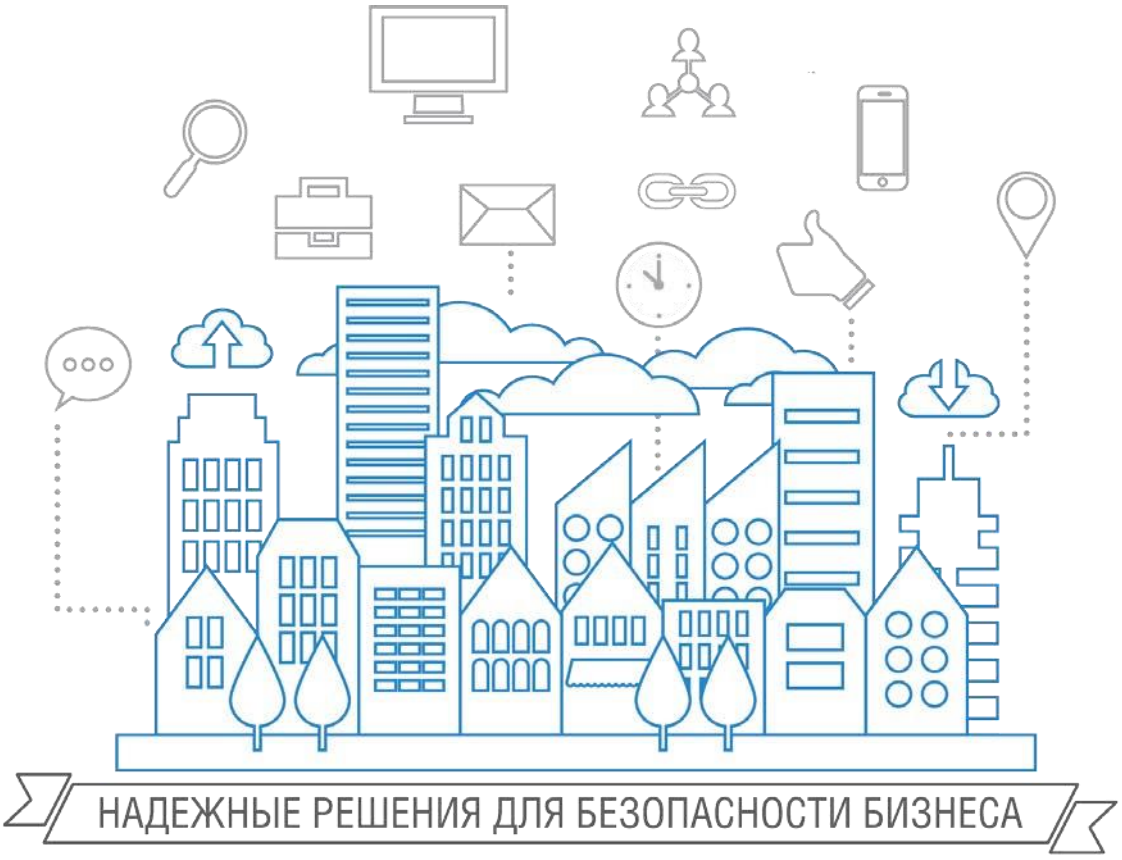
ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51 Почтовый адрес: 198096, г. Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт -Пет ербу рге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»

Руководство пользователя



Санкт-Петербург, 2018

Содержание

1. Общие сведения

1.1. Назначение СЗИ «Блокхост-сеть 2.0»

СЗИ «Блокхост-сеть 2.0» является программно-аппаратной системой, предназначенной для комплексной и многофункциональной защиты информационно-программных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС) на базе персональных компьютеров (ПК) под управлением ОС Windows 2008R2/7/8.1/2012/2012R2/10/2016.

1.2. Необходимая информация

Для работы с компьютером, защищенным СЗИ «Блокхост-сеть 2.0», пользователь должен знать и иметь:

№ п/п	Наименование	Описание
1	Имя	Идентификатор пользователя для СЗИ «Блокхост-сеть 2.0» и ОС Windows
2	Пароль	Для проверки подлинности пользователя в СЗИ «Блокхост-сеть 2.0» и ОС Windows
3	Домен	Тип аутентификации в ОС Windows (локальная или на контроллере домена)
4	Уровень доступа	Режим обработки информации для СЗИ «Блокхост-сеть 2.0»
5	Персональный идентификатор (eToken/SafeNet eToken/JaCarta/AvBign/ESMART Token/ ruToken/USB-накопитель/дискета/ персональный идентификатор пользователя, расположенный в защищённом хранилище реестра Windows)	Для хранения ключевой информации СЗИ «Блокхост-сеть 2.0» и аутентификации пользователя (при использовании двухфакторной аутентификации)
6	PIN-код	Пароль персонального идентификатора для доступа к ключевой информации СЗИ «Блокхост-сеть 2.0» (при использовании двухфакторной аутентификации)

Перечисленные выше идентификационные данные и персональные идентификаторы должны использоваться и храниться с применением мер безопасности организационного характера, исключающих возможность их несанкционированного использования.

2. Вход в систему

На компьютере, защищенном СЗИ «Блокхост-сеть 2.0», выполняется процедура двухфакторной аутентификации. Суть её заключается в том, что система защиты требует от пользователя «предъявить» ей не только информацию, которую он должен помнить (имя, пароль, PIN-код), но и «вещественные доказательства» истинности пользователя. В качестве таких «доказательств» в СЗИ «Блокхост-сеть 2.0» используются персональные идентификаторы: eToken\SafeNet eToken\ruToken\JaCarta\AvBign\ESMART Token\USB-накопитель или дискета\персональный идентификатор пользователя, расположенный в защищённом хранилище реестра Windows (далее – персональный идентификатор в реестре), на которых записана ключевая информация для доступа в систему. При использовании двухфакторной аутентификации СЗИ «Блокхост-сеть 2.0» вход пользователя в систему и дальнейшая загрузка ОС без предъявления электронного идентификатор невозможны.

Информация для аутентификации на персональных идентификаторах защищена специальным паролем – PIN-кодом. Стандартный PIN-код идентификаторов для ruToken – «12345678», для eToken и SafeNet eToken – «1234567890», для JaCarta – «1234567890», для ESMART Token – «12345678», для AvBign – «12345678». В дальнейшем стандартный PIN-код может быть изменен. Для USB-накопителя, дискеты PIN-код и персонального идентификатора в реестре задается средствами СЗИ «Блокхост-сеть 2.0».

При задании PIN-кода для персональных электронных идентификаторов eToken, SafeNet eToken, ruToken JaCarta, AvBign и ESMART Token не следует использовать русские буквы.

При использовании двухфакторной аутентификации СЗИ «Блокхост-сеть 2.0» в случае незнания PIN-кода или утери персонального идентификатора, вход в систему будет невозможен. Для его восстановления следует обратиться к администратору безопасности.

Реакция СЗИ «Блокхост-сеть 2.0» на случаи неправильного ввода идентификационной информации (неправильный логин или пароль пользователя, предъявление стороннего персонального идентификатора и/или ввод неверного PIN-кода доступа к нему) настраивается администратором безопасности в консоли администрирования СЗИ и предполагает блокировку пользователя, от имени которого осуществлялась авторизация, на определенное время.

Указанные при входе пользователя в ОС значения мандатной метки и категорий определяют права доступа пользователя (уровень доступа) по обработке конфиденциальной информации и возможности взаимодействия с другими рабочими станциями ЛВС. При этом значение мандатной метки равное **1**, без указания значений неиерархических категорий, соответствует режиму обработки открытой информации, и взаимодействие с другими рабочими станциями ЛВС разрешено (при условии, что взаимодействие не запрещено дискреционной политикой персонального экрана). Если же значение мандатной метки больше **1**, и/или указано значение неиерархической категории – то это режим обработки конфиденциальной информации. При этом возможны следующие варианты:

- уровни доступа пользователя (метка и категория субъекта) и уровень конфиденциальности сетевого ресурса (метка и категория объекта) равны – субъект получает полный доступ к объекту;

- уровень доступа пользователя (субъекта) больше уровня конфиденциальности сетевого ресурса – субъект получает доступ к объекту по чтению. Пользователь может сохранить объект на своей рабочей станции только с уровнем конфиденциальности, равным своему уровню доступа;
- уровень доступа пользователя (субъекта) меньше уровня конфиденциальности сетевого ресурса – субъект не имеет доступа к объекту.

Стоит отметить, что независимо от значения уровня доступа пользователя, **первый вход в ОС** он должен выполнить, **указав значение мандатной метки, равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

При вводе пароля каждый его символ отображается на экране в виде «*». При этом необходимо учитывать, что строчные и прописные буквы, кириллица и латиница различаются. Если при вводе имени, пароля или PIN-кода была неправильно нажата какая-либо клавиша, можно скорректировать ошибочно набранные символы в строке и заново повторить ввод.

Особенности входа в ОС в безопасном режиме

Необходимо обратить внимание на то, что войти в ОС в безопасном режиме на рабочую станцию с установленным СЗИ «Блокхост-сеть 2.0» можно только под встроенной учетной записью администратора ОС Windows (домена).

2.1. Аутентификация в ОС Windows 7/Server 2008R2

При аутентификации в ОС Windows 7/Server 2008R2 при загрузке системы предусмотрены следующие виды входа в систему (рис. 1):

- вход с предъявлением электронного идентификатора ruToken;
- вход с предъявлением электронного идентификатора eToken, SafeNet eToken (также используется для входа с электронным идентификатором JaCarta PRO, JaCarta ГОСТ, JaCarta PKI);
- вход с предъявлением электронного идентификатора Avest Token;
- вход с предъявлением электронного идентификатора ESMART Token;
- вход с предъявлением отчуждаемого носителя (USB-накопитель/дискета);
- вход по сертификату;
- вход использованием персонального идентификатора пользователя, хранящегося в реестре Windows (значок появляется при условии, что хотя бы одному пользователю в СЗИ присвоен носитель данного вида);
- вход администратора без предъявления электронного идентификатора.

Рисунок 1. Аутентификация в ОС Windows 2008R2/7

2.1.1 Аутентификация с предъявлением электронного идентификатора ruToken

Для аутентификации в системе с предъявлением электронного идентификатора ruToken необходимо подключить электронный идентификатор ruToken, затем нажать кнопку ***RuToken <Имя носителя>*** и заполнить следующие поля (рис. 2):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате *Domain_name\User_name*;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код доступа к электронному идентификатору ruToken;
- ***Мандатная метка*** – вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

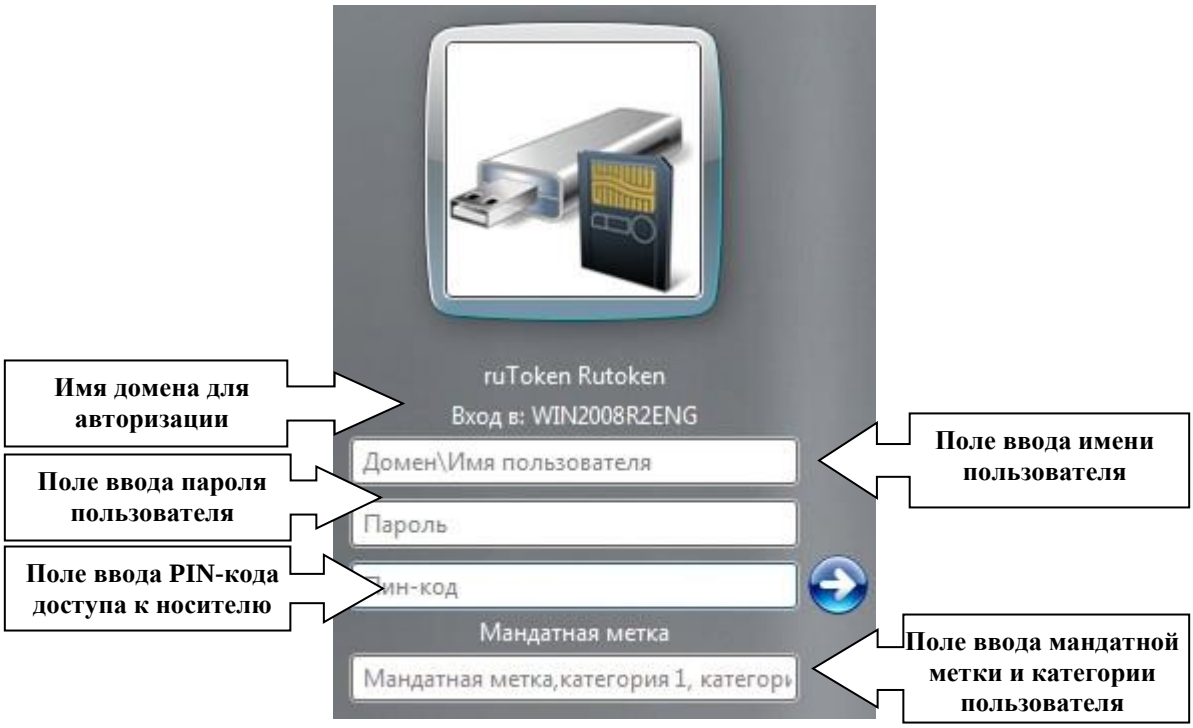


Рисунок 2. Аутентификация в ОС Windows 2008R2/7 с предъявлением ruToken

2.1.2 Аутентификация с предъявлением электронного идентификатора eToken/Safe Net eToken/JaCarta

Для аутентификации с предъявлением электронного идентификатора eToken/SafeNet eToken/JaCarta необходимо подключить электронный идентификатор eToken/SafeNet eToken/JaCarta затем нажать кнопку ***eToken <Имя устройства считывания>*** (рис. 1) и заполнить поля (рис.3):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате `Domain_name\User_name`;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 3. Аутентификация в ОС Windows 2008R2/7 с предъявлением eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI

2.1.3 Аутентификация с предъявлением электронного идентификатора Avest Token

Для аутентификации с предъявлением электронного идентификатора Avest Token необходимо подключить электронный идентификатор AvBign, затем нажать кнопку ***Avest <Имя носителя>*** (рис.1) и заполнить поля (рис. 4):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате `Domain_name\User_name`;

- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4. Аутентификация в ОС Windows 2008R2/7 с предъявлением Avest Token

2.1.4 Аутентификация с предъявлением электронного идентификатора ESmart Token

Для аутентификации с предъявлением электронного идентификатора ESmart Token необходимо подключить электронный идентификатор ESmart, затем нажать кнопку ***ESmart <Имя носителя>*** (рис. 1) и заполнить поля (рис. 5):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате *Domain_name\User_name*;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 5. Аутентификация в ОС Windows 2008R2/7 с предъявлением ESmart Token

2.1.5 Аутентификация с предъявлением отчуждаемого носителя

Для аутентификации с предъявлением отчуждаемого носителя (USB-накопителя/дискеты) необходимо подключить USB-накопитель/вставить дискету, затем нажать кнопку ***Removable <Буква диска: метка тома>*** (рис. 1) и заполнить поля (рис. 6):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате *Domain_name\User_name*;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя**;**
- ***PIN-код*** **–** вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** **–** вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 6. Аутентификация в ОС Windows 2008R2/7 с предъявлением отчуждаемого носителя

2.1.6 Аутентификация по сертификату пользователя

В СЗИ «Блокхост-сеть 2.0» реализована возможность двухфакторной аутентификации пользователей в домене Microsoft Active Directory *с использованием цифровых сертификатов пользователей*, выработанных, в том числе с использованием российских криптографических алгоритмов (ГОСТ).

Для аутентификации по сертификату необходимо подключить персональный электронный идентификатор (eToken/SafeNet eToken/JaCarta/ESMART Token/Avest Token/ruToken), содержащий сертификат пользователя и нажать кнопку ***Вход со смарт-картой <Имя пользователя>*** (рис. 1). В появившемся окне (рис. 7) нужно в соответствующие поля ввести PIN-код подключенного носителя и перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю (независимо от значения мандатной метки пользователя в СЗИ, **первый вход в ОС** он должен выполнить, указав значение метки, **равное 1**, **без ввода имен категорий**, это необходимо для корректного создания профиля пользователя операционной системой). Остальные данные пользователя будут автоматически считаны с носителя.

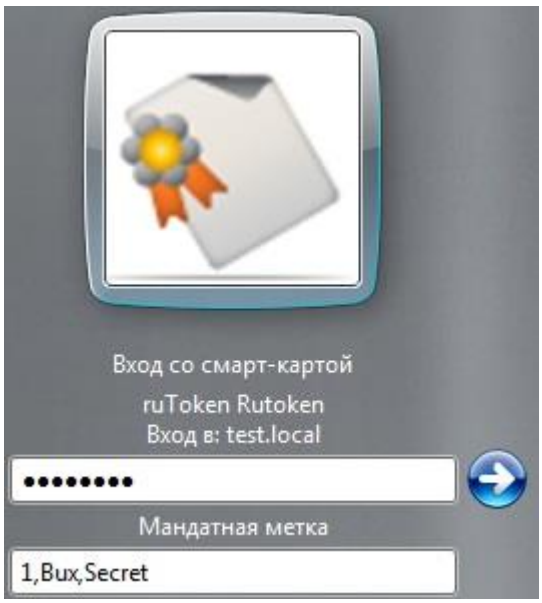


Рисунок 7. Вход ОС Windows 2008R2/7 по сертификату

Процедура настройки центра сертификации в ОС Windows 2008R2 и получение цифрового сертификата пользователя описаны в Приложении 3 к настоящему руководству.

2.1.7 Аутентификация с использованием персонального идентификатора пользователя, хранящегося в реестре Windows

Для аутентификации с использованием персонального идентификатора пользователя, хранящегося в реестре Windows, следует нажать кнопку ***Registry <Имя контейнера>*** (рис. 1) и заполнить поля (рис. 8):

- ***Имя пользователя*** – вводится имя учетной записи пользователя. При необходимости сменить домен входа имя пользователя вводится в формате `Domain_name\User_name`;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код персонального идентификатора (при этом необходимо выбрать из списка идентификатор в реестре Windows, сопоставленный данному пользователю);
- ***Мандатная метка*** – вводятся перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав только значение метки, **равное 1, без ввода имен категорий**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 8. Аутентификация в ОС Windows 2008R2/7 с предъявлением персонального идентификатора, хранящегося в реестре Windows

2.1.8 Вход без токена

В СЗИ «Блокхост-сеть 2.0» существует возможность входа пользователей в ОС по паролю без предъявления ключевого носителя. Если администратор безопасности предоставил пользователю возможность входа в ОС без предъявления ключевого носителя, то для входа пользователя в ОС необходимо нажать кнопку ***Вход пользователя*** (см. рис. 1) и заполнить поля, показанные на рисунке 9:

- ***Имя пользователя*** **–** вводится логин пользователя, который имеет право входа в ОС без предъявления ключевого носителя. При необходимости сменить домен входа имя пользователя вводится в формате `Domain_name\User_name`;
- ***Пароль*** – вводится пароль встроенного администратора.

Рисунок 9. Вход пользователя в ОС Windows 2008R2/7 без предъявления ключевого носителя

2.2. Аутентификация в ОС Windows 8.1/Server 2012/2012R2

При аутентификации в ОС Windows Server 8.1/2012/2012R2 при загрузке системы предусмотрены следующие виды входа в систему (рис. 10 и 11):

- вход с предъявлением электронного идентификатора ruToken;
- вход с предъявлением электронного идентификатора eToken/SafeNet eToken (также используется для входа с электронным идентификатором JaCarta PRO, JaCarta ГОСТ, JaCarta PKI);
- вход с предъявлением электронного идентификатора Avest Token;
- вход с предъявлением электронного идентификатора ESmart Token;
- вход с предъявлением отчуждаемого носителя (USB-накопитель/дискета);
- вход по сертификату;
- вход использованием персонального идентификатора пользователя, хранящегося в реестре Windows (значок появляется при условии, что хотя бы одному пользователю в СЗИ присвоен носитель данного вида);
- вход администратора без предъявления электронного идентификатора.

Рисунок 10. Аутентификация в ОС Windows 8.1/2012/2012R2

Если какая-либо кнопка, соответствующая перечисленному выше виду аутентификации не видна, следует передвинуть ползунок, расположенный в нижней части экрана, вправо (рис. 4.12).

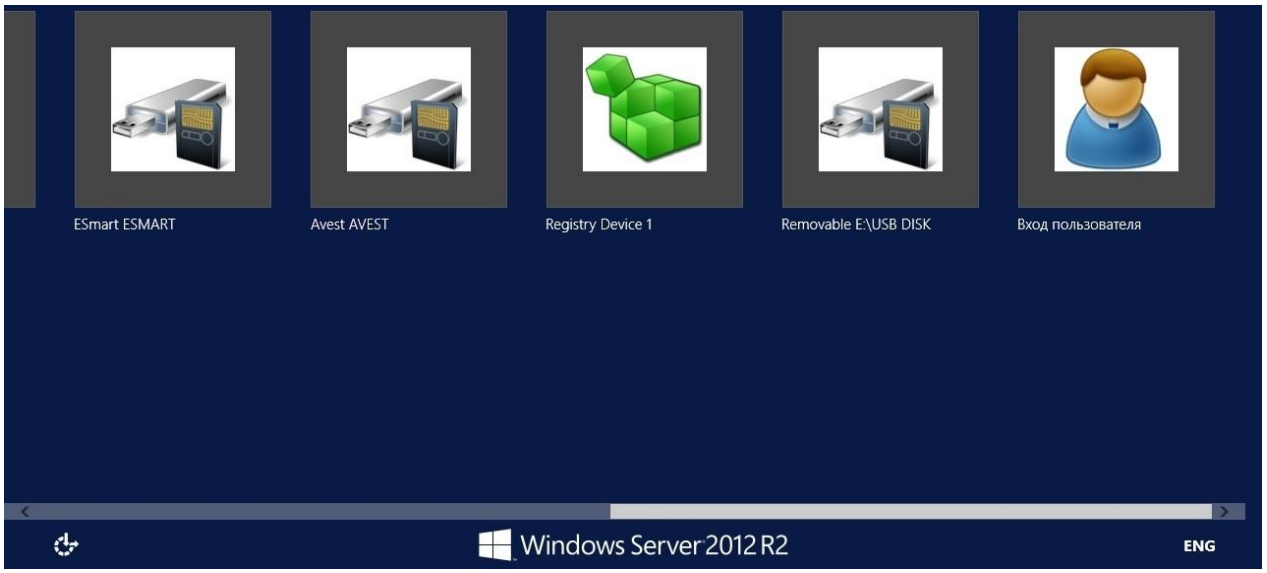


Рисунок 11. Аутентификация в ОС Windows 8.1/2012/2012R2

2.2.1 Аутентификация с предъявлением электронного идентификатора ruToken

Для аутентификации в системе с предъявлением электронного идентификатора ruToken необходимо подключить электронный идентификатор ruToken, затем нажать кнопку ***RuToken <Имя носителя>*** и заполнить все поля все поля в диалоговом окне аутентификации пользователя (рис. 12). Подробное описание назначения полей приведено в п. 2.1.1 настоящего руководства.

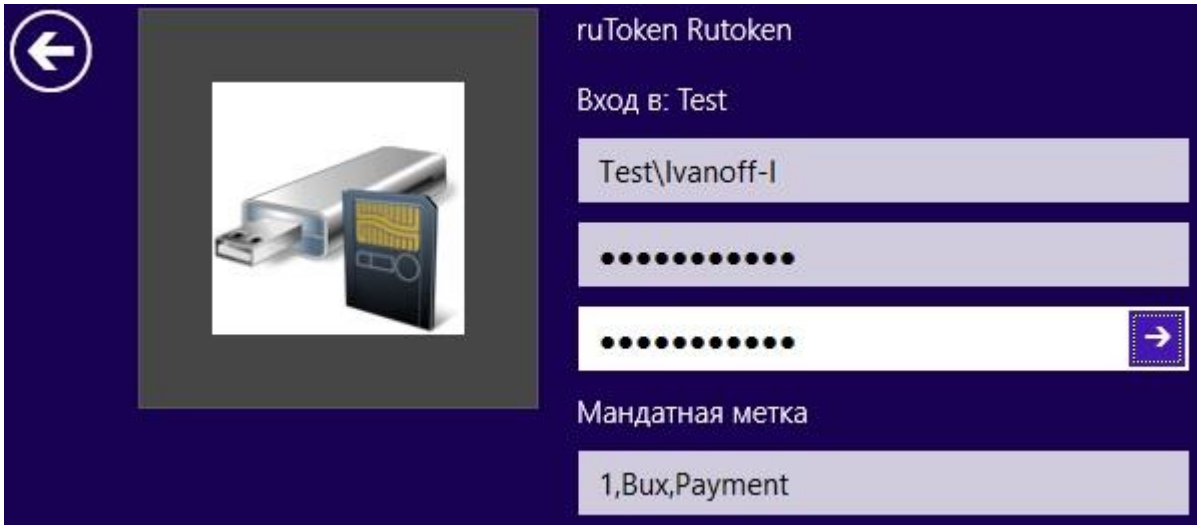


Рисунок 12. Аутентификация в ОС Windows 8.1/2012/2012R2 с предъявлением ruToken

2.2.2 Аутентификация с предъявлением электронного идентификатора eToken/SafeNet eToken/JaCarta

Для аутентификации с предъявлением электронного идентификатора eToken/SafeNet eToken/JaCarta необходимо подключить электронный идентификатор eToken/SafeNet eToken/JaCarta затем нажать кнопку ***eToken <Имя устройства считывания>*** (рис. 10) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 13). Подробное описание назначения полей приведено в п. 2.1.2 настоящего Руководства.

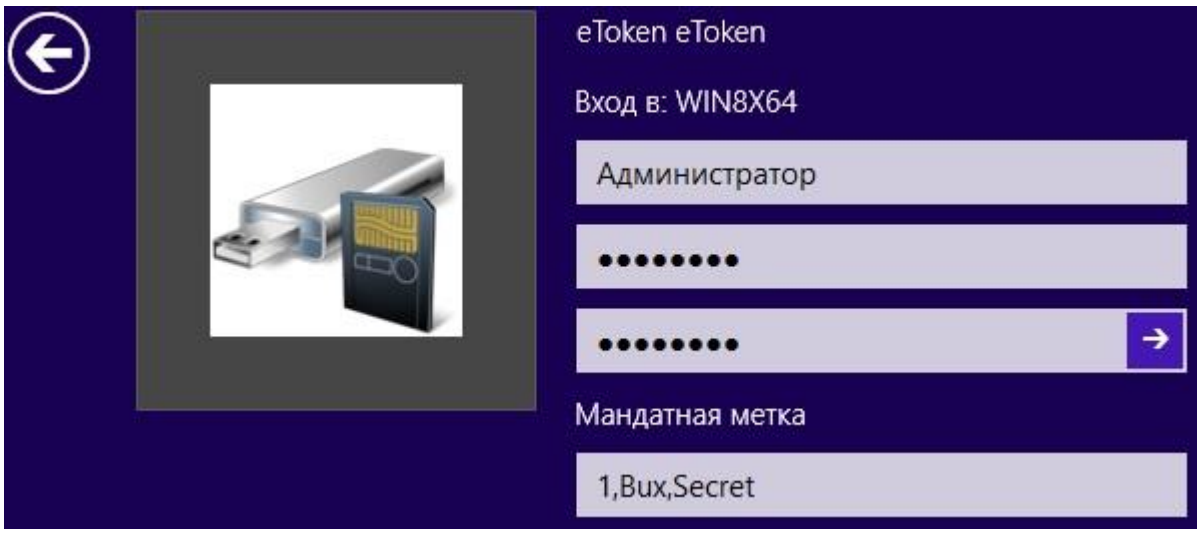


Рисунок 13. Аутентификация в ОС Windows 8.1/2012/2012R2
с предъявлением eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI

2.2.3 Аутентификация с предъявлением электронного идентификатора Avest Token

Для аутентификации с предъявлением электронного идентификатора Avest Token необходимо подключить электронный идентификатор AvBign, затем нажать кнопку ***Avest <Имя носителя>*** (рис. 10) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 14). Подробное описание назначения полей приведено в п. 2.1.3 настоящего Руководства.

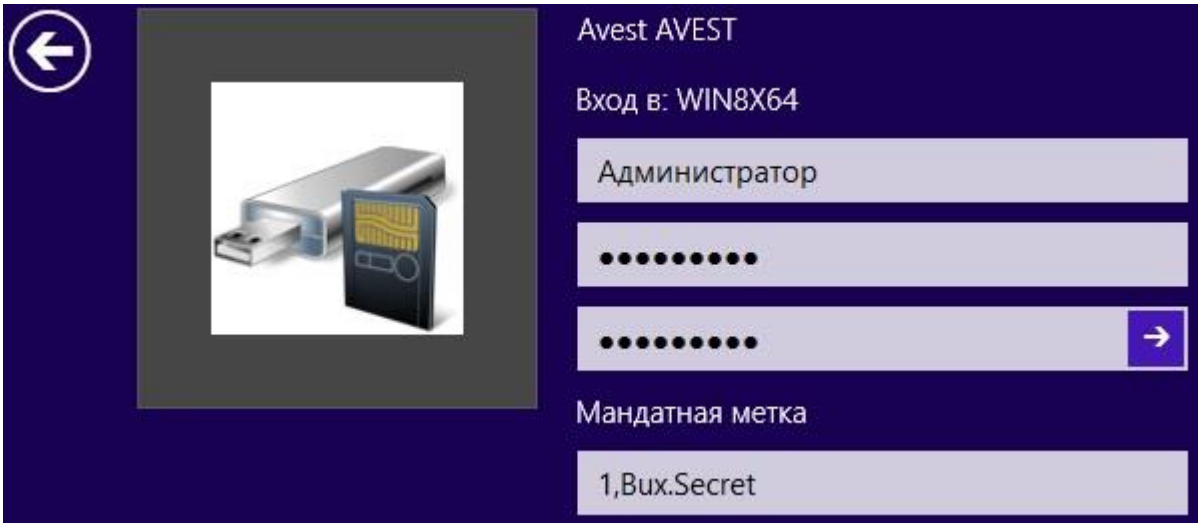


Рисунок 14. Аутентификация в ОС Windows 8.1/2012/2012R2 с предъявлением Avest Token

2.2.4 Аутентификация с предъявлением электронного идентификатора ESMART Token

Для аутентификации с предъявлением электронного идентификатора ESMART Token необходимо подключить электронный идентификатор ESmart, затем нажать кнопку ***ESMART <Имя носителя>*** (рис. 10) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 15). Подробное описание назначения полей приведено в п. 2.1.4 настоящего Руководства.

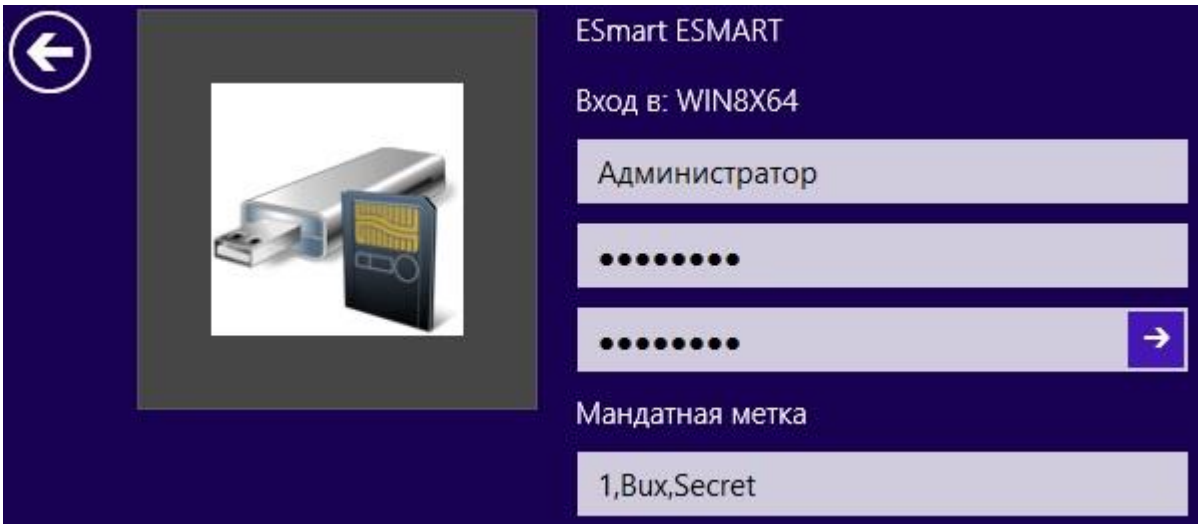


Рисунок 15. Аутентификация в ОС Windows 8.1/2012/2012R2 с предъявлением ESmart Token

2.2.5 Аутентификация с предъявлением отчуждаемого носителя

Для аутентификации с предъявлением отчуждаемого носителя (USB-накопителя/дискеты) необходимо подключить USB-накопитель/вставить дискету, затем

нажать кнопку ***Removable <Буква диска: метка тома>*** (рис. 11) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 16). Подробное описание назначения полей приведено в п. 2.1.5 настоящего Руководства.

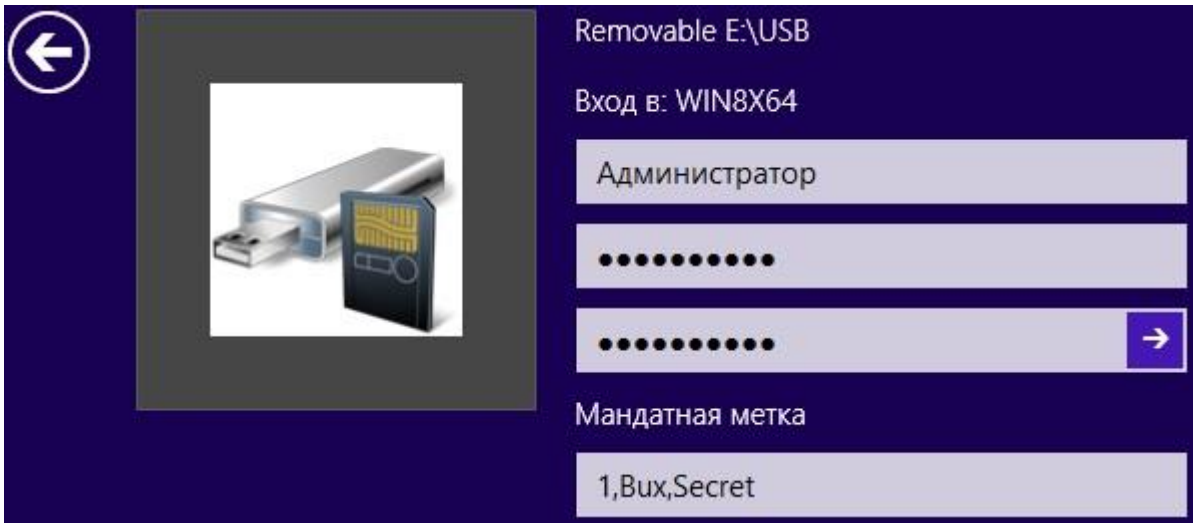


Рисунок 16. Аутентификация в ОС Windows 8.1/2012/2012R2
с предъявлением отчуждаемого носителя

2.2.6 Аутентификация по сертификату пользователя

В СЗИ «Блокхост-сеть 2.0» реализована возможность двухфакторной аутентификации пользователей в домене Microsoft Active Directory с использованием цифровых сертификатов пользователей, выработанных, в том числе с использованием российских криптографических алгоритмов (ГОСТ).

Для аутентификации по сертификату необходимо подключить электронный идентификатор (eToken/SafeNet eToken/JaCarta/Avest Token/ESMART Token/ruToken), содержащий сертификат пользователя и нажать кнопку ***Вход со смарт-картой <Имя пользователя>*** (рис. 10). В открывшемся диалоговом окне идентификации пользователя нужно в соответствующие поля ввести PIN-код доступа к подключенному носителю и значение мандатной метки пользователя:

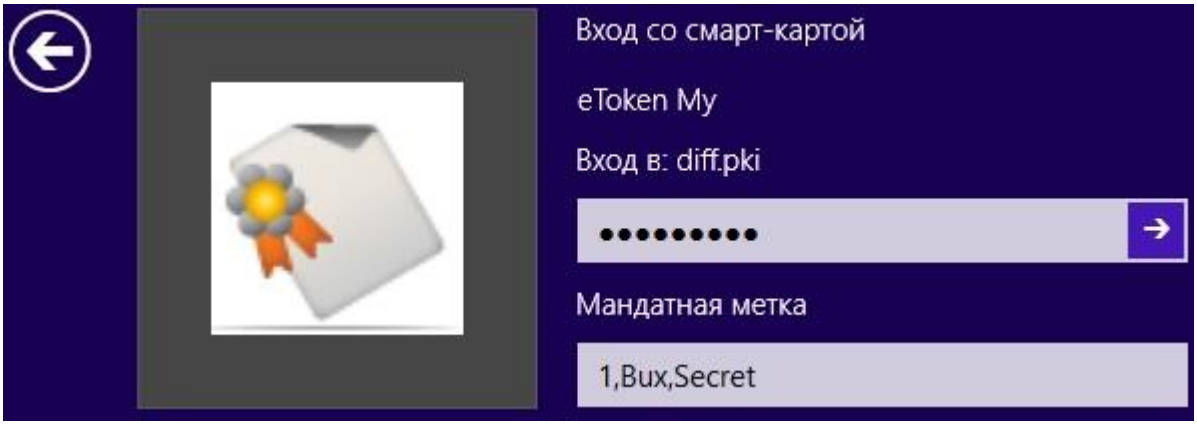


Рисунок 17. Вход в ОС Windows 8.1/2012/2012R2 по сертификату

Остальные данные пользователя будут автоматически считаны из сертификата, записанного на носителе.

2.2.7 Аутентификация с использованием персонального идентификатора пользователя, хранящегося в реестре Windows

Для аутентификации с использованием персонального идентификатора пользователя, хранящегося в реестре Windows, следует нажать кнопку ***Registry <Имя контейнера>*** (рис. 11) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 18). Подробное описание назначения полей приведено в п. 2.1.7 настоящего Руководства.

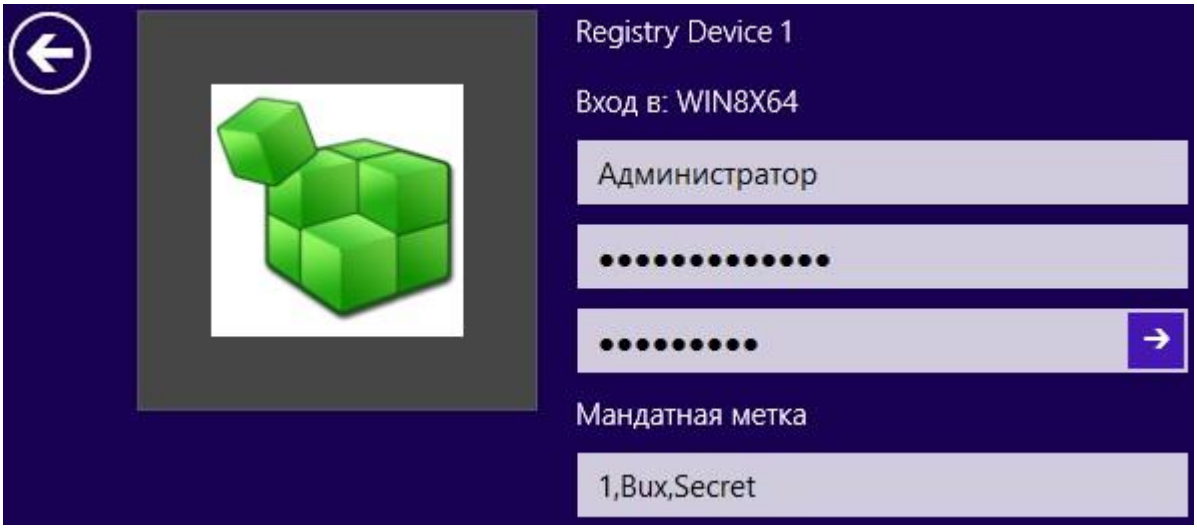


Рисунок 18. Аутентификация в ОС Windows 8.1/2012/2012R2 с предъявлением персонального идентификатора, хранящегося в реестре Windows

2.2.8 Вход без токена

В СЗИ «Блокхост-сеть 2.0» существует возможность входа пользователей в ОС по паролю без предъявления ключевого носителя. Если администратор безопасности предоставил пользователю возможность входа в ОС без предъявления ключевого носителя, то для входа пользователя в ОС необходимо нажать кнопку ***Вход пользователя*** (см. рис. 11) и заполнить поля, показанные на рисунке 19. Подробное описание назначения полей диалогового окна аутентификации пользователя без предъявления ключевого носителя приведено в п. 2.1.8 настоящего Руководства.

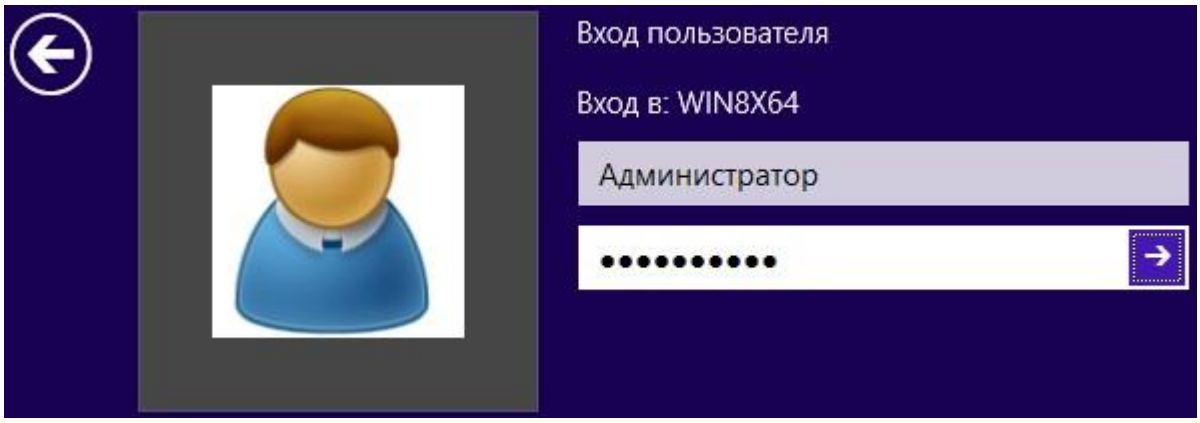


Рисунок 19. Вход пользователя в ОС Windows Windows 8.1/2012/2012R2 без предъявления ключевого носителя

2.3. Аутентификация в ОС Windows 10/Server 2016

При аутентификации в ОС Windows 10/Server 2016 при загрузке системы предусмотрены следующие виды входа в систему (рис. 20):

- вход с предъявлением электронного идентификатора ruToken;
- вход с предъявлением электронного идентификатора eToken/SafeNet eToken (также используется для входа с электронным идентификатором JaCarta PRO, JaCarta ГОСТ, JaCarta PKI);
- вход с предъявлением электронного идентификатора Avest Token;
- вход с предъявлением электронного идентификатора ESmart Token;
- вход с предъявлением отчуждаемого носителя (USB-накопитель/дискета);
- вход по сертификату;
- вход использованием персонального идентификатора пользователя, хранящегося в реестре Windows (значок появляется при условии, что хотя бы одному пользователю в СЗИ присвоен носитель данного вида);
- вход администратора без предъявления электронного идентификатора.

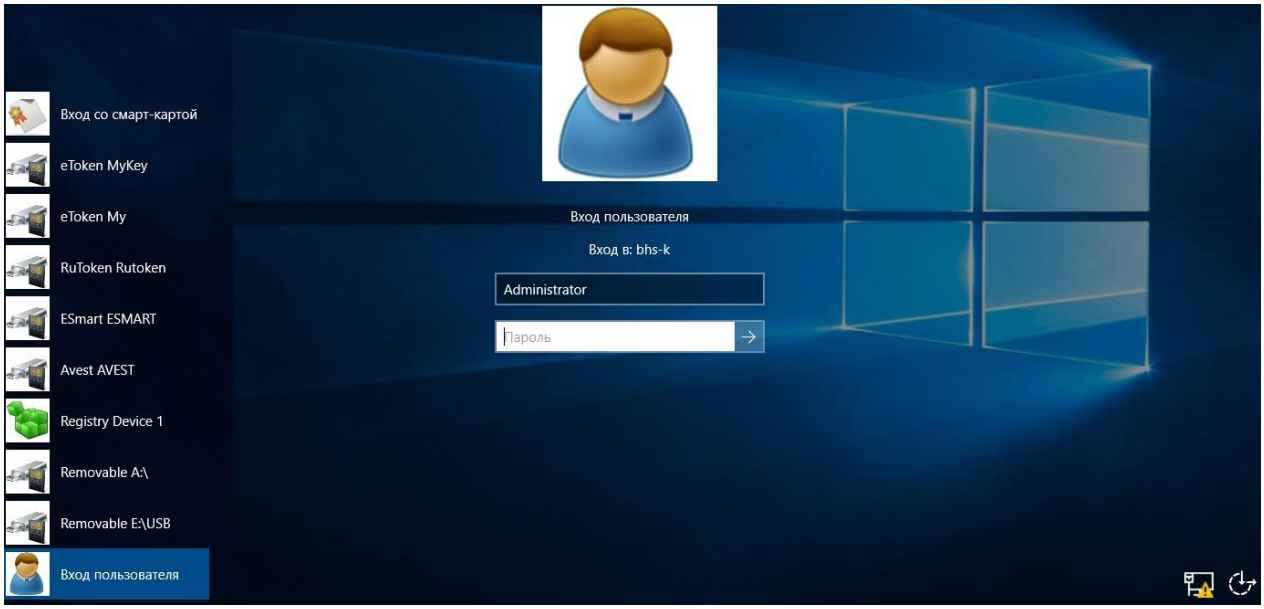


Рисунок 20. Аутентификация в ОС Windows 10/2016

2.3.1 Аутентификация с предъявлением электронного идентификатора ruToken

Для аутентификации в системе с предъявлением электронного идентификатора ruToken необходимо подключить электронный идентификатор ruToken, затем нажать кнопку ***RuToken <Имя носителя>*** и заполнить все поля все поля в диалоговом окне аутентификации пользователя (рис. 21). Подробное описание назначения полей приведено в п. 2.1.1 настоящего руководства.

Рисунок 21. Аутентификация в ОС Windows 10/2016 с предъявлением ruToken

2.3.2 Аутентификация с предъявлением электронного идентификатора eToken/SafeNet eToken/JaCarta

Для аутентификации с предъявлением электронного идентификатора eToken/SafeNet eToken/JaCarta необходимо подключить электронный идентификатор eToken/SafeNet eToken/JaCarta затем нажать кнопку ***eToken <Имя устройства считывания>*** (рис. 20) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 22). Подробное описание назначения полей приведено в п. 2.1.2 настоящего Руководства.

Рисунок 22. Аутентификация в ОС Windows 10/2016
с предъявлением eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI

2.3.3 Аутентификация с предъявлением электронного идентификатора Avest Token

Для аутентификации с предъявлением электронного идентификатора Avest Token необходимо подключить электронный идентификатор AvBign, затем нажать кнопку ***Avest <Имя носителя>*** (рис. 20) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 23). Подробное описание назначения полей приведено в п. 2.1.3 настоящего Руководства.

Рисунок 23. Аутентификация в ОС Windows 10/2016 с предъявлением Avest Token

2.3.4 Аутентификация с предъявлением электронного идентификатора ESMART Token

Для аутентификации с предъявлением электронного идентификатора ESMART Token необходимо подключить электронный идентификатор ESmart, затем нажать кнопку ***ESMART <Имя носителя>*** (рис. 20) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 24). Подробное описание назначения полей приведено в п. 2.1.4 настоящего Руководства.

Рисунок 24. Аутентификация в ОС Windows 10/2016 с предъявлением ESmart Token

2.3.5 Аутентификация с предъявлением отчуждаемого носителя

Для аутентификации с предъявлением отчуждаемого носителя (USB-накопителя/дискеты) необходимо подключить USB-накопитель/вставить дискету, затем нажать кнопку ***Removable <Буква диска: метка тома>*** (рис. 20) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 25). Подробное описание назначения полей приведено в п. 2.1.5 настоящего Руководства.

Рисунок 25. Аутентификация в ОС Windows 10/2016 с предъявлением отчуждаемого носителя

2.3.6 Аутентификация по сертификату пользователя

В СЗИ «Блокхост-сеть 2.0» реализована возможность двухфакторной аутентификации пользователей в домене Microsoft Active Directory с использованием цифровых сертификатов пользователей, выработанных, в том числе с использованием российских криптографических алгоритмов (ГОСТ).

Для аутентификации по сертификату необходимо подключить электронный идентификатор (eToken/SafeNet eToken/JaCarta/Avest Token/ESMART Token/ruToken), содержащий сертификат пользователя и нажать кнопку ***Вход со смарт-картой <Имя пользователя>*** (рис. 20). В открывшемся диалоговом окне идентификации пользователя нужно в соответствующие поля ввести PIN-код доступа к подключенному носителю и значение мандатной метки пользователя (рис. 26).

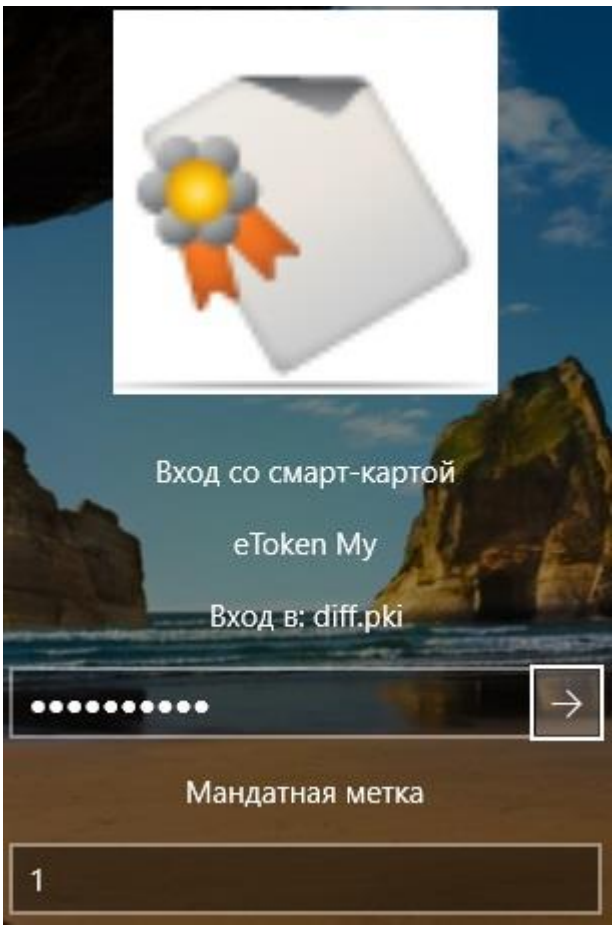


Рисунок 26. Вход в ОС Windows 10/2016 по сертификату

Остальные данные пользователя будут автоматически считаны из сертификата, записанного на носителе.

2.3.7 Аутентификация с использованием персонального идентификатора пользователя, хранящегося в реестре Windows

Для аутентификации с использованием персонального идентификатора пользователя, хранящегося в реестре Windows, следует нажать кнопку ***Registry <Имя контейнера>*** (рис. 20) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 27). Подробное описание назначения полей приведено в п. 2.1.7 настоящего Руководства.

Рисунок 27. Аутентификация в ОС Windows 10/2016 с предъявлением персонального идентификатора, хранящегося в реестре Windows

2.3.8 Вход без токена

В СЗИ «Блокхост-сеть 2.0» существует возможность входа пользователей в ОС по паролю без предъявления ключевого носителя. Если администратор безопасности предоставил пользователю возможность входа в ОС без предъявления ключевого носителя, то для входа пользователя в ОС необходимо нажать кнопку ***Вход пользователя*** (см. рис. 20) и заполнить поля, показанные на рисунке 28. Подробное описание назначения полей диалогового окна аутентификации пользователя без предъявления ключевого носителя приведено в п. 2.1.8 настоящего Руководства.

Рисунок 28. Вход пользователя в ОС Windows 10/2016 без предъявления ключевого носителя

2.4. Виды входа

Чтобы войти в систему с установленным СЗИ «Блокхост-сеть 2.0», необходимо ввести имя пользователя и пароль, а также «предъявить» персональный идентификатор и ввести PIN-код доступа к нему.

В СЗИ «Блокхост-сеть 2.0» поддерживаются два варианта (режима) входа в систему:

- с вводом пароля с клавиатуры (стандартная аутентификация);
- с автоматическим вводом пароля, предварительно записанным на электронный идентификатор (для режима двухфакторной аутентификации).

2.4.1. Вход по паролю (стандартная аутентификация)

После появления приглашения на вход в систему (см. рис. 1, 2, 10) необходимо выбрать тип идентификатора входа в ОС, в открывшемся окне ввести идентификационные данные пользователя, PIN-код доступа к персональному идентификатору и значение мандатной метки, с которой пользователь выполнит вход в систему.

Если пользователь осуществляет вход в ОС Windows 7/8.1/2008R2/2012/2012R2 со своим идентификатором уже не в первый раз, то, при наличии подключенного к рабочей станции персонального идентификатора пользователя, в качестве первоначального окна приглашения входа в систему открывается диалог ввода идентификационных данных пользователя для этого типа ключевого носителя. При этом в поля ***Домен*** и ***Имя пользователя*** уже введены учетные данные последнего входившего в ОС пользователя.

Следует помнить, что при вводе пароля различаются строчные и прописные буквы, кириллица и латиница. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, необходимо удалить ошибочно набранные символы в строке и заново ввести необходимые значения.

Если все данные, необходимые для аутентификации пользователя, указаны правильно, продолжится загрузка операционной системы. В процессе загрузки на экран будут выводиться сообщения о выполняемых механизмами ОС действиях.

2.4.2. Вход в систему с автоматическим вводом пароля

В СЗИ «Блокхост-сеть 2.0» существует возможность сохранения пароля пользователя на персональном идентификаторе (ключевом носителе). Такая возможность может использоваться для того, чтобы у пользователя не было необходимости запоминать пароль и вводить его при каждом входе в систему. Порядок смены пароля описан в разделе 2.5, а порядок сохранения пароля на персональный идентификатор пользователя – в разделе 2.6 настоящего руководства.

После появления приглашения на вход в систему (окно приглашения входа в систему описано в пунктах 2.1, 2.2 и 2.3 настоящего руководства) пользователю необходимо:

- предъявить свой персональный идентификатор (подключить eToken/SafeNet eToken/ruToken/JaCarta/ESmart Token/Avest Token/USB-накопитель к USB-разъему, вставить дискету в дисковод);
- выбрать тип идентификатора;
- заполнить поля ***Имя пользователя***, ***PIN-код*** и ***Мандатная метка***;
- поле ввода пароля оставить пустым;
- нажать кнопку ***ОК***.

Реакция СЗИ «Блокхост-сеть 2.0» зависит от информации о пароле, записанной на персональном идентификаторе. Возможны следующие варианты:

1. персональный идентификатор содержит актуальный пароль;
2. персональный идентификатор содержит другой пароль, не совпадающий с имеющимся в системе (например, из-за того, что срок действия пароля истек и он был заменен, но не записан на персональный идентификатор);
3. на персональном идентификаторе нет пароля (он не записан).

При наличии на персональном идентификаторе актуального пароля процедура аутентификации успешно завершится и продолжится загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

Если на персональном идентификаторе содержится другой пароль или он отсутствует, на экране появится окно-сообщение **«Пароль неверен»**. Необходимо ввести актуальный пароль в поле ввода ***Пароль*** и нажать кнопку ***ОК***. Реакция СЗИ «Блокхост-сеть 2.0» на неправильный ввод пароля настраивается администратором безопасности в консоли администрирования СЗИ и предполагает блокировку пользователя, от имени которого осуществлялась авторизация, на определенное время.

Если при первом входе пользователя в ОС появляется окно смены пароля, это может означать, например, что нарушены требования к минимальной длине пароля (8 символов). В этом случае необходимо задать пароль, удовлетворяющий требованиям к минимальной длине пароля.

При входе по сертификату необходимо предъявить электронный идентификатор (eToken/SafeNet eToken/ruToken/JaCarta/ESmart Token/Avest Token), содержащий сертификат пользователя, ввести PIN-код доступа к ключевому носителю и указать значение мандатной метки пользователя. Остальные данные пользователя будут автоматически считаны с носителя.

2.5. Смена пароля

2.5.1. Смена пароля в ОС Windows 2008R2/7

Для смены пароля текущего пользователя в ОС Windows 7/Server 2008R2 необходимо:

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
2) нажать кнопку-ссылку ***Сменить пароль*** (***Change a password***);
3) в открывшемся диалоге смены пароля заполнить поля ***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***:

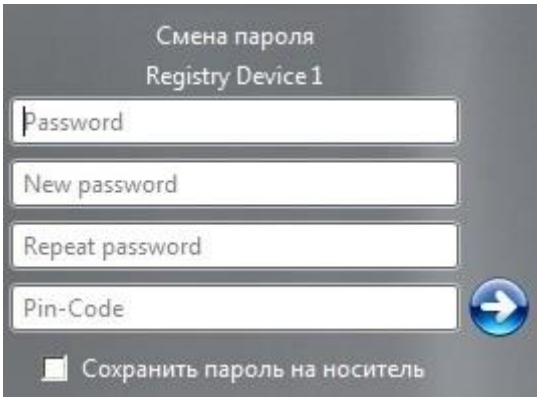


Рисунок 29. Диалоговое окно смены пароля в ОС 2008R2/7

4) ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;
5) при необходимости сохранения нового пароля пользователя на ключевом носителе отметить параметр ***Сохранить пароль на носитель***;
6) нажать кнопку подтверждения или клавишу **<Enter>**.

Если требования, предъявляемые в системе (домене) к паролям, нарушены, старый пароль или PIN-код доступа к идентификатору указаны неправильно, на экране появится сообщение об ошибке. Нажмите кнопку ***ОК*** в окне сообщения и исправьте неверные данные, установив новый пароль в соответствии с установленными политиками.

2.5.2. Смена пароля в ОС Windows 8.1/Server 2012/2012R2

Для смены пароля текущего пользователя в ОС Windows 8.1/Server 2012/2012R2 необходимо:

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
2) нажать кнопку ***Сменить пароль*** (***Change a password***);
3) в открывшемся диалоге смены пароля (рис. 30) заполнить поля ***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***;

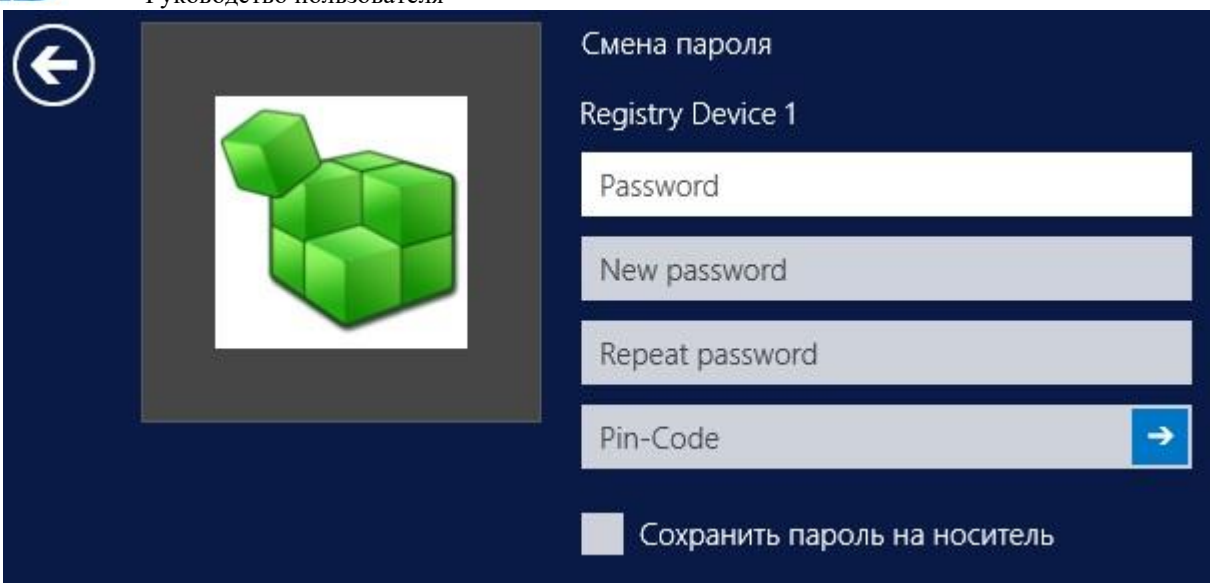


Рисунок 30. Диалоговое окно смены пароля в ОС Windows 8.1/2012/2012R2

4) ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;

5) при необходимости сохранения нового пароля пользователя на ключевом носителе отметить параметр ***Сохранить пароль на носитель***;

6) нажать кнопку подтверждения или клавишу **<Enter>**.

Если требования, предъявляемые в системе (домене) к паролям, нарушены, старый пароль или PIN-код доступа к идентификатору указаны неправильно, на экране появится сообщение об ошибке. Нажмите кнопку ***ОК*** в окне сообщения и исправьте неверные данные, установив новый пароль в соответствии с установленными политиками.

2.5.3. Смена пароля в ОС Windows 10/Server 2016

Для смены пароля текущего пользователя в ОС Windows 10/Server 2016 необходимо:

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;

2) нажать кнопку ***Сменить пароль*** (***Change a password***);

3) в открывшемся диалоге смены пароля (рис. 31) заполнить поля ***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***;

4) ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;

5) при необходимости сохранения нового пароля пользователя на ключевом носителе отметить параметр ***Сохранить пароль на носитель***;

6) нажать кнопку подтверждения или клавишу **<Enter>**.

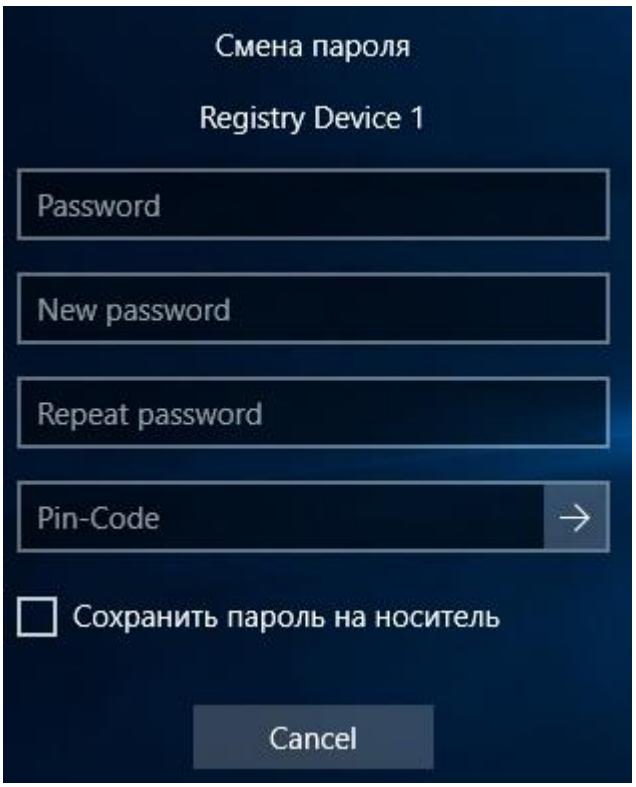


Рисунок 31. Диалоговое окно смены пароля в ОС Windows 10/2016

Если требования, предъявляемые в системе (домене) к паролям, нарушены, старый пароль или PIN-код доступа к идентификатору указаны неправильно, на экране появится сообщение об ошибке. Нажмите кнопку ***ОК*** в окне сообщения и исправьте неверные данные, установив новый пароль в соответствии с установленными политиками.

2.6. Сохранение пароля пользователя на персональный идентификатор

Для записи текущего пароля пользователя на носитель, с которым был осуществлен вход пользователя в ОС Windows, необходимо:

- нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
- в отобразившемся меню нажать кнопку-ссылку ***Сменить пароль*** (***Change a password***);
- в открывшемся диалоге смены пароля (см. примеры на рис. 29, 30, 31) ввести во все поля (***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***) значение текущего пароля пользователя;
- ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;
- отметить параметр ***Сохранить пароль на носитель***;
- нажать кнопку подтверждения или клавишу **<Enter>**;
- нажать кнопку ***ОК*** в окне с сообщением об ошибке операции смены пароля пользователя.

Если PIN-код доступа к персональному идентификатору и пароль пользователя были введены правильно, то пароль текущего пользователя будет записан на персональный идентификатор.

Процедура входа в систему с предъявлением персонального идентификатора с сохраненным паролем описана в пункте 2.4.2 настоящего руководства.

2.7. Изменение PIN-кода персонального идентификатора

Возможность изменения пользователем PIN-кода доступа к ключевым носителям в ОС Windows 2008R2/7/8.1/2012/2012R2/10/2016 через диалоговое окно СЗИ «Блокхост-сеть 2.0» отсутствует.

Для изменения пользователем PIN-кода персональных идентификаторов eToken, SafeNet eToken, JaCarta, ESMART Token, Avest Token и ruToken необходимо воспользоваться специальным программным обеспечением, поставляемым совместно с идентификатором.

Изменить PIN-код доступа к персональным идентификаторам дискета, USB-носитель и реестр ОС Windows может только администратор безопасности из серверной или локальной консоли администрирования СЗИ.

2.8. Временная блокировка компьютера

Если необходимо временно прервать работу на компьютере, то для защиты его от несанкционированного использования можно воспользоваться функцией блокировки и запретить любые действия кроме разблокировки.

2.8.1 Блокировка и разблокировка компьютера в ОС Windows 2008R2/7

Для временной блокировки компьютера вручную:

1. Нажмите комбинацию клавиш **<Ctrl>+<Alt>+<Del>.**
2. Нажмите кнопку ***Блокировать компьютер*/*Lock this computer***.
3. Клавиатура и экран монитора будут заблокированы.

Для блокировки компьютера можно также воспользоваться комбинацией клавиш **<Win>+<L>**, после нажатия этих клавиш рабочая станция будет заблокирована.

Разблокировать компьютер может только работающий на нем пользователь.

Для разблокирования компьютера пользователю необходимо нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**.

В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 32). Пользователю необходимо ввести пароль и PIN-код доступа к своему персональному идентификатору. В случае хранения пароля пользователя на носителе в окне разблокировки достаточно ввести только PIN-код доступа к носителю. При вводе верных идентификационных данных пользователя (пароль и PIN-код) рабочая станция будет разблокирована.

Рисунок 32. Ввод данных пользователя для разблокировки в ОС 2008R2/7

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоге разблокировки системы (см. рис. 32) будет произведен возврат состояния компьютера в режим блокировки.

2.8.2 Блокировка и разблокировка компьютера в ОС Windows 8.1/Server 2012/2012R2

Для временной блокировки компьютера вручную:

1. Нажмите комбинацию клавиш **<Ctrl>+<Alt>+<Del>**.
2. Нажмите кнопку ***Блокировать компьютер*/*Lock this computer***.
3. Клавиатура и экран монитора будут заблокированы.

Для блокировки компьютера можно также воспользоваться комбинацией клавиш **<Win>+<L>**, после нажатия этих клавиш рабочая станция будет заблокирована.

Разблокировать компьютер может только работающий на нем пользователь.

Для разблокирования компьютера пользователю необходимо нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**.

В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 33). Пользователю необходимо ввести пароль и PIN-код доступа к своему персональному идентификатору. В случае хранения пароля пользователя на носителе в окне разблокировки достаточно ввести только PIN-код доступа к носителю. При вводе верных идентификационных данных пользователя (пароль и PIN-код) рабочая станция будет разблокирована.

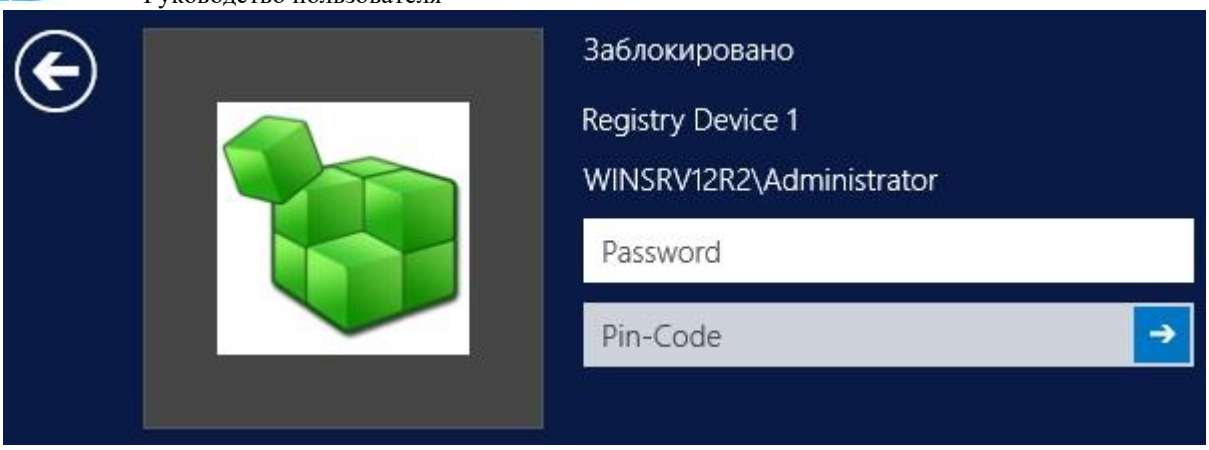


Рисунок 33. Ввод данных пользователя для разблокировки в ОС Windows 8.1/2012/2012R2

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоге разблокировки системы (см. рис. 33) будет произведен возврат состояния компьютера в режим блокировки.

2.8.3 Блокировка и разблокировка компьютера в ОС Windows 10/Server 2016

Для временной блокировки компьютера вручную:

1. Нажмите комбинацию клавиш **<Ctrl>+<Alt>+<Del>**.
2. Нажмите кнопку ***Заблокировать/Lock***.
3. Клавиатура и экран монитора будут заблокированы.

Для блокировки компьютера можно также воспользоваться комбинацией клавиш **<Win>+<L>**, после нажатия этих клавиш рабочая станция будет заблокирована.

Разблокировать компьютер может только работающий на нем пользователь.

Для разблокирования компьютера пользователю необходимо нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**.

В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 34). Пользователю необходимо ввести пароль и PIN-код доступа к своему персональному идентификатору. В случае хранения пароля пользователя на носителе в окне разблокировки достаточно ввести только PIN-код доступа к носителю. При вводе верных идентификационных данных пользователя (пароль и PIN-код) рабочая станция будет разблокирована.

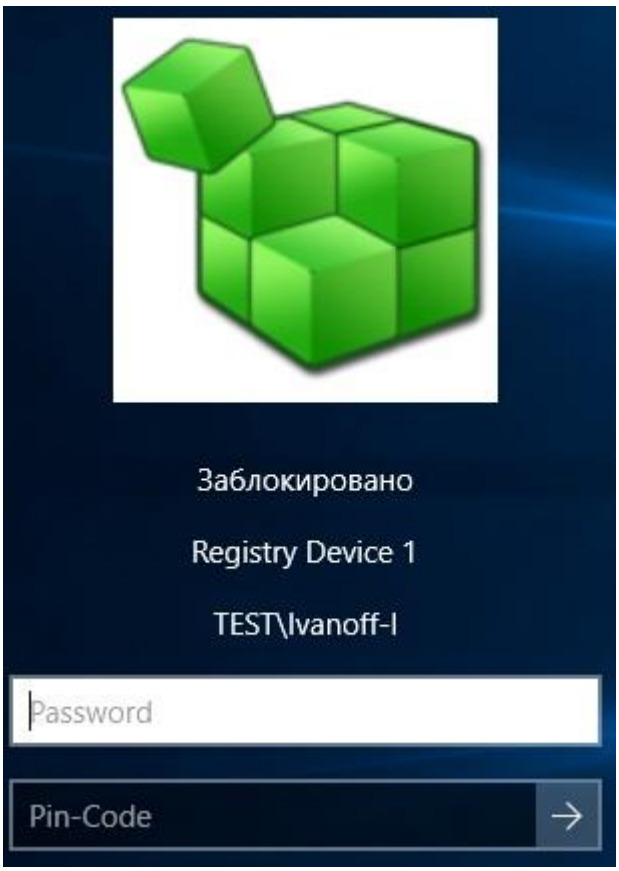


Рисунок 34. Ввод данных пользователя для разблокировки в ОС Windows 10

2.8.4. Автоматическая блокировка компьютера при отключении ключевого носителя

Для рабочих станций-клиентов СЗИ «Блокхост-сеть 2.0», **включенных в домен**, можно настроить автоматическую блокировку ОС в момент изъятия (отключения) из компьютера ключевого носителя пользователя. Для этого необходимо воспользоваться механизмом настройки групповых политик домена:

1. на контроллере домена настроить политику действий при изъятии смарт-карты: ***Параметры безопасности →Локальные политики →Параметры безопасности →Интерактивный вход в систему: поведение при извлечении смарт-карты →Блокировка смарт-карты***;

2. на рабочей станции-клиенте СЗИ запустить службу ***Политика удаления смарт-карт*** и установить для нее автоматический запуск при старте ОС.

В результате после того, как пользователь извлечет из компьютера свой ключевой носитель, рабочая станция будет заблокирована.

Для разблокировки пользователю необходимо вставить свой ключевой носитель в компьютер и произвести действия по авторизации, описанные в пунктах 2.8.1 – 2.8.3 настоящего руководства.

Для рабочих станций, не включенных в домен, а находящихся в рабочей группе, например, Workgroup, настройка локальной политики действий при изъятии смарт-карты не приведет к автоматической блокировке ОС при извлечении из компьютера ключевого носителя пользователя.

3. Работа в условиях ограничения доступа к ресурсам

3.1. Механизмы разграничения доступа

СЗИ «Блокхост-сеть 2.0» реализует дискреционный и мандатный механизмы разграничения доступа пользователей к локальным и сетевым ресурсам компьютера. Эти механизмы позволяет обеспечить надежную защиту ресурсов от несанкционированного доступа и организовать эффективную работу пользователей в защищенной информационной среде.

Дискреционный механизм

Дискреционный режим позволяет разграничить доступ к информации на основе прав и разрешений. Администратором безопасности может быть определен список ресурсов (например, файлов и папок), доступ к которым пользователю разрешен, разрешен только для чтения или запрещен. Для правильного использования этого механизма необходимо учитывать следующие особенности:

- дискреционный механизм разграничения доступа СЗИ «Блокхост-сеть 2.0» работает самостоятельно и совместно с аналогичным «штатным» механизмом ОС семейства Windows. Взаимодействие этих двух механизмов осуществляется по схеме «И» в сторону ужесточения правил доступа;
- у каждого из защищаемых ресурсов есть владелец, который может самостоятельно реализовать права и разрешения доступа к своему ресурсу для каждого пользователя.

Мандатный механизм

Мандатный механизм разграничения доступа основан на возможности назначения администратором безопасности пользователям и ресурсам числовых (иерархических) меток, характеризующих уровень полномочий пользователей и уровень конфиденциальности (доступности) ресурсов, соответственно, и неиерархических категорий. При обращении к объектам информации данные об уровне полномочий пользователя, хранящиеся в базе данных настроек СЗИ, сравниваются с уровнем конфиденциальности информации и, на основе этих данных, принимается решение о возможности проведения операций пользователя над информацией. Для правильного использования этого механизма необходимо учитывать следующие особенности:

- чем больше значение иерархической метки, тем большими правами обладает пользователь и тем выше уровень конфиденциальности защищаемых ресурсов;
- только администратор безопасности или пользователь, наделенный правами администратора безопасности, может изменять значение метки и категории;
- мандатный механизм разграничения доступа СЗИ «Блокхост-сеть 2.0» работает совместно с его дискреционным механизмом и дискреционным механизмом ОС Windows. Взаимодействие всех механизмов осуществляется по схеме «И» в сторону ужесточения правил доступа;
- существует возможность задания для пользователя динамической иерархической метки, которая позволит ему работать с документами разных уровней конфиденциальности. Для смены уровня доступа пользователю в этом

случае достаточно войти в систему с указанием другого значения метки и/или категории.

Работа мандатного и дискреционного механизмов разграничения доступа дополняется возможностью организации аудита событий и наличием механизма гарантированного удаления объектов, которые помогают сделать систему более защищенной и контролируемой.

3.2. Правила работы с конфиденциальными ресурсами

При мандатном режиме работы пользователи могут осуществлять следующие виды доступа к файлам:

- Доступ на ***чтение***. **Пользователь может читать информацию из файла, если его уровень доступа не меньше, чем уровень конфиденциальности файла, к которому выполняется попытка доступа**. Пользователь может скопировать файл при условии строгого равенства уровня доступа пользователя, уровня конфиденциальности копируемого объекта и уровня конфиденциальности объекта файловой системы (например, папки или файла), в который производится копирование.
- Доступ на ***запись***. **Пользователь может осуществлять запись в объект, только если его уровень доступа равен уровню конфиденциальности объекта.**

Для выполнения операции записи пользователю, имеющему большее значение уровня доступа, необходимо выполнить вход в систему с тем уровнем доступа, который соответствует значению ресурса, открываемого на запись.

Вид доступа	Соотношение уровня доступа субъекта (МС) и уровня конфиденциальности объекта (МО)
Чтение	**МС ≥ МО**
Запись	**МС = МО**

При дискреционном режиме работы возможны следующие виды доступа:

- Доступ на ***чтение***. Пользователю разрешается читать информацию из файла или папки и предоставляется возможность копирования объекта в любое место, незапрещенное данным или другим механизмом разграничения доступа.
- Доступ на ***запись***. С помощью этого вида доступа осуществляется управление доступом пользователей по изменению содержимого файла, удалению, переименованию и перемещению файла.