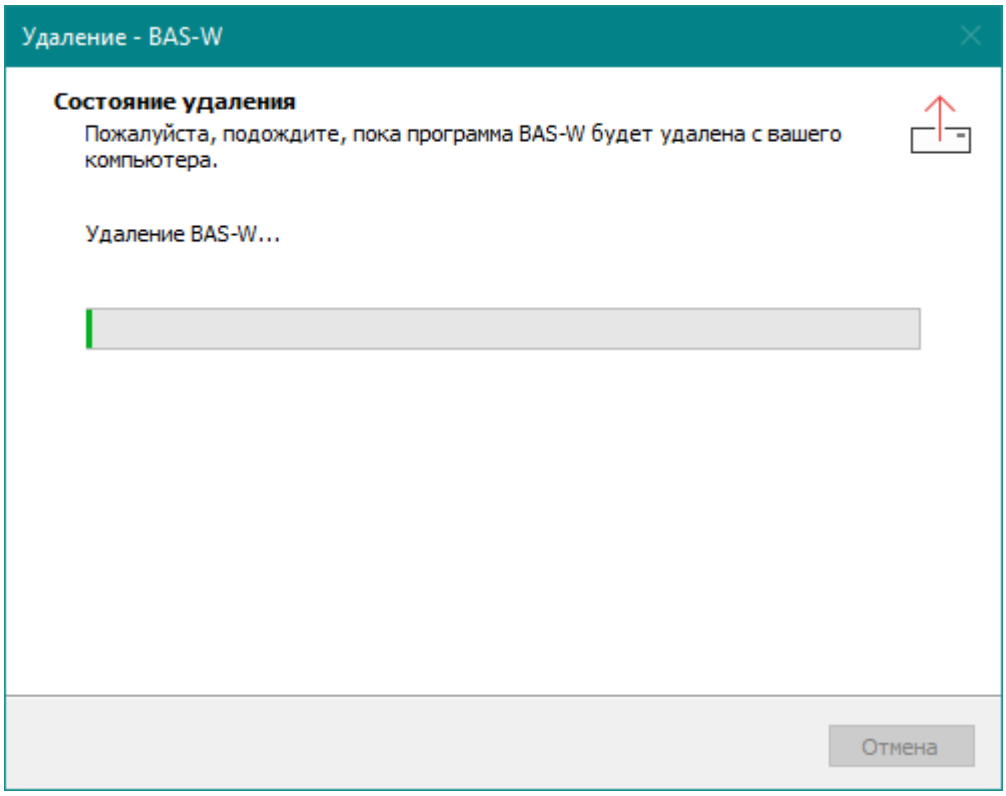

Рис. 75

Необходимо дождаться пока программы удаления полностью удалит КП «БАС-W» и отобразится окно с соответствующим сообщением (рис. 76).

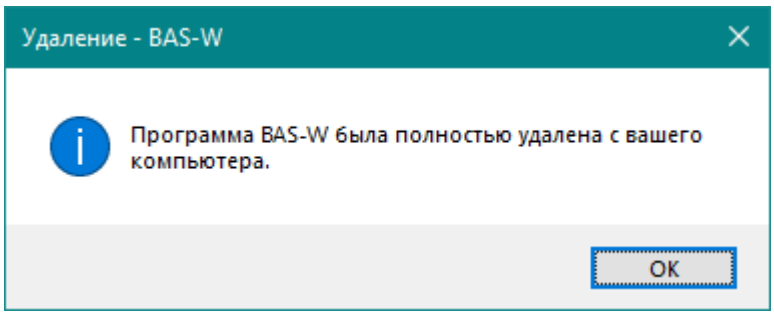

Рис. 76

3.5. Восстановление и переустановка

Восстановление КП «БАС-W» может понадобиться, если КП «БАС-W» провалил самотестирование и перешел в состояние блокировки.

Переустановка КП «БАС-W» может понадобиться при выходе новых версий КП «БАС-W».

Восстановление или переустановка КП «БАС-W» производится Администратором путем запуска программы установки «BasWSetup_x32.exe» или «BasWSetup_x64.exe». Процесс схож с установкой с несколькими отличиями:

– после выбора языка установки Администратору необходимо подтвердить переустановку КП «БАС-W» (рис. 77). Если предлагаемая версия КП «БАС-W» совпадает с установленной, то

выполняется восстановление. Если предлагаемая версия КП «БАС-W» выше установленной, то выполняется переустановка. Если предлагаемая версия КП «БАС-W» ниже установленной, то процесс завершается, а в системе остается версия без изменений;

– Администратору не предлагается выбрать место на диске для КП «БАС-W» и нет необходимости выполнять какие-либо настройки среды, т.к. используются текущее место установки и настройки.

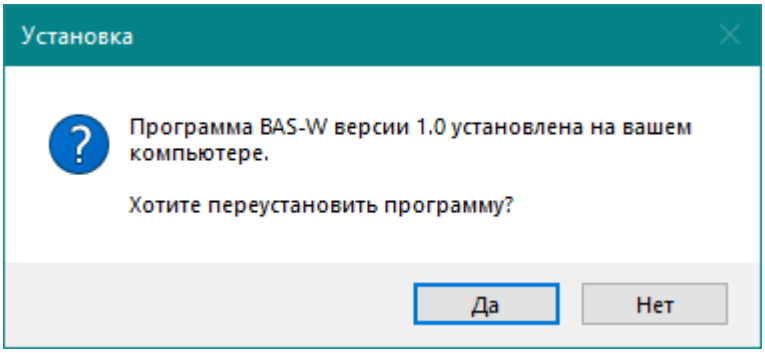

Рис. 77

Если во время восстановления или переустановки произошла ошибка, то КП «БАС-W» откатывается до того состояния, в котором был до восстановления или переустановки.

Если после восстановления КП «БАС-W» завершает самотестирование с ошибкой, то он полностью удаляется.

4. СООБЩЕНИЯ ОПЕРАТОРУ

КП «БАС-W» не предоставляет специфических сообщений оператору, не описанных в данном документе.

Сообщения о результатах работы КП «БАС-W» выводятся в журналы. Сообщения четко описывают причину их появления и не нуждаются в разъяснении.

При возникновении ситуаций, влияющих на безопасность КП «БАС-W», оператору предоставляются сообщения об этом. Данные ситуации могут привести к блокировке КП «БАС-W». Пользователь должен сообщить Администратору о наступлении таких ситуаций.

ПРИЛОЖЕНИЕ А

ОПИСАНИЕ ОБОЗНАЧЕНИЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Алгоритмы шифрования:

– belt_cbc – алгоритм шифрования СТБ 34.101.31 в режиме сцепления блоков;

– belt_cfb – алгоритм шифрования СТБ 34.101.31 в режиме гаммирования с обратной связью;

– belt_ctr – алгоритм шифрования СТБ 34.101.31 в режиме счётчика.

Алгоритмы контроля целостности:

– belt_mac – алгоритм выработки иммитовставки СТБ 34.101.31;

– belt_hmac – алгоритм ключезависимого хэширования СТБ 34.101.47.

Алгоритмы выработки псевдослучайных чисел:

– prfbrng_ctr – алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме счётчика;

– prfbrng_hmac – алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме HMAC;

Алгоритм Диффи-Хеллмана:

– ecp256bign – алгоритм Диффи-Хеллмана в соответствии с СТБ 34.101.66, Приложение А.

Алгоритм преобразования ключа:

– keyrep – алгоритм преобразования ключа СТБ 34.101.31.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					