GIS ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3»

Руководство пользователя

Санкт-Петербург, 2019

Содержание

1 Общие сведения

1.1 Назначение СЗИ «Блокхост-Сеть 3»

Средство защиты информации «Блокхост-Сеть 3» является программным средством защиты информации от несанкционированного доступа к информации, предназначенным 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 операционных систем (ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

1.2 Необходимая информация

Для работы с компьютером, защищенным СЗИ «Блокхост-Сеть 3», пользователь должен знать и иметь:

№ п/п	Наименование	Описание
1	Имя	Идентификатор пользователя для СЗИ «Блокхост-Сеть 3» и ОС Windows
2	Пароль	Для проверки подлинности пользователя в СЗИ «Блокхост-Сеть 3» 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 3»
5	Персональный идентификатор (eToken/SafeNet eToken/JaCarta/AvBign/E SMART Token/ ruToken/USB-накопитель/дискета/ персональный идентификатор пользователя, расположенный в реестре Windows)	Для хранения ключевой информации СЗИ «Блокхост-Сеть 3» и аутентификации пользователя (при использовании двухфакторной аутентификации)
6	PIN-код	Пароль персонального идентификатора для доступа к ключевой информации СЗИ «Блокхост-Сеть 3» (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 3», 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 3» используются персональные идентификаторы: eToken\SafeNet eToken\ruToken\JaCarta\AvBign\ESMART Token\USB-накопитель или дискета\ персональный идентификатор пользователя, расположенный в хранилище реестра Windows (далее – персональный идентификатор в реестре), на которых записана ключевая информация для доступа в систему. При использовании двухфакторной аутентификации СЗИ «Блокхост-Сеть 3» 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 3».

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 3» 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 3» 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. 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 3» можно только под встроенной учетной записью администратора ОС Windows (домена).

2.1. Виды аутентификации при входе в систему

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, eToken, SafeNet eToken; JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, Avest Token, ESMART Token;
- вход с предъявлением отчуждаемого носителя (USB-накопитель/дискета);
- вход по сертификату;
- вход использованием персонального идентификатора в реестре Windows (значок появляется при условии, что одному или более пользователей в СЗИ присвоен носитель данного вида);
- вход пользователя без предъявления электронного идентификатора.

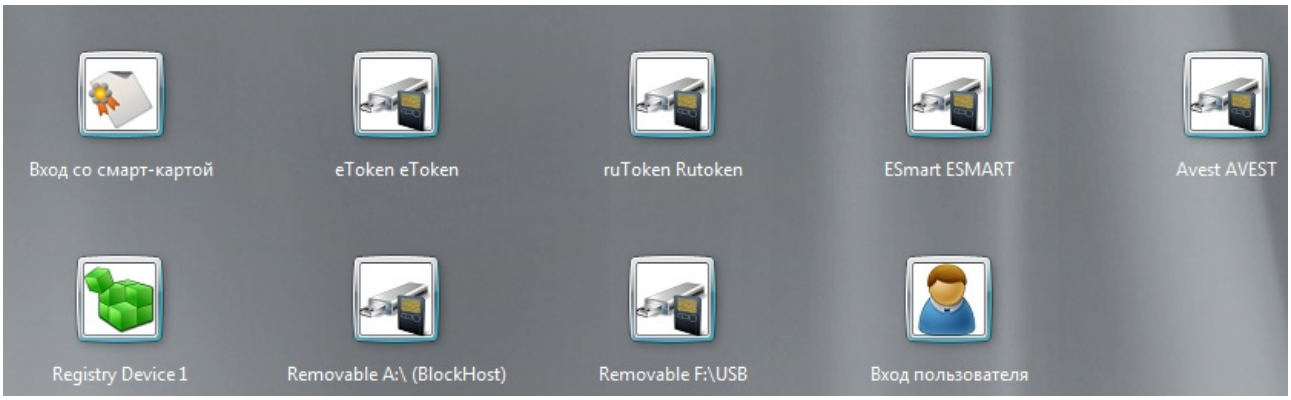

Рисунок 1 – Аутентификация в ОС Windows 2008R2/7

2.1.1 Аутентификация с предъявлением электронного идентификатора/отчуждаемого носителя/персонального идентификатора пользователя в реестре Windows

Для аутентификации в системе с предъявлением электронного идентификатора, отчуждаемого носителя или персонального идентификатора в реестре Windows, необходимо подключить электронный идентификатор /отчуждаемый носитель/персональный идентификатор в реестре Windows, затем нажать кнопку с необходимым типом 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 носителю;
- ***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.

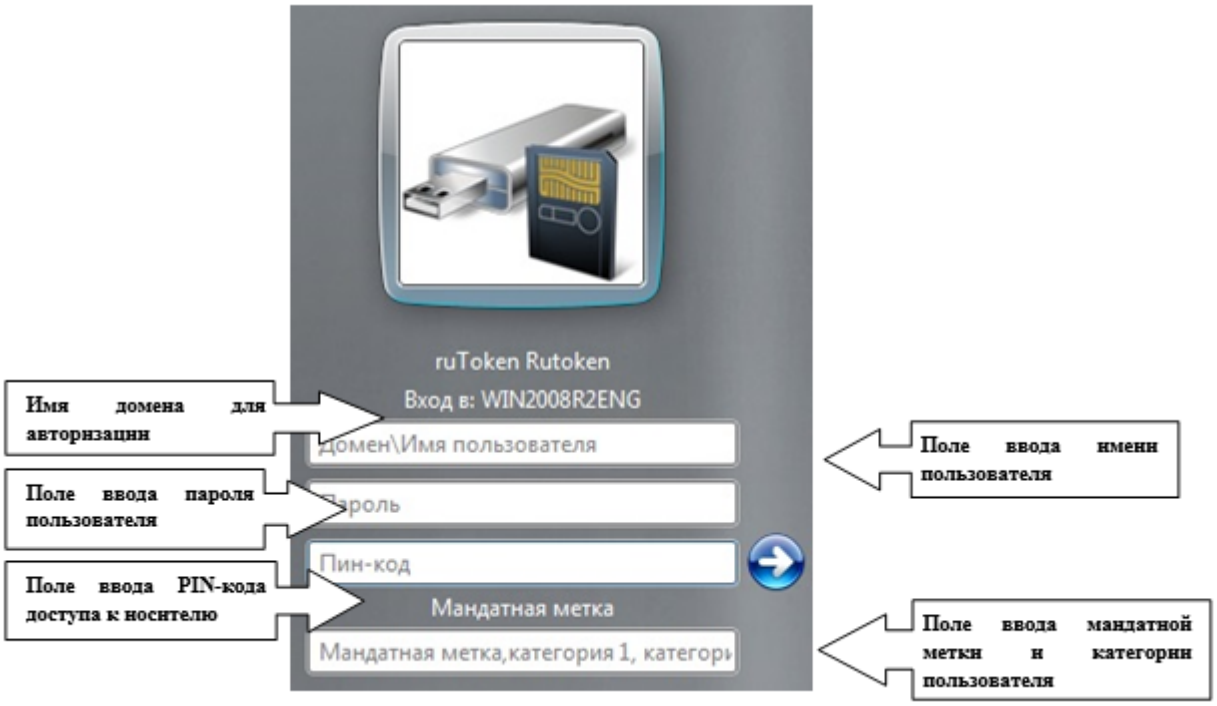

Рисунок 2 – Аутентификация в ОС Windows Server 2008R2 с предъявлением ruToken

2.1.2 Аутентификация по сертификату пользователя

В СЗИ «Блокхост-Сеть 3» реализована возможность двухфакторной аутентификации пользователей средствами СЗИ, при входе в ОС Windows с использованием цифровых сертификатов пользователей.

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. 3) 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.

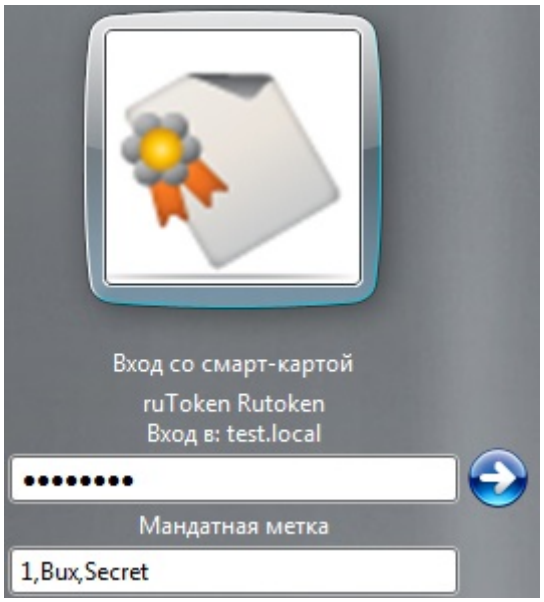

Рисунок 3 – Вход ОС Windows 2008R2/7 по сертификату

2.1.3 Вход без токена

В СЗИ «Блокхост-Сеть 3» 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 пользователя, который имеет право входа в ОС без предъявления ключевого носителя.

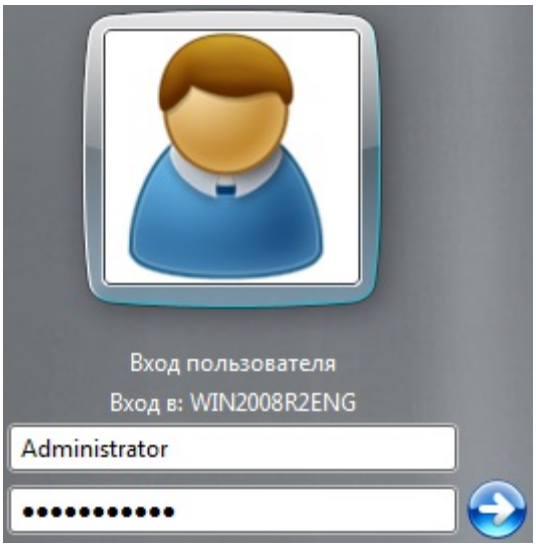

Рисунок 4 – Вход пользователя в ОС Windows 2008R2/7 без предъявления ключевого носителя

2.2 Виды входа в ОС

Чтобы войти в систему с установленным СЗИ «Блокхост-Сеть 3», необходимо ввести имя пользователя и пароль, а также «предъявить» персональный идентификатор и ввести PIN-код доступа к нему.

В СЗИ «Блокхост-Сеть 3» поддерживаются два варианта (режима) входа в систему:

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

Дополнительно в СЗИ «Блокхост-Сеть 3», при использовании режима двухфакторной аутентификации, реализована функция ***Автовход***, которая позволяет осуществлять вход от имени заданного пользователя в систему без ввода данных в окно аутентификации СЗИ «Блокхост-Сеть 3».

После включения данной опции, при загрузке ОС происходит автоматический вход в систему под учетной записью указанного пользователя, при этом интерактивная работа пользователя блокируется с целью обеспечения защиты информации от несанкционированного использования (окно блокировки интерактивной сессии операционной системы). Для разблокирования сессии пользователю необходимо ввести свои идентификационные и аутентификационные данные.

Подробнее работа функции ***Автовход*** рассмотрена в руководстве администратора.

2.2.1 Вход по паролю (стандартная аутентификация)

После появления приглашения на вход в систему (см. рис. 1) 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.

2.2.2 Вход в систему с автоматическим вводом пароля

В СЗИ «Блокхост-Сеть 3», при использовании режима двухфакторной аутентификации пользователя, 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 2.3, а порядок сохранения пароля на персональный идентификатор пользователя – в разделе 2.4 настоящего руководства.

После появления приглашения на вход в систему (окно приглашения входа в систему описано в пункте 2.1 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 3» 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).

Если в персональном идентификаторе содержится актуальный пароль, то после успешной проверки прав пользователя на вход в систему продолжится загрузка операционной системы. В процессе загрузки на экран будут выводиться сообщения о выполняемых механизмами ОС действиях.

Если идентификатор содержит другой пароль, или пароль на идентификаторе отсутствует, на экране появится сообщение о неверном пароле. После ознакомления с сообщением (нажатие кнопки ***ОК***) произойдет возврат в диалог ввода идентификационной информации пользователя, в котором необходимо выбрать домен, ввести имя пользователя и его актуальный пароль, PIN-код доступа к персональному идентификатору и мандатную метку. В случае трехкратного ввода неправильного пароля, операционная система перезагрузится.

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.

2.3 Смена пароля пользователя

Для смены пароля текущего пользователя необходимо (в данном разделе приведен пример смены пароля в ОС Windows 7/Server 2008R2):

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

2) нажать кнопку-ссылку ***Сменить пароль***;

3) в открывшемся диалоге смены пароля заполнить поля ***Пароль***, ***Новый пароль***, ***Повторите новый пароль***:

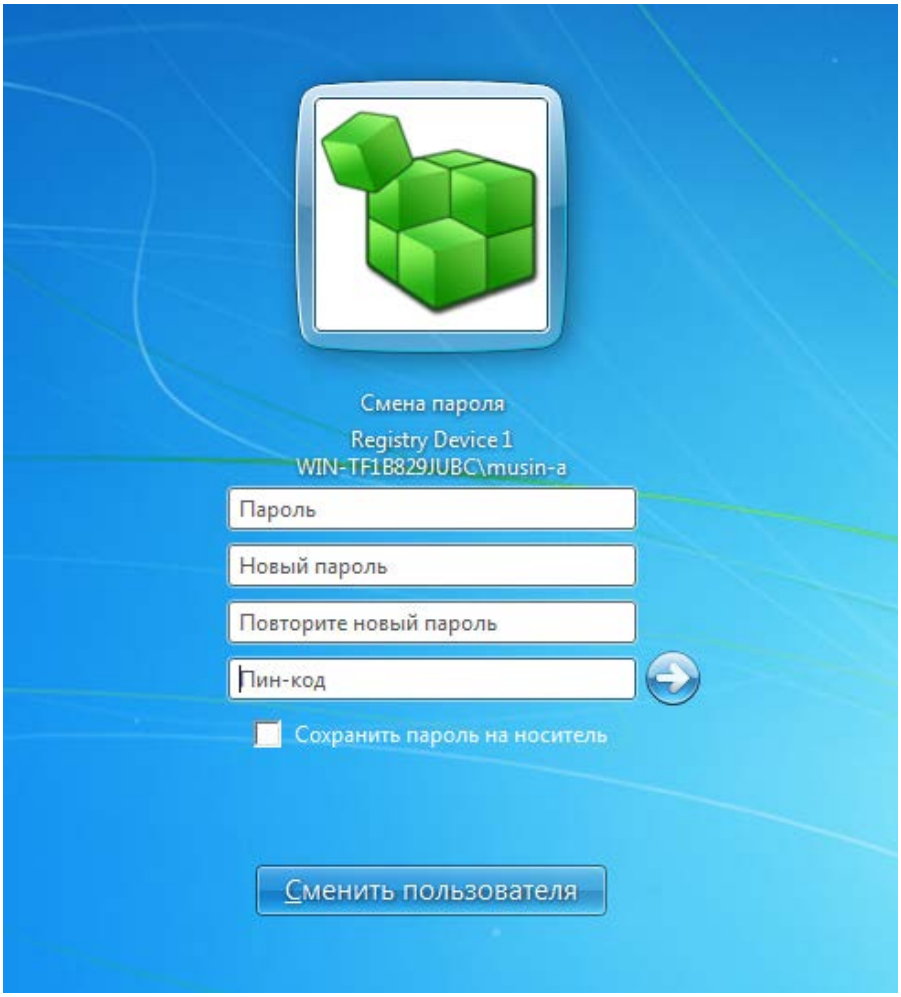

Рисунок 5 – Диалоговое окно смены пароля в ОС 2008R2/7

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

2.4 Запись 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 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.

2.5 Изменение PIN-кода персонального идентификатора

При задании/изменении PIN-кода для персональных электронных идентификаторов eToken, SafeNet eToken, ruToken, JaCarta, ESMART Token и Avest Token с использованием СЗИ «Блокхост-Сеть 3» не следует использовать символы русского алфавита.

Операция смены PIN-кода персонального идентификатора пользователя может быть произведена самостоятельно пользователем – через диалоговое окно СЗИ «Блокхост-Сеть 3» (в случае несоответствия PIN-кода требованиям установленной политики

безопасности или в случае установки АБ требования смены PIN-кода в консоли администрирования, рисунок 6).

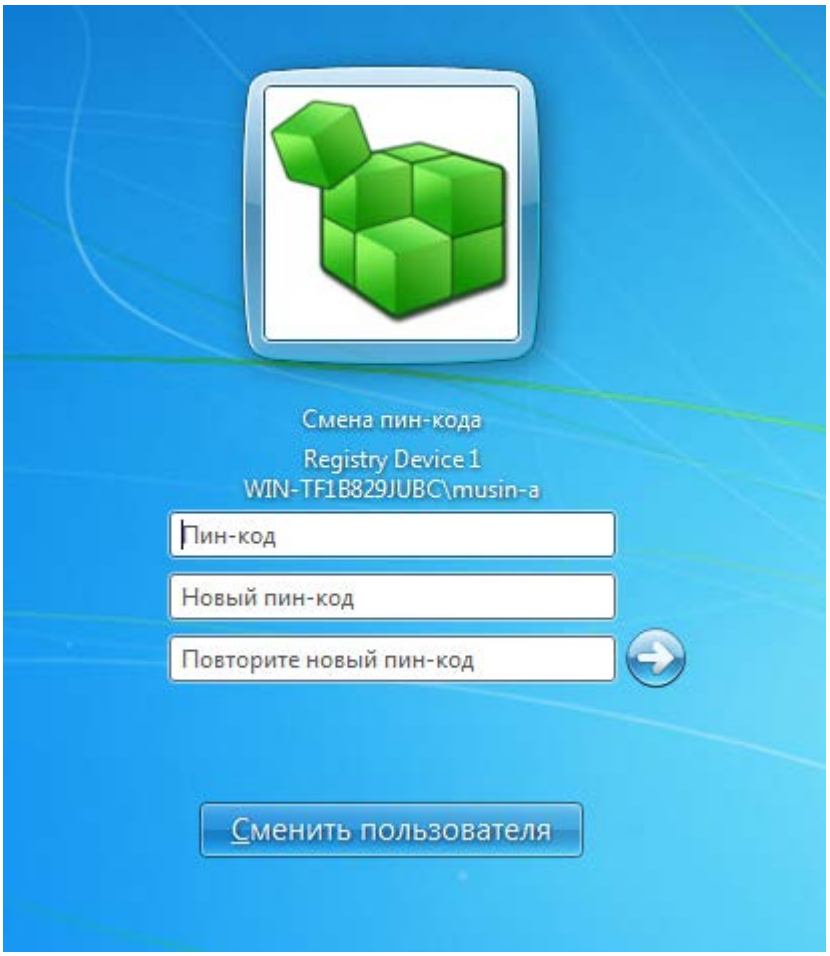

Рисунок 6 – Диалоговое окно смены PIN-кода в ОС Windows Server 2008R2

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.

2.6 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.

2.6.1 Блокировка и разблокировка компьютера

Для временной блокировки компьютера вручную (в данном разделе приведен пример блокировки/разблокировки в ОС Windows 7/Server 2008R2):

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 7). 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.

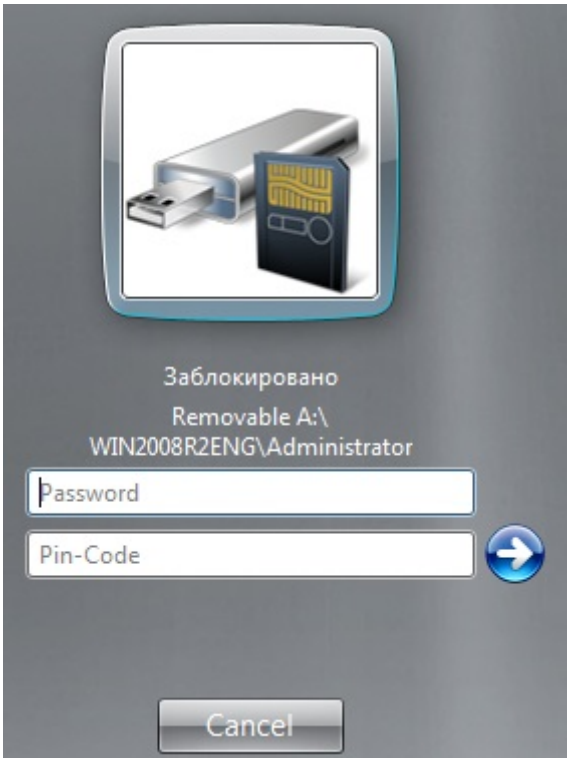

Рисунок 7 – Ввод данных пользователя для разблокировки в ОС Windows Server 2008R2

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоге разблокировки системы (см. рис. 7) будет произведен возврат состояния компьютера в режим блокировки.

2.6.2 Автоматическая блокировка компьютера при отключении ключевого носителя

Для рабочих станций-клиентов СЗИ «Блокхост-Сеть 3», **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 пункте 2.6.1 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 3» реализует дискреционный механизм и мандатное разграничение 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.

3.1.1 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 3» 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.

3.1.2 Мандатное разграничение

Мандатное разграничение доступа основано 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;

- мандатное разграничение доступа СЗИ «Блокхост-Сеть 3» 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.