ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство пользователя

Санкт-Петербург, 2024

Аннотация

В документе содержатся требования к аутентификации пользователя при входе пользователя в операционную систему (ОС) и описаны возможные виды входа пользователя в ОС при работе на рабочей станции, защищенной СЗИ от НСД «Блокхост-Сеть 4».

Содержание

1 Назначение СЗИ от НСД «Блокхост-Сеть 4» 4
1.1 Назначение СЗИ от НСД «Блокхост-Сеть 4» 4
1.2 Требования к программной и аппаратной конфигурации 4
1.3 Пакеты для функционирования СЗИ под управлением ОС Linux 6
1.4 Требования к аутентификации пользователя 8
2 Защищенный вход в систему 9
3 Виды аутентификации при входе в ОС Windows 10
3.1 Аутентификация по паролю на токене 10
3.2 Аутентификация по сертификату на токене 17
3.3 Вход без токена 19
3.4 Перевыпуск токена пользователю 20
4 Виды аутентификации при входе в ОС Linux 21
4.1 Безопасный вход по паролю на токене 22
4.2 Аутентификация по сертификату на токене 31
4.3 Вход без токена 35
4.4 Перевыпуск токена пользователю 36
4.5 Разблокировка сессии пользователя 37
5 Копирование пароля с токена 39
5.1 Копирование пароля с токена в ОС Linux 40
6 Работа в условиях ограничения доступа к ресурсам 41
6.1 Механизмы разграничения доступа 41
6.2 Правила работы с конфиденциальными ресурсами 42
Перечень сокращений 44

1 Назначение СЗИ от НСД «Блокхост-Сеть 4»

1.1 Назначение СЗИ от НСД «Блокхост-Сеть 4»

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4» 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 на базе персональных компьютеров под управлением ОС Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/11/2016/2019/2022, Astra Linux Special Edition (Смоленск), Альт 8 СП, РЕД ОС 7.3 Муром.

1.2 Требования к программной и аппаратной конфигурации

СЗИ от НСД «Блокхост-Сеть 4» устанавливается на ПК с процессорами, имеющими архитектуру x86 и AMD64. Поддерживаемые ОС, под управлением которых функционирует СЗИ, приведены в таблице 1.1.

Таблица 1.1 – Перечень поддерживаемых операционных систем

ОС
MS Windows
Windows Server 2008R2 Foundation Edition SP1 (64-разрядная)
Windows Server 2008R2 Standard Edition SP1 (64-разрядная)
Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная)
Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная)
Windows Server 2012/2012R2 Foundation (64-разрядная)
Windows Server 2012/2012R2 Essentials (64-разрядная)
Windows Server 2012/2012R2 Standard (64-разрядная)
Windows Server 2012/2012R2 Datacenter (64-разрядная)
Windows Server 2016 Standard (64-разрядная)
Windows Server 2016 Datacenter (64-разрядная)
Windows Server 2016 Essentials (64-разрядная)
Windows Server 2019 (64-разрядная)
Windows Server 2022 Standard (64-разрядная)
Windows Server 2022 Essentials (64-разрядная)
Windows Server 2022 Datacenter (64-разрядная)
Windows 7 Professional SP1 (32-разрядная/64-разрядная)
Windows 7 Enterprise SP1 (32-разрядная/64-разрядная
Windows 7 Ultimate SP1 (32-разрядная/64-разрядная)
Windows 8.1 Core (32-разрядная/64-разрядная)

ОС
MS Windows
Windows 8.1 Professional (32-разрядная/64-разрядная)
Windows 8.1 Enterprise (32-разрядная/64-разрядная)
Windows 10 Home (32-разрядная/64-разрядная)
Windows 10 Pro (32-разрядная/64-разрядная)
Windows 10 Enterprise (32-разрядная/64-разрядная)
Windows 11 Home (64-разрядная)
Windows 11 Professional (64-разрядная)
Linux
AstraLinux SE (Смоленск)
Альт 8СП
РЕД ОС 7.3 Муром

Программные и аппаратные требования к средствам вычислительной техники, на которых функционирует клиентская и серверная часть СЗИ приведены в таблице 1.2.

Таблица 1.2 – Программные и аппаратные требования к средствам вычислительной техники, на которых функционирует клиентская и серверная часть СЗИ

Требования	Наименование	Примечание
Требования к производительности	Обусловлены требованиями используемых ОС	см. таблицу 2.1
Аппаратные требования	**Использование персональных идентификаторов**	
	USB-порт	
Дополнительное программное обеспечение	**Обновления**	
	KB3033929, KB4474419, KB4490628	для ОС Windows 7 и Windows Server 2008/2008R2
	KB2921916	в ОС Windows 7 и Windows Server 2008/2008R2 для механизма «Контроль печати»
	Реализация аутентификации с использованием ГОСТ сертификатов – КриптоПро[1]	
	СКЗИ «КриптоПро CSP»	версии 3.6 и выше
	Драйверы токенов	
	Драйверы устройств производителей	
	Программная платформа	
	распространяемый пакет Microsoft Visual C++ 2015-2019 Redistributable	
	NET Framework 4.5.2	При использовании подсистемы ГУПТ

[1] При использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

Требования	Наименование	Примечание
	обновление «Remote Server Administration Tools»: • для ОС Windows 7 "Remote Server Administration Tools for Windows 7" (https://www.microsoft.com/en-us/download/details.aspx?id=7887); • для ОС Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (https://www.microsoft.com/en-us/download/details.aspx?id=28972); для ОС Windows 10 до версии 1903 "Remote Server Administration Tools for Windows 10" (https://www.microsoft.com/en-us/download/details.aspx?id=45520).	При использовании подсистемы управления токенами на клиентских ОС
Системы управления базами данных (СУБД)	СУБД «PostgreSQL»	
	СУБД «Jatoba»	Сертификат соответствия ФСТЭК России № 4327 от 19.11.2020

Ограничения при эксплуатации СЗИ от НСД «Блокхост-Сеть 4» описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Описание применения».

1.3 Пакеты для функционирования СЗИ под управлением ОС Linux

Перед установкой серверной части СЗИ от НСД «Блокхост-Сеть 4», агента развертывания, клиента Блокхост-Сеть или консоли управления, необходимо убедиться, что на рабочей станции под управлением ОС Linux установлены следующие пакеты:

– для ОС AstraLinux SE (Смоленск):

Пакет СЗИ от НСД «Блокхост-Сеть 4»	Сторонние зависимости, наличие которых должен обеспечить администратор для полноценной работы пакета	Сторонние зависимости, устанавливаемые вместе с пакетом автоматически
Серверная часть	-	libxcb-xinerama0 libpq5 ldap-utils libsasl2-modules-gssapi-mit
Клиентская часть	libxcb-xinerama0 ldap-utils libsasl2-modules-gssapi-mit	-
Консоль	libxcb-xinerama0 ldap-utils libsasl2-modules-gssapi-mit	-
Подсистема развертывания	libxcb-xinerama0	-

Пакет СЗИ от НСД «Блокхост-Сеть 4»	Сторонние зависимости, наличие которых должен обеспечить администратор для полноценной работы пакета	Сторонние зависимости, устанавливаемые вместе с пакетом автоматически
Подсистема аутентификации	-	-

– для ОС Альт 8 СП:

Пакет СЗИ от НСД «Блокхост-Сеть 4»	Сторонние зависимости, наличие которых должен обеспечить администратор для полноценной работы пакета	Сторонние зависимости, устанавливаемые вместе с пакетом автоматически
Серверная часть	-	libxcbutil-image libxcbutil-icccm libxcbutil-keysyms libxcb-render-util openldap-clients
Клиентская часть	libxcbutil-image libxcbutil-icccm libxcbutil-keysyms libxcb-render-util openldap-clients	-
Консоль	libxcbutil-image libxcbutil-icccm libxcbutil-keysyms libxcb-render-util openldap-clients	-
Подсистема развертывания	libxcbutil-image libxcbutil-icccm libxcbutil-keysyms libxcb-render-util	-
Подсистема аутентификации	-	-

– для ОС РЕД ОС 7.3 Муром:

Пакет СЗИ от НСД «Блокхост-Сеть 4»	Сторонние зависимости, наличие которых должен обеспечить администратор для полноценной работы пакета	Сторонние зависимости, устанавливаемые вместе с пакетом автоматически
Серверная часть	-	xcb-util-image xcb-util-wm xcb-util-keysyms xcb-util-renderutil openldap-clients
Клиентская часть	xcb-util-image xcb-util-wm xcb-util-keysyms xcb-util-renderutil openldap-clients	-
Консоль	xcb-util-image xcb-util-wm xcb-util-keysyms xcb-util-renderutil openldap-clients	-

Пакет СЗИ от НСД «Блокхост-Сеть 4»	Сторонние зависимости, наличие которых должен обеспечить администратор для полноценной работы пакета	Сторонние зависимости, устанавливаемые вместе с пакетом автоматически
Подсистема развертывания	xcb-util-image xcb-util-wm xcb-util-keysyms xcb-util-renderutil	-
Подсистема аутентификации	-	-

1.4 Требования к аутентификации пользователя

Для обеспечения безопасности защищаемой информации при работе на рабочей станции, защищенной СЗИ от НСД «Блокхост-Сеть 4», пользователь должен обладать следующими данными, предназначенными для аутентификации:

Имя	Идентификатор пользователя для СЗИ от НСД «Блокхост-Сеть 4» и ОС Windows
Пароль	Для проверки подлинности пользователя в СЗИ от НСД «Блокхост-Сеть 4» и ОС Windows
Домен	Тип аутентификации в ОС Windows (локальная или на контроллере домена)
Токен (персональный идентификатор eToken/SafeNet eToken/JaCarta/ ESMART Token/Рутокен)	Для хранения ключевой информации СЗИ от НСД «Блокхост-Сеть 4» и аутентификации пользователя (при использовании двухфакторной аутентификации)
PIN-код	Пароль токена для доступа к ключевой информации (при использовании двухфакторной аутентификации)

2 Защищенный вход в систему

Общая схема аутентификации пользователя в СЗИ от НСД «Блокхост-Сеть 4» реализована следующим образом: идентификационные данные пользователя (имя учетной записи, пароль или, в случае двухфакторной аутентификации, предъявленный токен пользователя и PIN-код доступа к нему) проверяются на контролере домена и в локальной базе данных клиента СЗИ.

Осуществляется проверка введенных имени учетной записи и пароля пользователя:

– соответствие пароля требованиям сложности, установленным в СЗИ;

– сверка введенного пароля с копией в локальной базе данных клиента СЗИ (в режиме аутентификации пользователя без использования токена);

– PIN-код доступа к предъявленному токену пользователя;

– наличие у учетной записи пользователя возможности интерактивного входа в ОС Windows.

Если все проверки завершены успешно, пользователю разрешается вход в операционную систему.

3 Виды аутентификации при входе в ОС Windows

При загрузке предусмотрены следующие виды входа пользователя в систему:

– вход по токену и паролю (БВПП):
  - по PIN-коду со сменой пароля (вход с использованием назначенного токена и вводом PIN-кода токена вместо пароля, при первом входе после ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен);
  - по PIN-коду без смены пароля (вход с использованием назначенного токена и вводом PIN-кода токена вместо пароля, при первом входе после ввода PIN-кода, пароль пользователя будет сохранен на токен без изменений);
  - по паролю без PIN-кода (вход пользователя с использованием назначенного токена и вводом пароля пользователя);
– вход по токену с сертификатом;
– вход пользователя без предъявления токена:
  - по паролю (происходит проверка введенного пароля с паролем пользователя, хранящимся в БД);
  - доверять аутентификации ОС.

Назначение токена пользователю с возможностью записи на него сертификата для входа или используемого для записи сгенерированного пароля, осуществляется администратором безопасности с помощью подсистемы развертывания и аудита.

Описание приведено в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами».

3.1 Аутентификация по паролю на токене

При использовании двухфакторной аутентификации СЗИ от НСД «Блокхост-Сеть 4» вход пользователя в систему и дальнейшая загрузка ОС без предъявления токена невозможны.

При аутентификации с использованием БВПП на токене создается специальный контейнер. При входе пользователь выбирает этот контейнер и вводит PIN-код, при этом пароль пользователя хранится на токене.

Аутентификация с использованием БВПП возможна:

1) По PIN-коду со сменой пароля.

Для перехода на аутентификацию с использованием токена с БВПП со сменой пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-

кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

2) По PIN-коду без смены пароля.

Для перехода на аутентификацию с использованием токена с БВПП без смены пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет сохранен на токен без изменений.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

3) По паролю без PIN-кода.

Вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом пароля пользователя. PIN-код токена вводить не требуется. При этом контейнер БВПП на токене не создается. Для входа необходимо наличие подключенного к рабочей станции токена.

При входе в систему с использованием аутентификации по паролю на токене (для вариантов со сменой пароля и без смены пароля), реакция СЗИ от НСД «Блокхост-Сеть 4» зависит от наличия контейнера БВПП на токене. Возможны следующие варианты:

– на токене еще нет контейнера БВПП (первый вход для перехода на БВПП);
– токен содержит актуальный контейнер БВПП.

При аутентификации по паролю на токене необходимо подключить токен, выбрать контейнер БВПП и заполнить поля:

– ***Пароль*** – вводится пароль, соответствующий введенному имени учетной записи пользователя (только при первом входе);
– ***PIN-код*** – вводится PIN-код доступа к токену.

3.1.1 Первый вход пользователя с использованием пароля на токене

При первом входе пользователя с использованием аутентификации по паролю на токене (со сменой пароля и без смены пароля), СЗИ от НСД «Блокхост-Сеть 4» потребует ввод пароля учетной записи пользователя (рисунок 3.1).

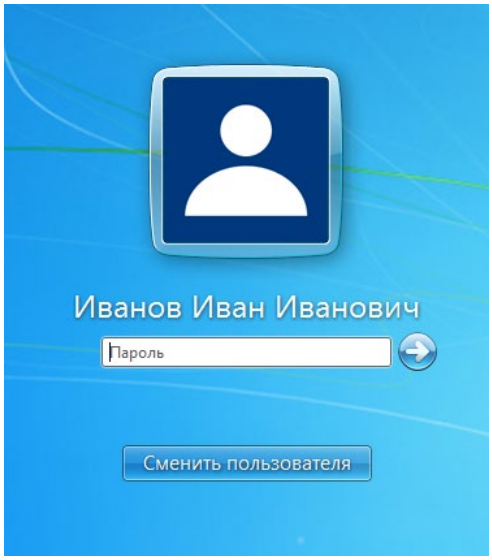


Рисунок 3.1 – Аутентификация по паролю на токене

После ввода пароля появится сообщение о необходимости перехода на двухфакторную аутентификацию (рисунок 3.2).

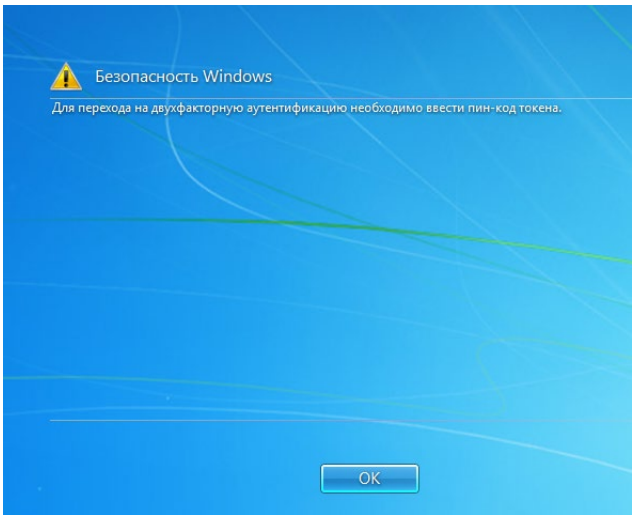


Рисунок 3.2 – Сообщение о необходимости перехода на двухфакторную аутентификацию

После нажатия кнопки ***OK*** появится окно ввода пароля пользователя (заполняется по умолчанию введённым ранее паролем) и PIN-кода к токену (рисунок 3.3).

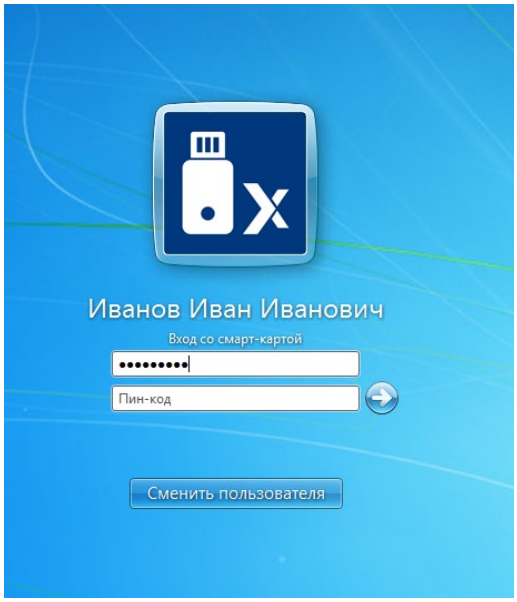


Рисунок 3.3 – Ввод пароля пользователя и PIN-кода токена

После ввода PIN-кода генерируется сложный пароль и записывается на токен, если был выбран вариант со сменой пароля, или записывается текущий пароль пользователя (вариант без смены пароля).

Если администратором безопасности при назначении токена пользователю установлена принудительная смена PIN-кода пользователя при первом входе пользователя по токену, появится сообщение о необходимости сменить PIN-код токена (рисунок 3.4).

Рисунок 3.4 – Необходимость смены PIN-кода токена

После нажатия кнопки ***OK*** появится окно для ввода нового значение PIN-кода пользователя (рисунок 3.5).

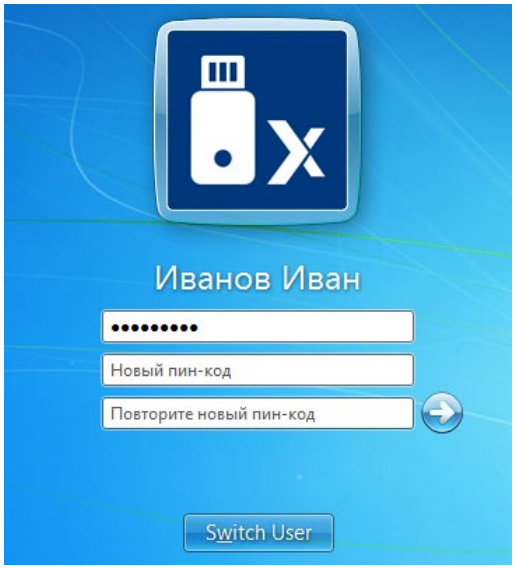


Рисунок 3.5 – Присвоение нового PIN-кода токена

Дальнейший вход пользователя в систему возможен только с использованием измененного PIN-кода.

3.1.2 Аутентификация пользователя по актуальному паролю на токене

Если пароль на токене актуальный, то после ввода PIN-кода токена и успешной проверки прав пользователя на вход в систему, продолжится загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых механизмами ОС действиях.

Окно приглашения на вход при аутентификации пользователя по актуальному паролю на токене приведено на рисунке 3.6.

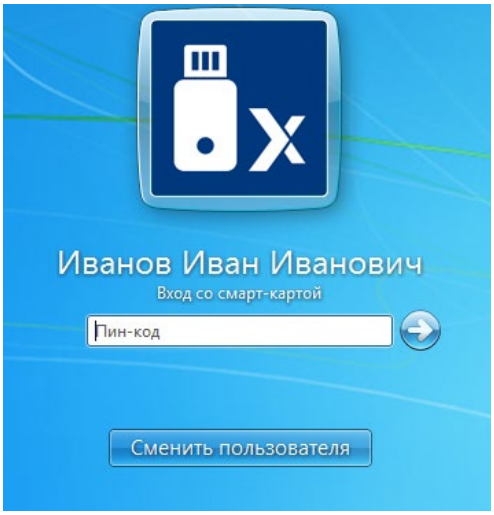
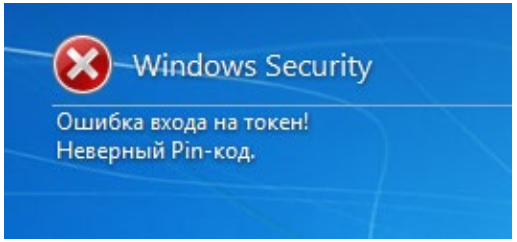
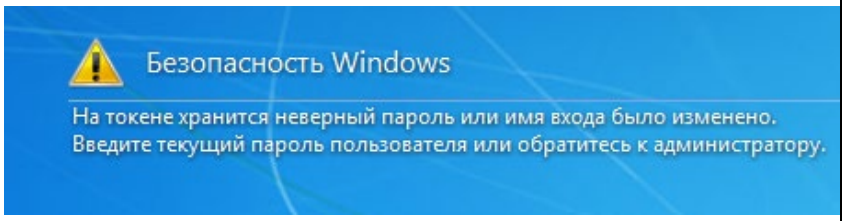
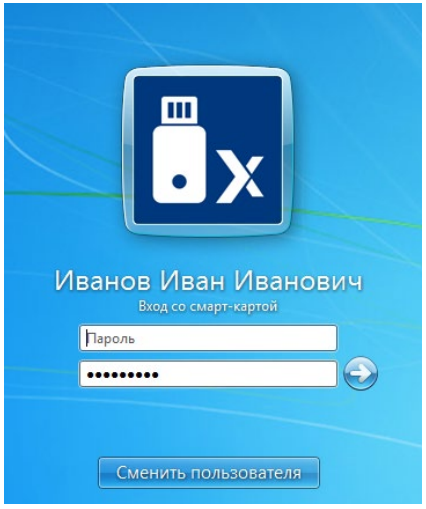
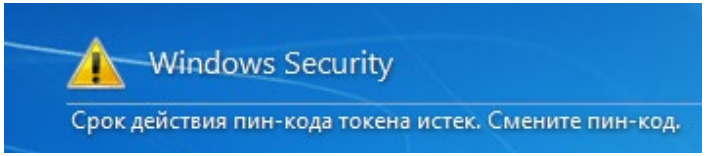
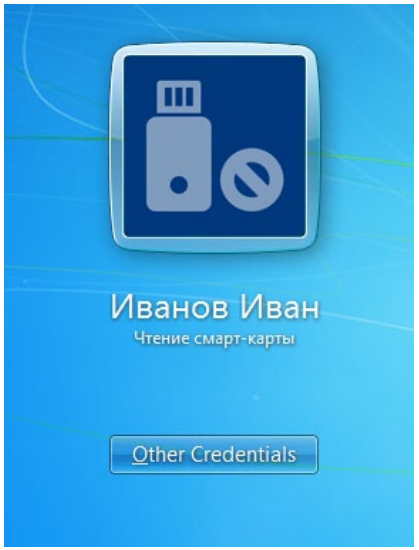
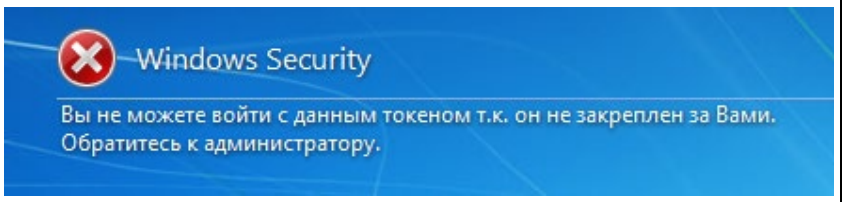


Рисунок 3.6 – Ввод PIN-кода токена

3.1.3 Ошибочные ситуации при аутентификации пользователя по паролю на токене

Введен неверный PIN-код	При вводе неверного PIN-кода появится сообщение об ошибке. После нажатия кнопки *OK*, произойдет возврат к окну аутентификации пользователя для повторного ввода PIN-кода.	
Доменный пароль не совпадает с имеющемся на токене	При входе пользователя с паролем на токене возможны ситуации, когда токен содержит другой пароль, не совпадающий с доменным паролем пользователя (например, пароль пользователя был изменен администратором безопасности).	
	После ознакомления с сообщением и нажатием кнопки *OK* произойдет возврат в диалоговое окно ввода аутентификационной информации пользователя, в котором необходимо ввести актуальный пароль учетной записи пользователя, выданный администратором (при этом PIN-код доступа к токену заполняется автоматически). После ввода пароля, сгенерируется новый пароль пользователя и запишется на токен.	

Срок действия PIN-кода истек	При истечении срока действия PIN-кода токена, появится сообщение о необходимости сменить PIN-код. После нажатия кнопки ***ОК*** появится окно в котором необходимо ввести новое значение PIN-кода пользователя	
Пароль на токене отсутствует	При случайном или намеренном удалении сторонними средствами пароля пользователя с токена, пользователь не сможет войти в систему с использованием токена. Необходимо обратиться к администратору для сброса пароля пользователя и войти с использованием нового пароля, выданным администратором. После ввода пароля, появится сообщение о переходе на двухфакторную аутентификацию. Дальнейшие действия аналогичны описанным в разделе ***Первый вход пользователя по паролю на токене.***	
Токен изъят администратором	При изъятии токена пользователя администратором, после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен не закреплен за пользователем. Необходимо обратиться к администратору для перевыпуска токена пользователю (раздел ***Перевыпуск токена пользователю***).	

3.2 Аутентификация по сертификату на токене

В СЗИ от НСД «Блокхост-Сеть 4» реализована возможность двухфакторной аутентификации пользователей с использованием цифровых сертификатов.

Для аутентификации по сертификату необходимо подключить токен, содержащий сертификат пользователя (рисунок 3.7).

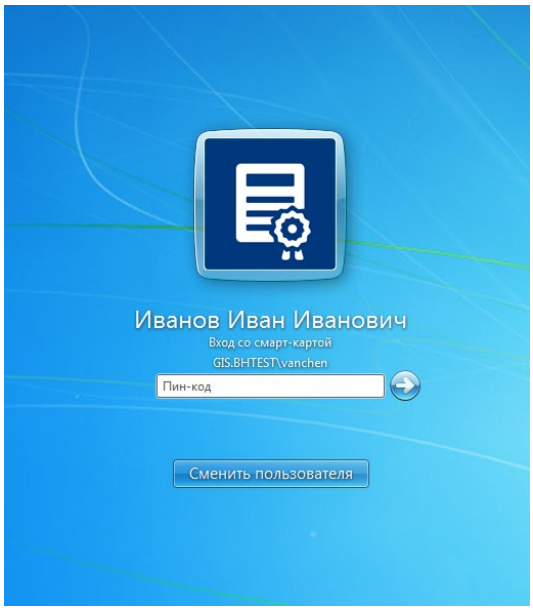
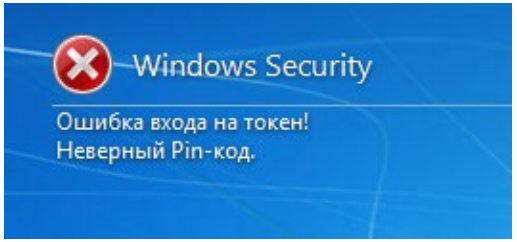
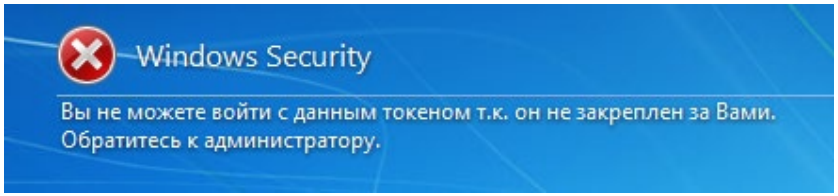


Рисунок 3.7 – Аутентификация пользователя по сертификату

В появившемся окне необходимо ввести PIN-код токена. Остальные данные пользователя будут автоматически считаны с токена.

3.2.1 Ошибочные ситуации при аутентификации пользователя по сертификату на токене

Введен неверный PIN-код	При вводе неверного PIN-кода появится сообщение об ошибке. После нажатия кнопки *OK*, произойдет возврат к окну аутентификации пользователя для повторного ввода PIN-кода.	
Токен временно выключен или отозван администратором,	При временном выключении или отзыве токена пользователя администратором после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен заблокирован администратором. Необходимо обратиться к администратору для включения токена или перевыпуска токена в случае отзыва (раздел ***Перевыпуск токена пользователю***)	
Токен изъят администратором	При изъятии токена пользователя администратором, после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен не закреплен за пользователем. Необходимо обратиться к администратору для перевыпуска токена пользователю (раздел ***Перевыпуск токена пользователю***).	

3.3 Вход без токена

В СЗИ от НСД «Блокхост-Сеть 4» существует возможность входа пользователей в ОС по паролю без предъявления токена.

Если администратор безопасности предоставил пользователю возможность входа в ОС без предъявления токена, то для входа пользователя в ОС необходимо ввести пароль учетной записи пользователя (рисунок 3.8).

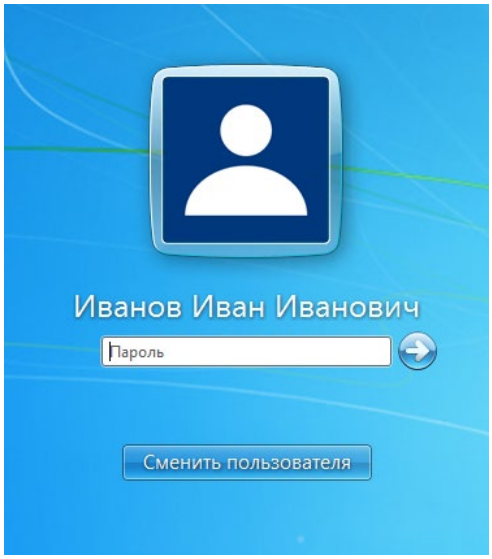


Рисунок 3.8 – Вход пользователя без токена

3.3.1 Ошибочные ситуации при аутентификации пользователя по паролю

Введен неверный пароль. **Пароль изменен администратором безопасности**	При вводе неверного пароля или в случае изменения пароля администратором безопасности появится сообщение об ошибке. После нажатия кнопки *OK*, произойдет возврат к окну аутентификации пользователя. Необходимо повторно ввести пароль пользователя. В случае неудачной попытки ввода пароля необходимо обратится к администратору безопасности.	

3.4 Перевыпуск токена пользователю

В ряде ошибочных ситуаций при аутентификации пользователя, при которых невозможен вход пользователя в ОС, требуется перевыпуск токена пользователю администратором безопасности.

При перевыпуске токена пользователю для входа по сертификату и для безопасного входа по паролю потребуется ввод PIN-кода пользователя на клиентской рабочей станции (рисунок 3.9).

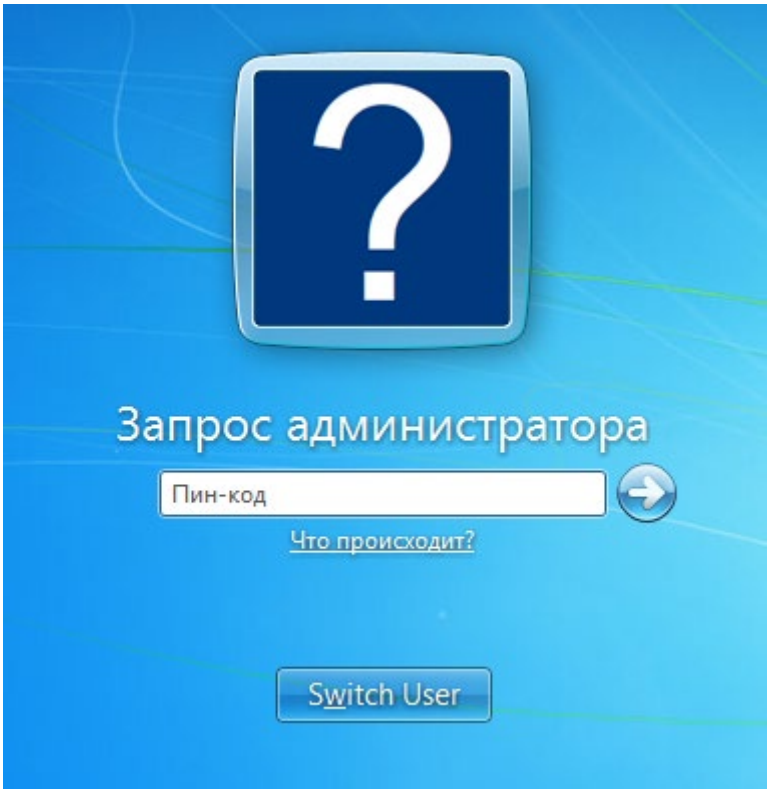


Рисунок 3.9 – Запрос PIN-кода пользователя администратором

В случае успешного ввода PIN-кода, пользователю будет перевыпущен токен для входа по сертификату или для безопасного входа по паролю.

4 Виды аутентификации при входе в ОС Linux

При загрузке предусмотрены следующие виды входа пользователя в систему:

– вход по токену с записанным паролем (БВПП);
  - по PIN-коду со сменой пароля (вход с использованием назначенного токена и вводом PIN-кода токена вместо пароля, при первом входе после ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен);
  - по PIN-коду без смены пароля (вход с использованием назначенного токена и вводом PIN-кода токена вместо пароля, при первом входе после ввода PIN-кода, пароль пользователя будет сохранен на токен без изменений);
  - по паролю без PIN-кода (вход пользователя с использованием назначенного токена и вводом пароля пользователя);
– вход по токену с сертификатом;
– вход пользователя без предъявления токена:
  - по паролю (происходит проверка введенного пароля с паролем пользователя, хранящимся в БД СЗИ);
  - аутентификация ОС.

При входе пользователя в ОС семейств Linux необходимо учитывать, если имя доменного и локального пользователя совпадают и при входе вводится только имя пользователя без домена (например, ***user1***), то вход будет осуществлён для локального пользователя. Для входа доменным пользователем необходимо ввести имя пользователя с указанием домена (например, ***user1@pki.local***).

При входе пользователя в ОС семейства Linux действует следующая очередность проверок предъявляемых пользователем средств аутентификации:

1) При предъявлении пользователем токена, в первую очередь выполняется проверка на наличие на устройстве сертификата для входа:

   если сертификат для входа присутствует на токене (вне зависимости от истечения срока действия сертификата, наличия возможности безопасного входа по паролю), будет осуществлена попытка входа по сертификату.

2) При отсутствии на предъявляемом токене сертификата для входа, выполняется проверка на наличие на устройстве возможности безопасного входа по паролю:

   если безопасный вход по паролю возможен для пользователя, будет осуществлена попытка входа по паролю на токене.

3) В случае невозможности входа по сертификату и по паролю на токене, пользователь может воспользоваться входом по паролю без предъявления токена, при этом предъявляемое для входа устройство необходимо извлечь (рисунок 4.1).

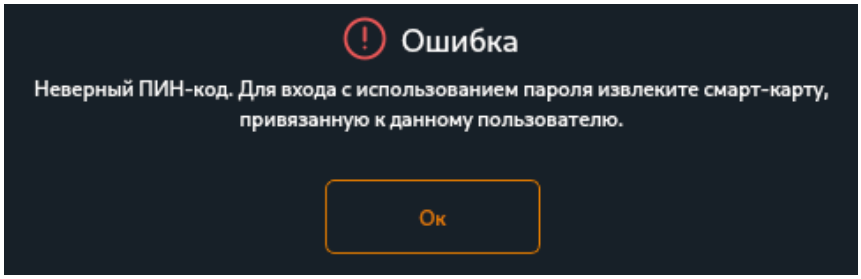


Рисунок 4.1 – Ошибка при попытке входа с предъявлением смарт-карты

Назначение токена пользователю с возможностью записи на него сертификата для входа или используемого для записи сгенерированного пароля, осуществляется администратором безопасности с помощью консоли управления.

Описание приведено в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами».

4.1 Безопасный вход по паролю на токене

При использовании двухфакторной аутентификации СЗИ от НСД «Блокхост-Сеть 4» вход пользователя в систему и дальнейшая загрузка ОС без предъявления токена невозможны.

Аутентификация с использованием БВПП возможна:

1) По PIN-коду со сменой пароля.

Для перехода на аутентификацию с использованием токена с БВПП со сменой пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

2) По PIN-коду без смены пароля.

Для перехода на аутентификацию с использованием токена с БВПП без смены пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо

пароля. Пароль будет считан и предъявлен автоматически.

3) По паролю без PIN-кода.

Вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом пароля пользователя. PIN-код токена вводить не требуется.

Для аутентификации по паролю на токене необходимо подключить токен и заполнить поля:

– ***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 учетной записи пользователя (только при первом входе), или вводится PIN-код доступа к токену (при последующих входах).

При входе в систему с использованием аутентификации по паролю на токене, реакция СЗИ от НСД «Блокхост-Сеть 4» зависит от информации о пароле, записанной на токене.

Возможны следующие варианты:

– на токене нет пароля (первый вход для записи пароля на токен);

– токен содержит актуальный пароль;

4.1.1 Первый вход пользователя с использованием пароля на токене

При первом входе пользователя с использованием аутентификации по паролю на токене, СЗИ от НСД «Блокхост-Сеть 4» потребует ввод пароля учетной записи пользователя (рисунок 4.2).

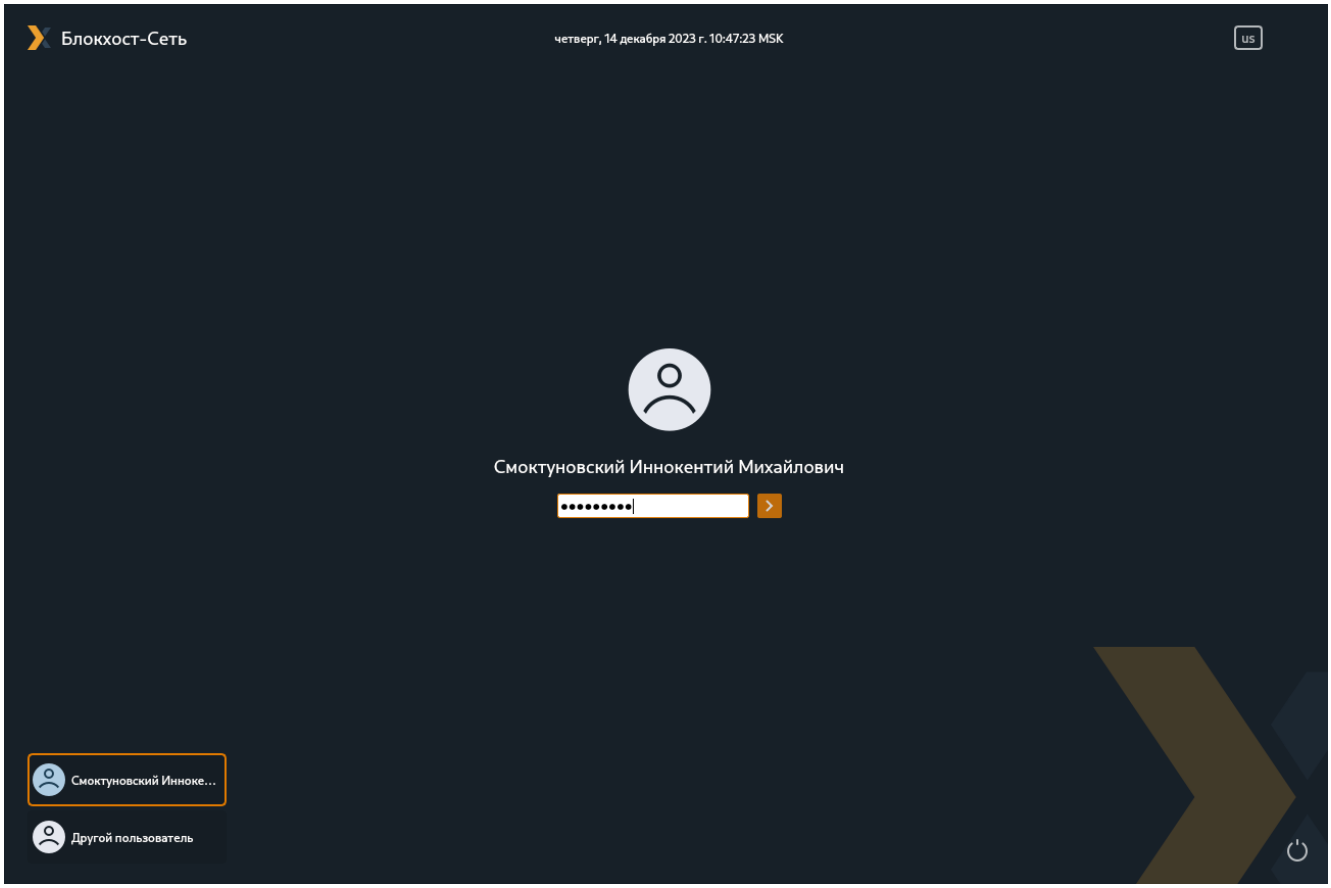


Рисунок 4.2 – Аутентификация по паролю на токене

После ввода пароля появится сообщение о необходимости перехода на двухфакторную аутентификацию (рисунок 4.3).

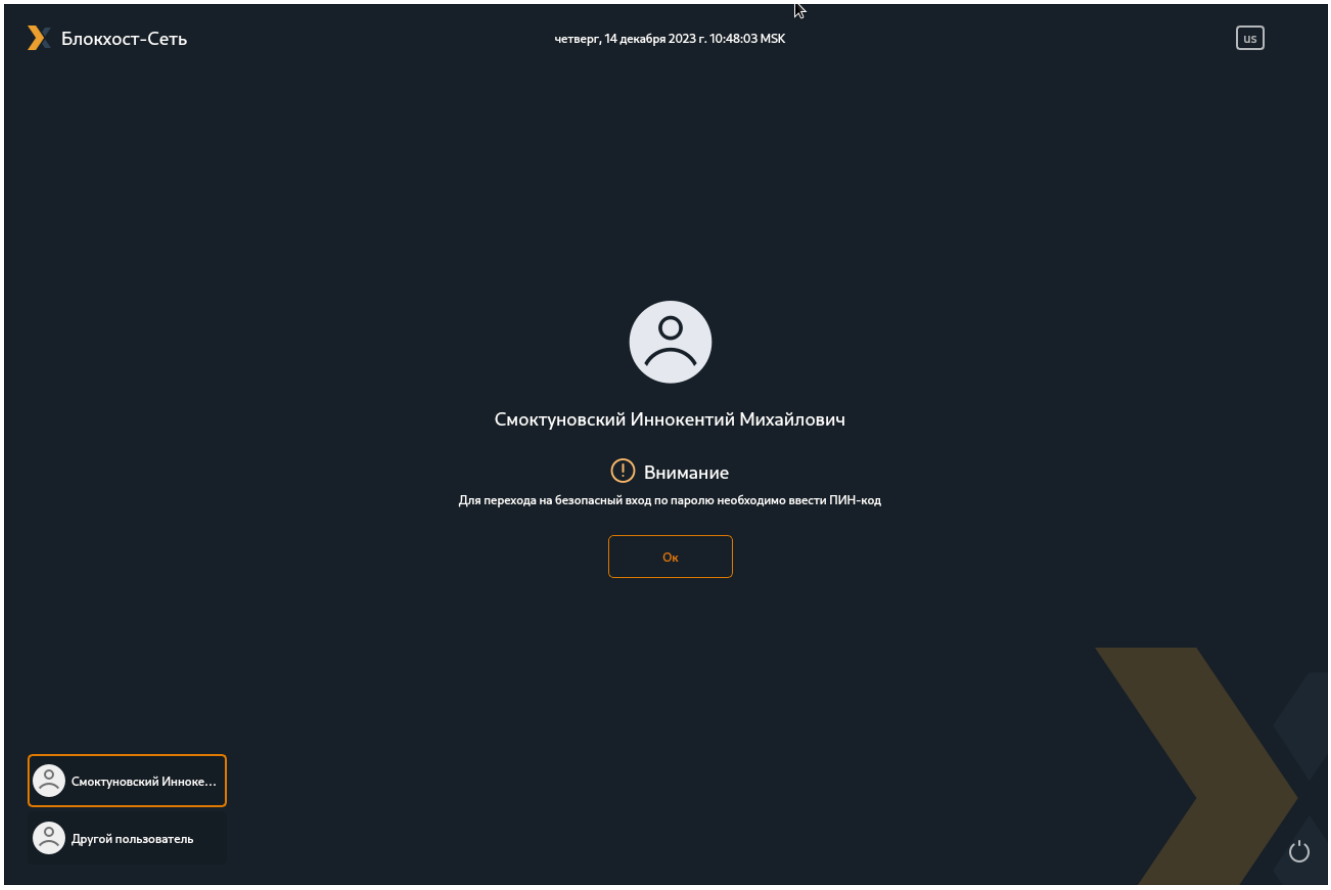


Рисунок 4.3 – Сообщение о необходимости перехода на двухфакторную аутентификацию

После нажатия кнопки ***Да*** появится окно ввода PIN-кода к токену (рисунок 4.4).

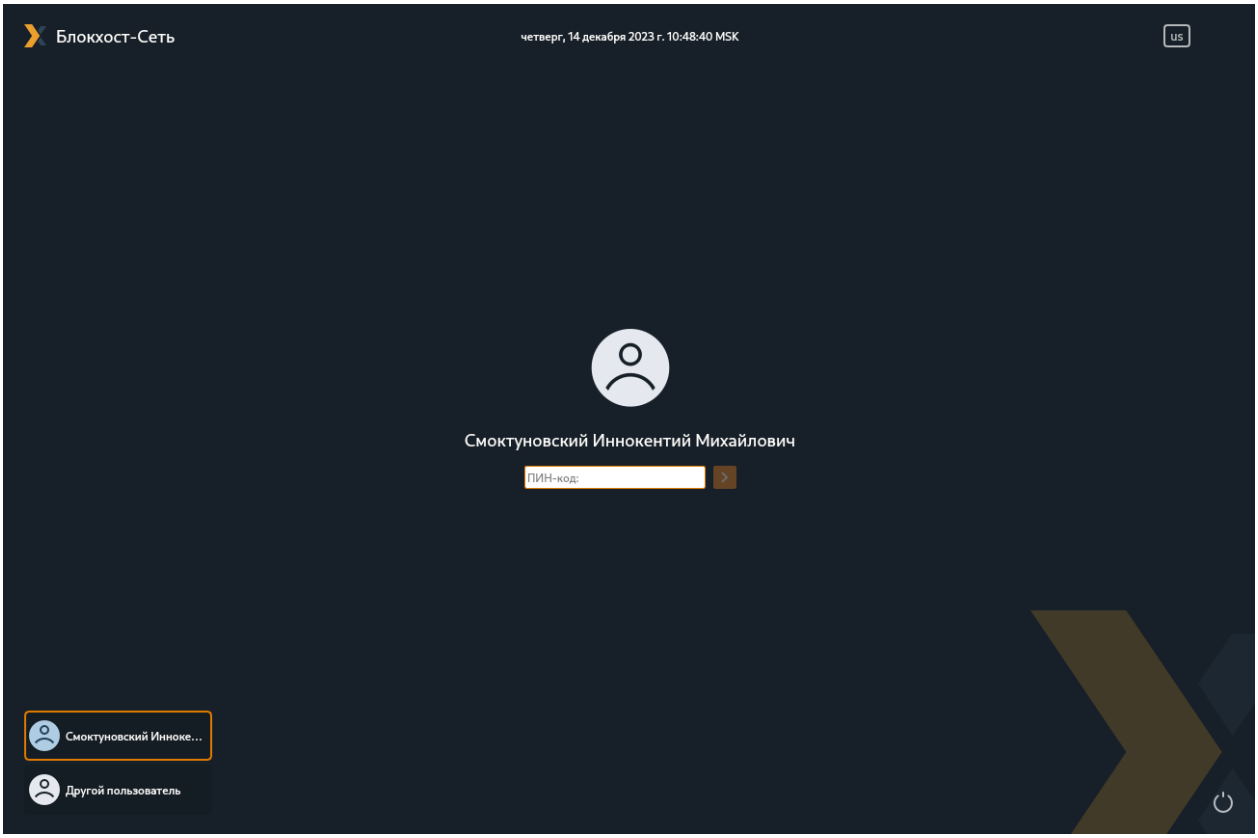


Рисунок 4.4 – Ввод ПИН-кода токена

После ввода PIN-кода генерируется пароль пользователя и записывается на токен.

Если администратором безопасности при назначении токена пользователю установлена принудительная смена PIN-кода пользователя при первом входе пользователя по токену, появится сообщение о необходимости сменить PIN-код токена (рисунок 4.5).

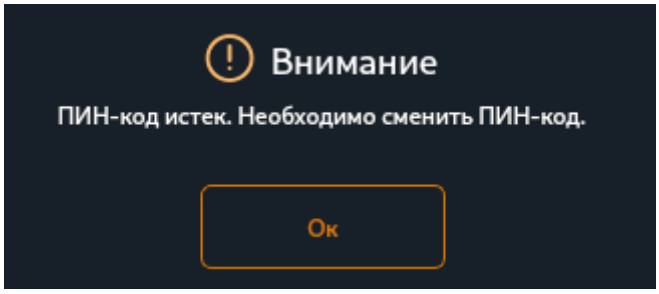


Рисунок 4.5 – Необходимость смены PIN-кода токена

После нажатия кнопки ***ОК*** появится окно для ввода нового значение PIN-кода пользователя (рисунки 4.6, 4.7).

Рисунок 4.6 – Ввод нового PIN-кода токена

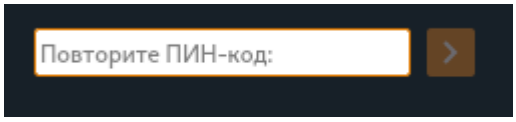


Рисунок 4.7 – Подтверждение нового PIN-кода токена

Дальнейший вход пользователя в систему возможен только с использованием измененного PIN-кода.

4.1.2 Аутентификация пользователя по актуальному паролю на токене

Если пароль на токене актуальный, то после ввода PIN-кода токена и успешной проверки прав пользователя на вход в систему, продолжится загрузка ОС.

Окно приглашения на вход при аутентификации пользователя по актуальному паролю на токене приведено на рисунке 4.8.

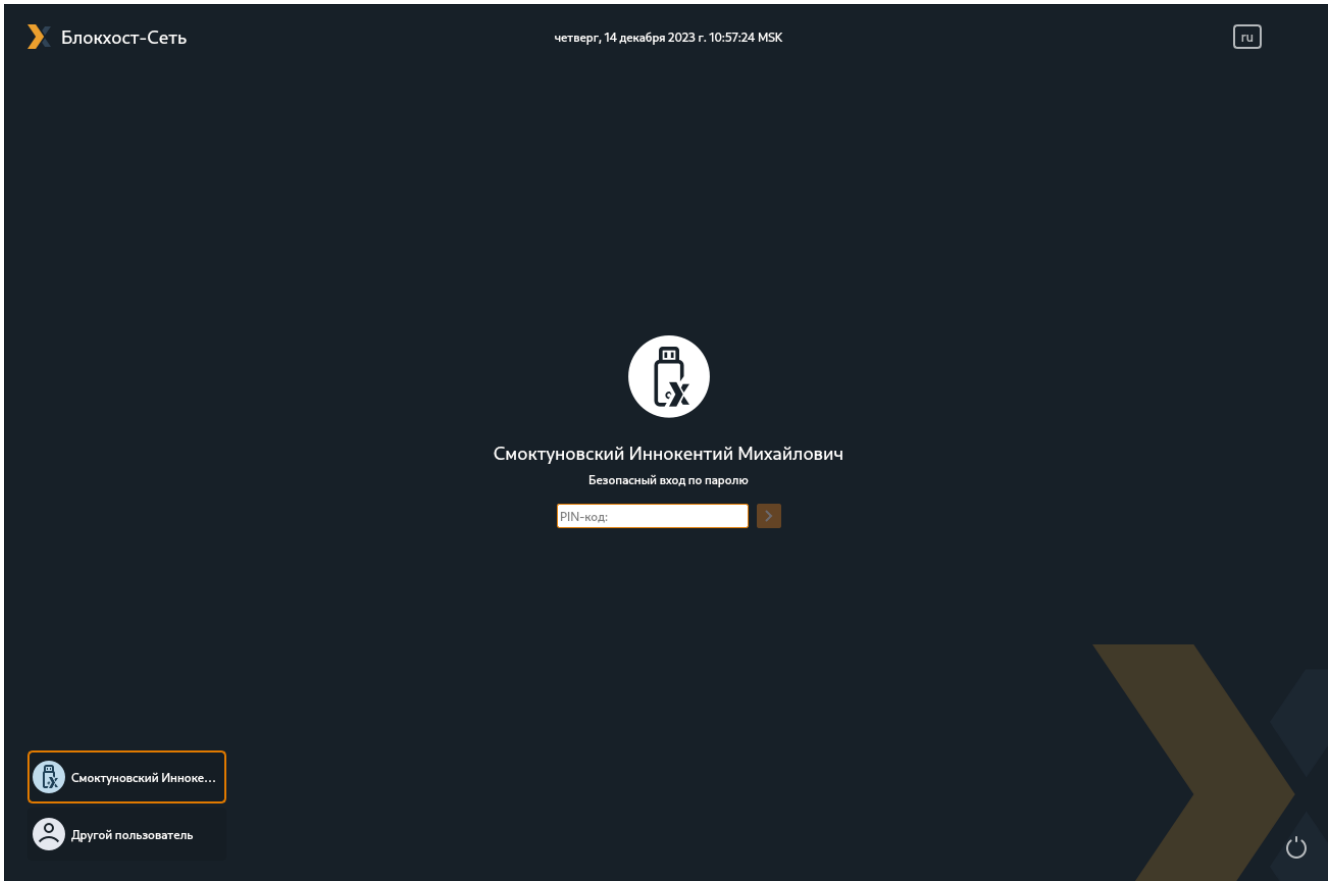
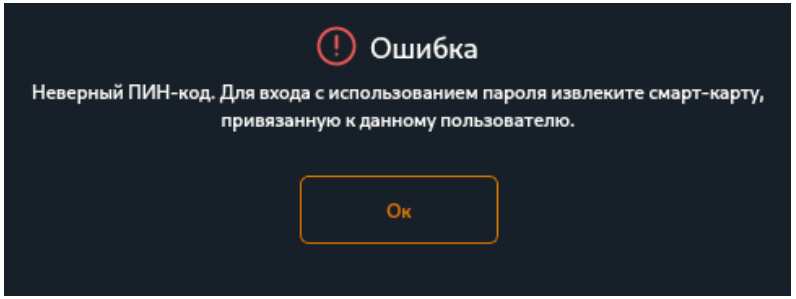
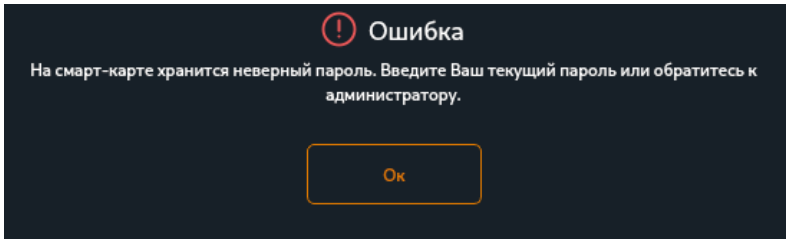
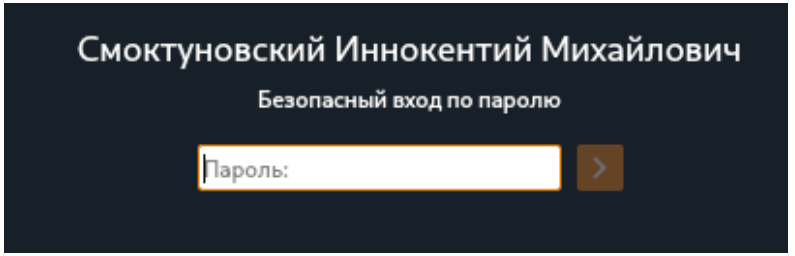
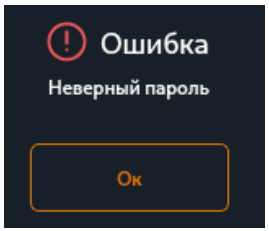
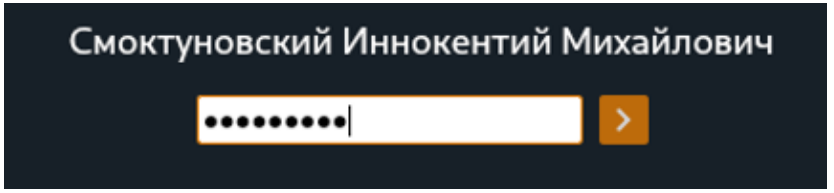
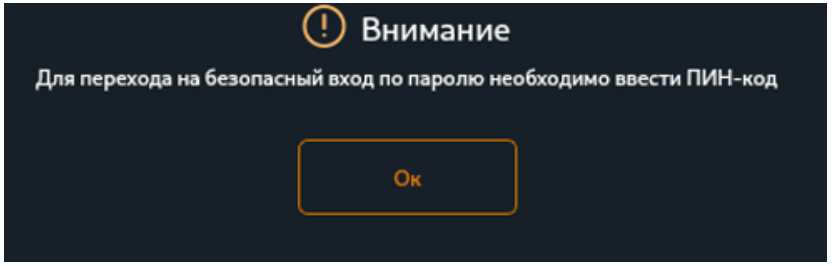
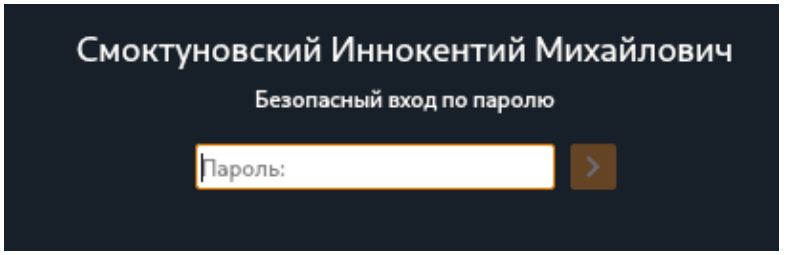
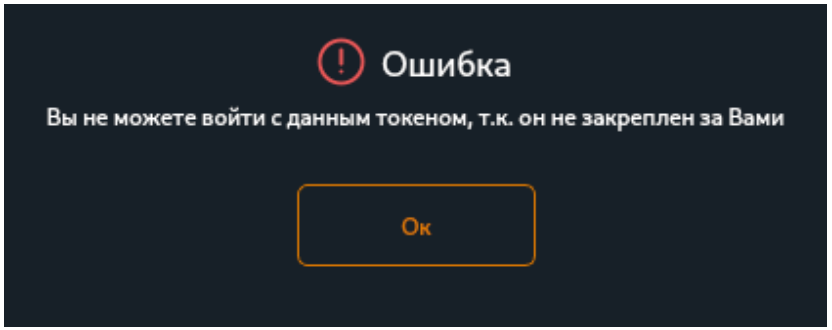
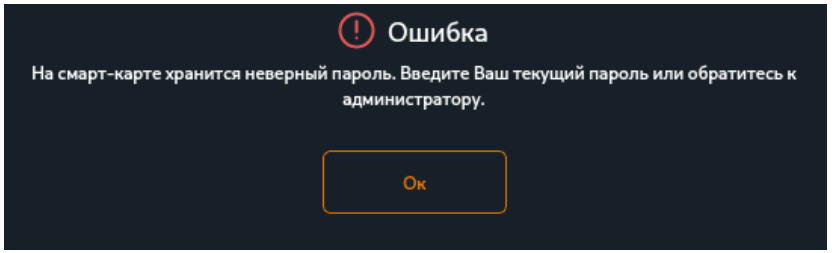


Рисунок 4.8 – Ввод PIN-кода токена

4.1.3 Ошибочные ситуации при аутентификации пользователя по паролю на токене

Введен неверный PIN-код	При вводе неверного PIN-кода появится сообщение об ошибке. После нажатия кнопки *Да*, произойдет возврат к окну аутентификации пользователя для повторного ввода PIN-кода.	
Пароль не совпадает с имеющемся на токене	При входе пользователя с паролем на токене возможны ситуации, когда токен содержит другой пароль, не совпадающий с паролем пользователя (например, пароль пользователя был изменен администратором безопасности).	
	После ознакомления с сообщением и нажатием кнопки *Да* произойдет возврат в диалоговое окно ввода аутентификационной информации пользователя, в котором необходимо ввести актуальный пароль учетной записи пользователя, выданный администратором. После ввода пароля, сгенерируется новый пароль пользователя и запишется на токен.	

Пароль на токене отсутствует	При случайном или намеренном удалении сторонними средствами пароля пользователя с токена, пользователь не сможет войти в систему с использованием токена. Необходимо обратиться к администратору для сброса пароля пользователя и войти с использованием нового пароля, выданным администратором. После ввода пароля, появится сообщение о переходе на двухфакторную аутентификацию. Дальнейшие действия аналогичны описанным в разделе ***Первый вход пользователя по паролю на токене.***	   
С токена, назначенного пользователю, удалена вся информация	При случайном или намеренном удалении сторонними средствами всей информации с токена, пользователь не сможет войти в систему с использованием токена. После сброса пароля администратором, и попытки входа	

(устройство отформатировано)	по новому паролю, появится сообщение о том, что на устройстве отсутствуют данные для входа. Необходимо обратиться к администратору для перевыпуска токена пользователю (раздел ***Перевыпуск токена пользователю***).	
Токен изъят администратором	При изъятии токена пользователя администратором, после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен не закреплен за пользователем. Необходимо обратиться к администратору для перевыпуска токена пользователю (раздел ***Перевыпуск токена пользователю***).	
Учетной записи пользователя доменными политиками запрещено менять пароль чаще заданного времени	При установке в доменных политиках запрета на смену пароля пользователя чаще заданного времени, при переходе на аутентификацию пользователя по паролю на токене, появится ошибка при смене пароля и пользователь будет переведен на аутентификацию по паролю на токене с текущим паролем. При этом при каждой последующей попытке аутентификации пользователя, будет производиться попытка записи пароля на токен до момента успешности данной операции.	

4.2 Аутентификация по сертификату на токене

В СЗИ от НСД «Блокхост-Сеть 4» реализована возможность двухфакторной аутентификации пользователей с использованием цифровых сертификатов.

Для аутентификации по сертификату необходимо подключить токен, содержащий сертификат пользователя. В окне приглашения на вход необходимо ввести PIN-код токена. Остальные данные пользователя будут автоматически считаны с токена (рисунок 4.9).

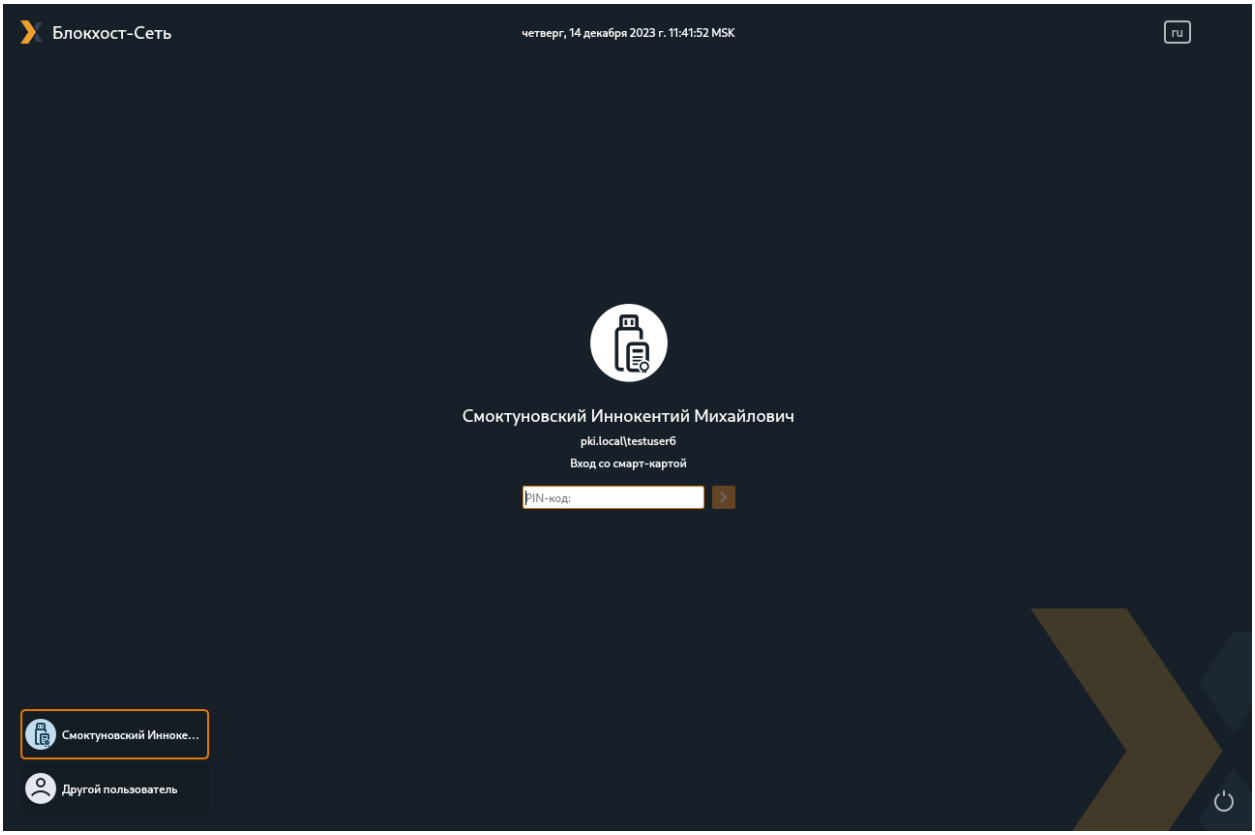


Рисунок 4.9 – Аутентификация пользователя по сертификату

Поддерживается также аутентификация пользователя, когда на токене содержится несколько сертификатов для одного и того же пользователя или для разных пользователей. В этом случае все сертификаты будут отображены в левом нижнем углу окна входа (рисунок 4.10).

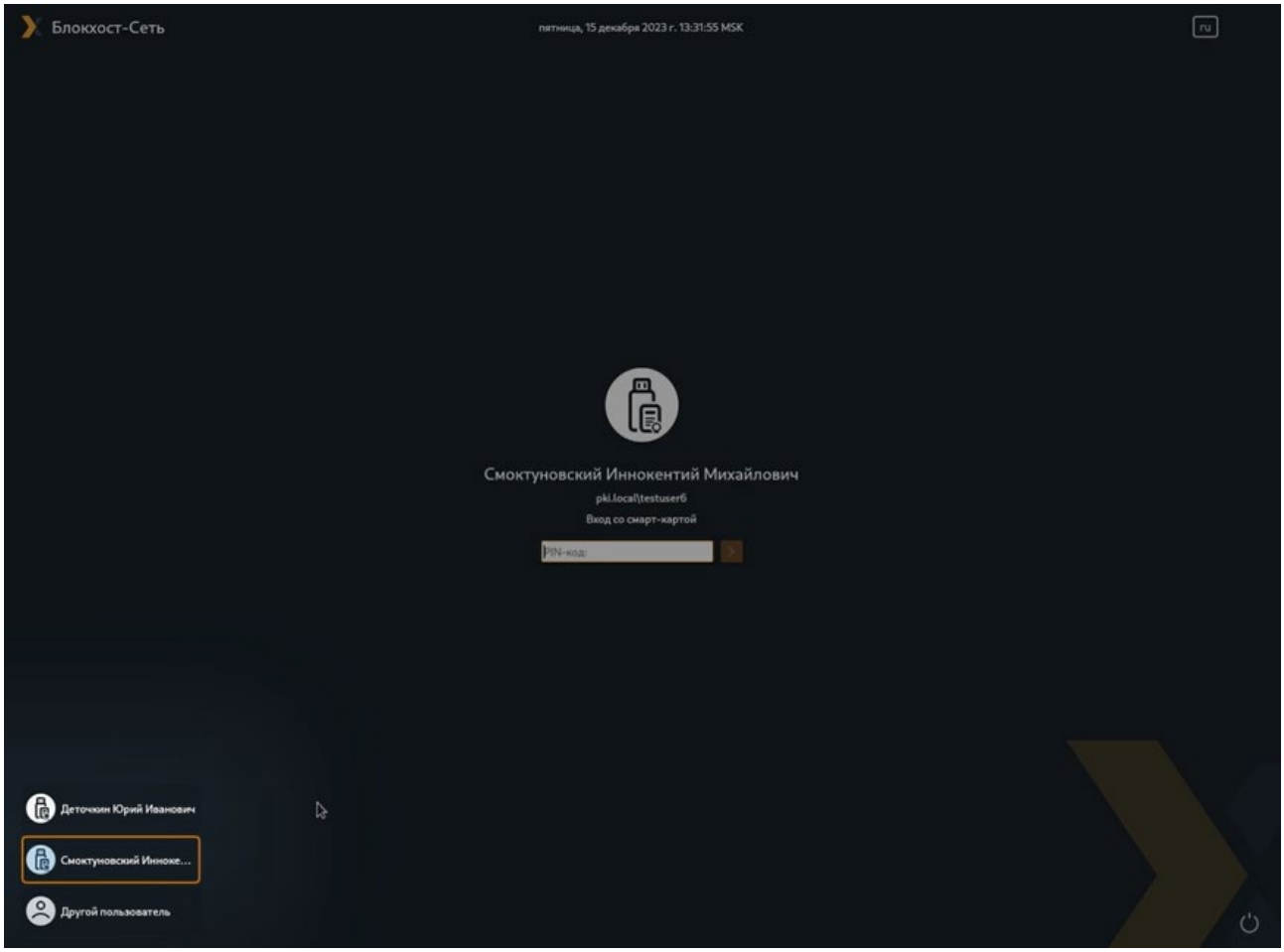
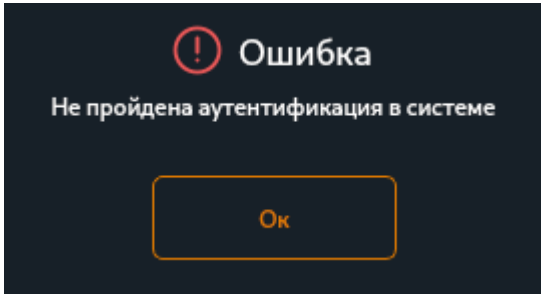
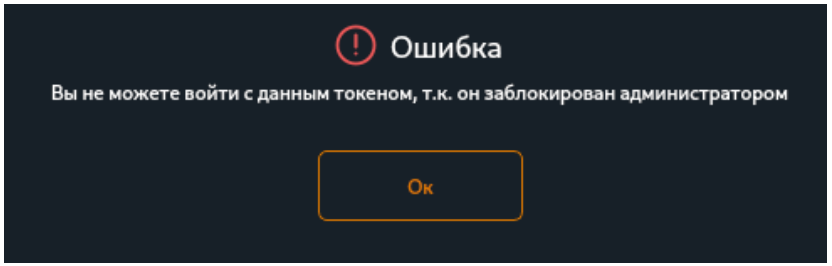
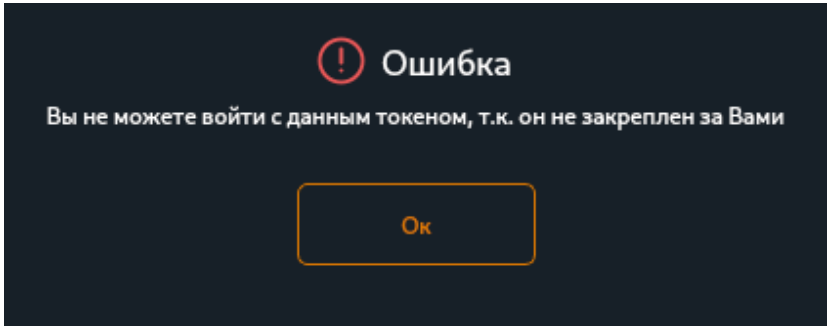
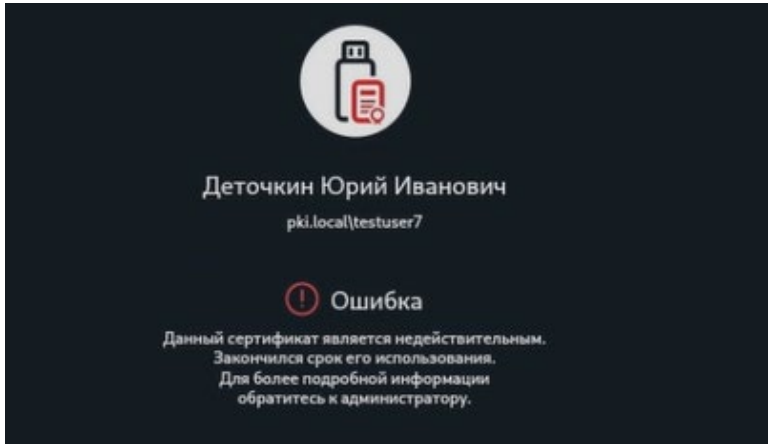


Рисунок 4.10 – Отображение нескольких сертификатов на токене

4.2.1 Ошибочные ситуации при аутентификации пользователя по сертификату на токене

Введен неверный PIN-код	При вводе неверного PIN-кода появится сообщение об ошибке. После нажатия кнопки *OK*, произойдет возврат к окну аутентификации пользователя для повторного ввода PIN-кода.	
Токен временно выключен или отозван администратором,	При временном выключении или отзыве токена пользователя администратором после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен заблокирован администратором. Необходимо обратиться к администратору для включения токена или перевыпуска токена в случае отзыва (раздел ***Перевыпуск токена пользователю***)	
Токен изъят администратором	При изъятии токена пользователя администратором, после успешного ввода PIN-кода токена в окне аутентификации, появится сообщение о том, что токен не закреплен за пользователем. Необходимо обратиться к администратору для перевыпуска токена пользователю (раздел ***Перевыпуск токена пользователю***).	

Сертификат на токене истек	При истечении срока действия сертификата на токене, появится сообщение о том, что срок действия сертификата закончился. Необходимо обратиться к администратору.	

4.3 Вход без токена

В СЗИ от НСД «Блокхост-Сеть 4» существует возможность входа пользователей в ОС по паролю без предъявления токена.

Если администратор безопасности предоставил пользователю возможность входа в ОС без предъявления токена, то для входа пользователя в ОС необходимо ввести пароль учетной записи пользователя (рисунок 4.11).

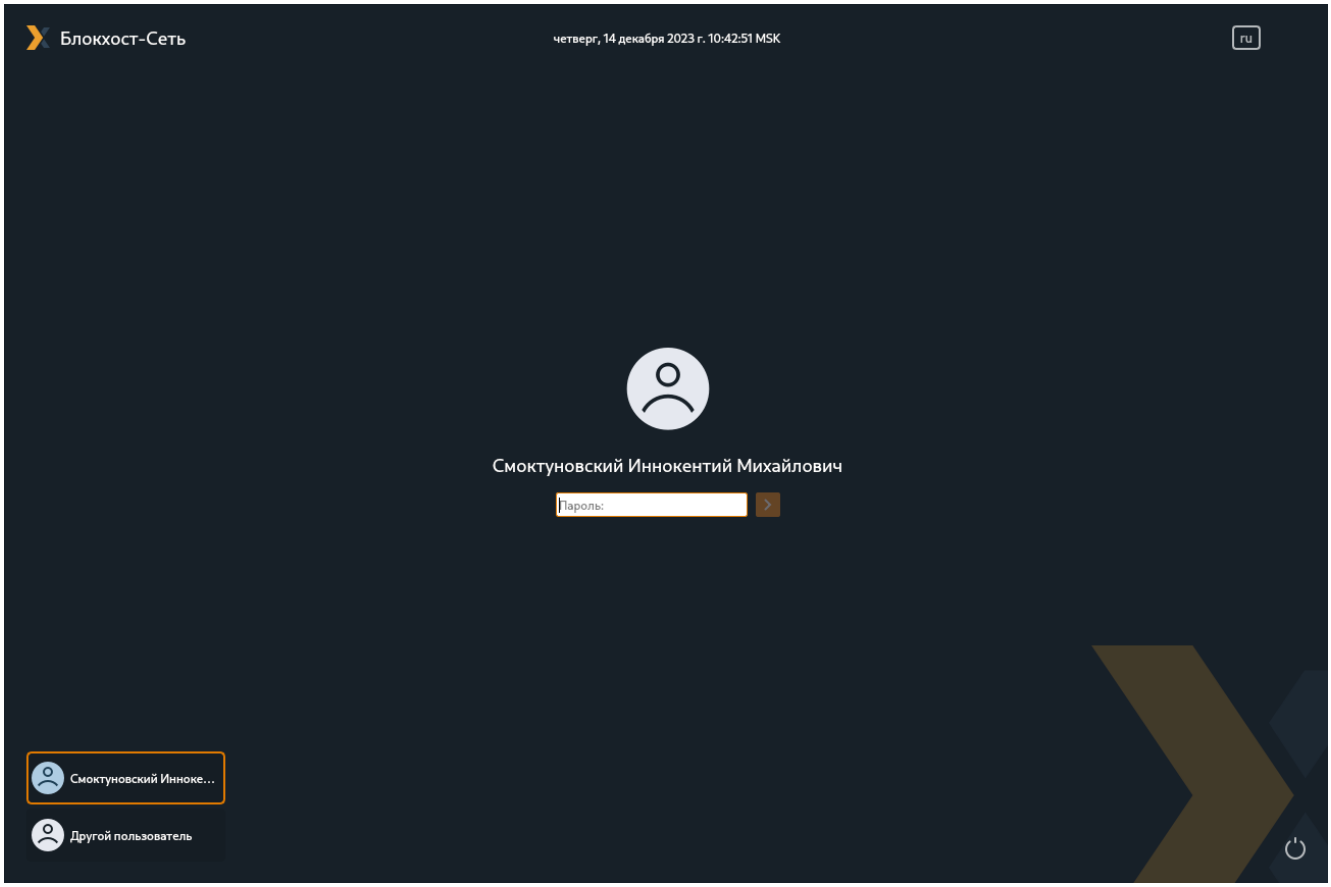
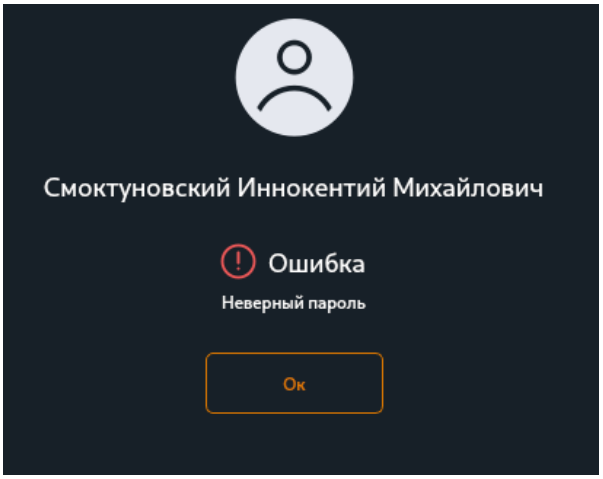


Рисунок 4.11 – Вход пользователя без токена

4.3.1 Ошибочные ситуации при аутентификации пользователя по паролю

Введен неверный пароль. **Пароль изменен администратором безопасности**	При вводе неверного пароля или в случае изменения пароля администратором безопасности появится сообщение об ошибке. После нажатия кнопки *OK*, произойдет возврат к окну аутентификации пользователя. Необходимо повторно ввести пароль пользователя. В случае неудачной попытки ввода пароля необходимо обратится к администратору безопасности.	

4.4 Перевыпуск токена пользователю

В ряде ошибочных ситуаций при аутентификации пользователя, при которых невозможен вход пользователя в ОС, требуется перевыпуск токена пользователю администратором безопасности.

При перевыпуске токена пользователю для входа по сертификату и для безопасного входа по паролю потребуется ввод PIN-кода пользователя на клиентской рабочей станции (рисунок 4.12).

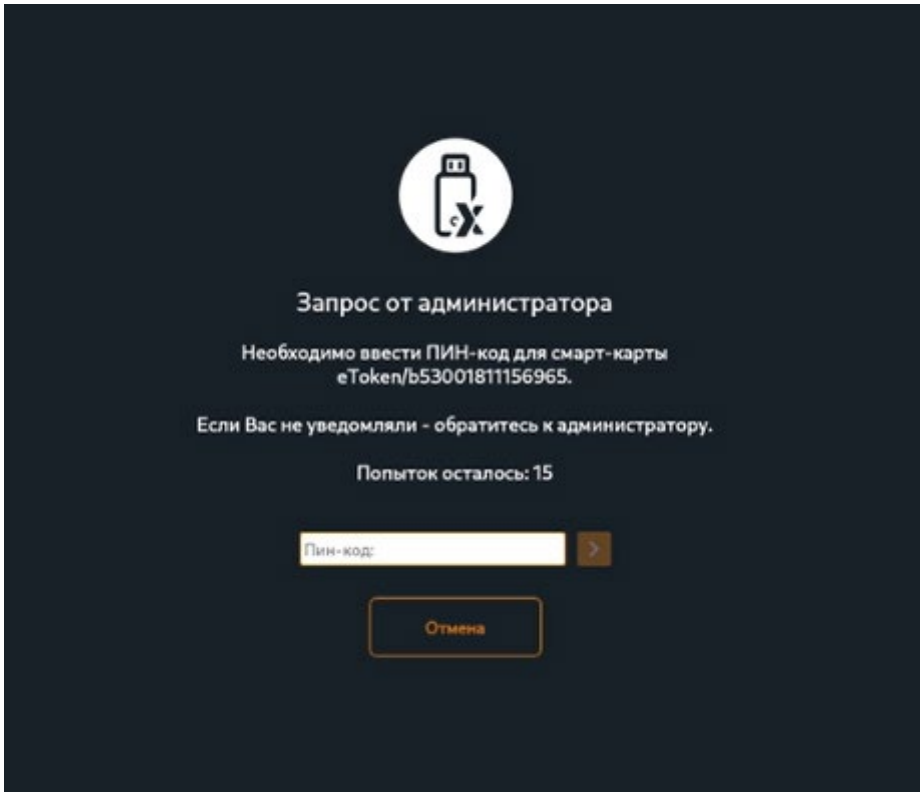


Рисунок 4.12 – Запрос PIN-кода пользователя администратором

В случае успешного ввода PIN-кода, пользователю будет перевыпущен токен для входа по сертификату или для безопасного входа по паролю.

4.5 Разблокировка сессии пользователя

Разблокировка сеанса пользователя приведена на примере ОС Astra Linux.

При разблокировке сеанса доступа в ОС Linux после времени бездействия (неактивности) пользователя недоступен вывод дополнительных сообщений о возникновении ошибок при аутентификации пользователя (п. 4.1.3).

В данном случае, при невозможности входа пользователя в систему (рисунок 4.13), необходимо для разблокировки сеанса обратиться к администратору для настройки разрешения входа пользователя без предъявления токена «Аутентификация ОС», при этом токен нужно предварительно извлечь и войти с использованием пароля, предоставленного администратором.

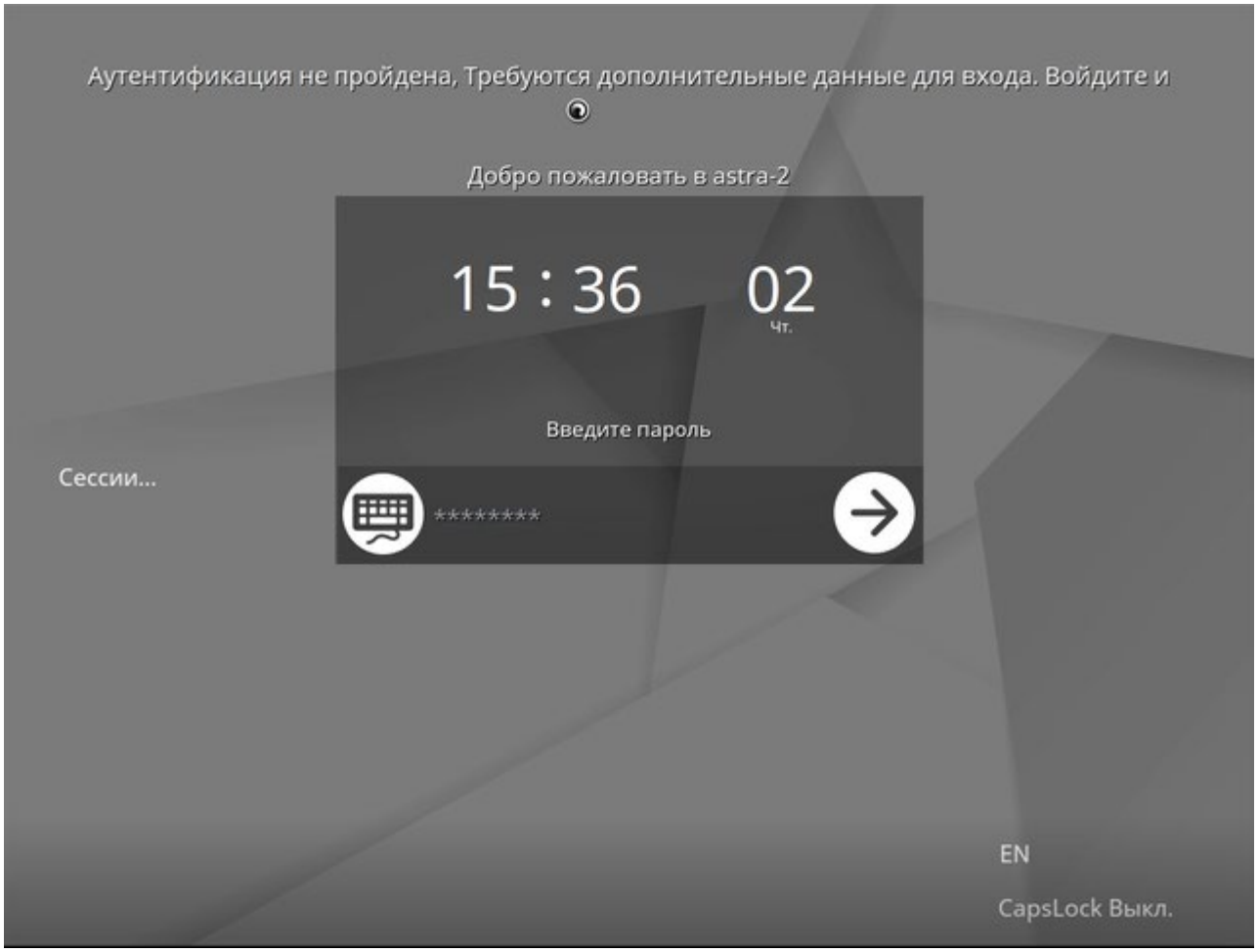


Рисунок 4.13 – Разблокировка сеанса

5 Копирование пароля с токена

При установке клиента Блокхост-Сеть на рабочую станцию, на панели задач появится иконка , позволяющая выполнять копирование пароля с токена, выпущенного для безопасного входа по паролю через подсистему управления токенами.

Для запуска процесса копирования пароля с токена необходимо нажать на иконку и выбрать ***Скопировать пароль с токена*** (рисунок 5.1).

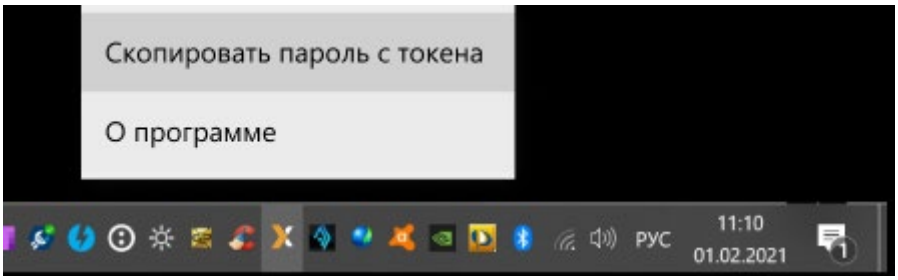


Рисунок 5.1 – Копирование пароля с токена

Появится окно для ввода PIN-кода токена, с которого пользователь вошел в ОС:

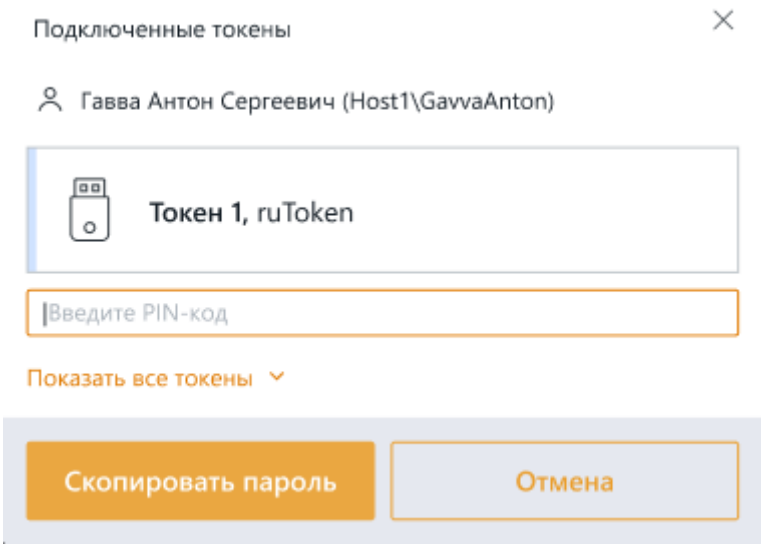


Рисунок 5.2 – Доступные пользователю токены

После ввода PIN-кода появится окно с информацией об успешном копировании пароля (рисунок 5.3).

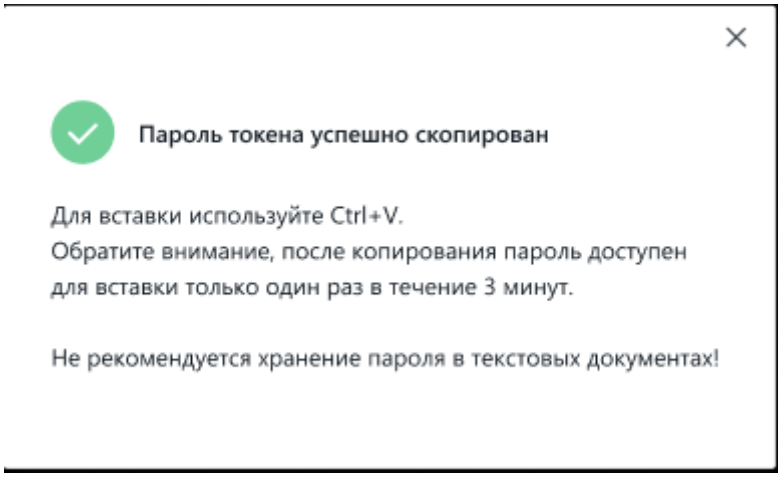


Рисунок 5.3 – Успешное копирование пароля с токена

Обратите внимание:
- копирование выполняется в защищенный буфер обмена Блокхост-Сеть;
- для вставки пароля используется комбинация клавиш ***Ctrl + V***;
- скопированный пароль доступен для вставки только один раз;
- вставка доступна в течении 3 минут.

5.1 Копирование пароля с токена в ОС Linux

Процедура копирования пароля с токена, выпущенного для безопасного входа по паролю через подсистему управления токенами, не отличается от аналогичной операции в ОС Windows (см. раздел ***Копирование пароля с токена***).

Запуск процедуры копирования пароля с токена доступен по иконке  на панели задач (рисунок 5.1).

После ввода PIN-кода появится окно с информацией об успешном копировании пароля (рисунок 5.3).

Обратите внимание:
- копирование выполняется в общий буфер обмена;
- для вставки пароля используется любая комбинация клавиш ***Ctrl + V***, ***Shift + Insert*** или пункт контекстного меню ***Вставить***;
- скопированный пароль доступен для вставки только один раз;
- вставка доступна в течении 3 минут.

6 Работа в условиях ограничения доступа к ресурсам

6.1 Механизмы разграничения доступа

СЗИ от НСД «Блокхост-Сеть 4» реализует дискреционный механизм и мандатное разграничение доступа пользователей к локальным и сетевым ресурсам компьютера. Эти механизмы позволяют обеспечить надежную защиту ресурсов от несанкционированного доступа и организовать эффективную работу пользователей в защищенной информационной среде.

6.1.1 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 от НСД «Блокхост-Сеть 4» 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.

6.1.2 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 от НСД «Блокхост-Сеть 4» 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.

6.2 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.

Перечень сокращений

PIN	–	Personal Identification Number (личный идентификационный номер)
БВПП	–	Безопасный вход по паролю
БД	–	База данных
ГУПТ	–	Гарантированное удаление по требованию
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
СЗИ	–	Средство защиты информации
СКЗИ	–	Средство криптографической защиты информации
СУБД	–	Система управления базами данных