Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0» (серверная консоль)

Руководство администратора безопасности

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-сеть 2.0» (далее по тексту – СЗИ «Блокхост-сеть 2.0» или СЗИ).

Структурно СЗИ «Блокхост-сеть 2.0» состоит из клиентской части СЗИ «Блокхост-сеть 2.0», в рамках которой реализованы базовые механизмы защиты, и серверной части – сервера безопасности, устанавливаемой на автоматизированное рабочее место (АРМ) администратора безопасности.

Клиентская часть обеспечивает защиту рабочей станции от НСД к информации, и может работать как на автономной рабочей станции, так и на рабочей станции в составе сети. Через серверную часть выполняется централизованное управление удаленными рабочими станциями. Настройка клиентской части может быть выполнена через локальную или серверную консоль администрирования СЗИ «Блокхост-сеть 2.0», настройка серверной части выполняется через серверную консоль.

Локальная консоль администрирования позволяет выполнять настройку СЗИ «Блокхост-сеть 2.0» непосредственно на рабочей станции. Серверная консоль предназначена для настройки тех же механизмов на удаленных рабочих станциях с рабочего места администратора безопасности.

В состав СЗИ «Блокхост-сеть 2.0» также входят дополнительные компоненты, реализованные в виде отдельных программных приложений:

- *модуль контроля целостности реестра* (автономный и сетевой варианты). Автономный вариант модуля устанавливается на защищаемые рабочие станции в составе ЛВС или работающие автономно, сетевой вариант – на АРМ администратора безопасности. Подробное описание модуля контроля целостности реестра приведено в документе «СЗИ «Блокхост-сеть 2.0. Контроль целостности реестра. Руководство администратора безопасности».
- *агент системы развертывания СЗИ «Блокхост-сеть 2.0»*. Устанавливается на защищаемые рабочие станции в составе ЛВС и позволяет удаленно устанавливать клиентские части СЗИ с АРМ администратора безопасности.

Руководство состоит из 8 глав и трех приложений:

- глава 1 описывает принципы назначение, состав и задачи, решаемые с помощью СЗИ «Блокхост-сеть 2.0»;
- в главе 2 приведены требования к программной и аппаратной составляющей рабочей станции для работы СЗИ «Блокхост-сеть 2.0»;
- в главе 3 описаны основные сведения по работе с интерфейсом СЗИ «Блокхост-сеть 2.0», а также – порядок формирования группы контролируемых рабочих станций и установка клиентской части СЗИ из серверной консоли администрирования СЗИ «Блокхост-сеть 2.0»;
- главы 4-7 содержат порядок настройки механизмов защиты информации, реализованных в СЗИ «Блокхост-сеть 2.0»;
- в главе 8 приведено описание механизма оперативного контроля событий, влияющих на безопасность информации;

- в Приложении 1 приведено описание возможностей СЗИ «Блокхост-сеть 2.0» по сбору диагностической информации по выявлению проблем функционирования СЗИ;
- в Приложении 2 приведено описание настройки центра сертификации в ОС Windows 2008R2 для организации работы входа пользователей в операционную систему по сертификатам;
- в Приложении 3 приведено описание проверок при проведении регламентного тестирования СЗИ «Блокхост-сеть 2.0»

Знаки, расположенные на полях руководства, указывают на примечания. Степени важности примечаний:

 Важная информация, информация предостерегающего характера.

 Дополнительная информация, примеры.

1. Назначение, задачи и состав СЗИ «Блокхост-сеть 2.0»

1.1. Назначение СЗИ «Блокхост-сеть 2.0»

Средство защиты информации «Блокхост-сеть 2.0» является программно-техническим средством защиты информации от несанкционированного доступа к информации, и предназначено 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 Microsoft Windows 2008R2/Vista/7/8/8.1/2012/2012R2.

Реализованные в СЗИ «Блокхост-сеть 2.0» механизмы защиты информации позволяют администратору безопасности решать следующие задачи:

- усиление защиты от несанкционированного доступа в систему;
- разграничение доступа пользователей к ресурсам;
- обеспечение гарантированного удаления информации;
- разграничение доступа к запуску программ;
- контроль целостности объектов файловой системы;
- контроль целостности реестра;
- очистка памяти после завершения работы приложений;
- контроль вывода информации на печать, маркировка документов;
- разграничение доступа пользователей к администрированию СЗИ;
- просмотр информационных сообщений СЗИ в ходе работы;
- контроль событий, связанных с безопасностью защищаемой информации.

Для обеспечения безопасности защищаемой информации администратор безопасности обязан:

- осуществить настройку СЗИ «Блокхост-сеть 2.0». Настройка осуществляется в соответствии с данным руководством и заключается в определении пользователей, которым надлежит обеспечить доступ к защищаемому средству вычислительной техники, и формировании для них политик безопасности на основе реализованных механизмов разграничения доступа и защиты информации;
- выполнять аудит информационной безопасности компьютера. Ведение оперативного контроля событий необходимо для выявления ошибок в настройках и корректировки правил разграничения доступа, а также для своевременного реагирования на осуществление несанкционированного доступа к защищаемой информации.

1.2. Локальная и централизованная защита информации

СЗИ «Блокхост-сеть 2.0» обеспечивает защиту от несанкционированного доступа к информации, содержащейся на:

- автономном компьютере (без подключения к сети);

- сетевом компьютере (в одноранговой или доменной сети), как под управлением серверной части СЗИ «Блокхост-сеть 2.0», так и без таковой.

СЗИ «Блокхост-сеть 2.0» дополняет функциональные возможности операционной системы по защите информации. Таким образом, информация защищается от несанкционированного доступа следующими компонентами (рис. 1.1).

Рисунок 1.1. Компоненты защиты от несанкционированного доступа

1.3. Состав СЗИ «Блокхост-сеть 2.0»

СЗИ «Блокхост-сеть 2.0» включает в себя:

- **специализированный программный комплекс**, состоящий из клиентской и серверной частей СЗИ;
- **аппаратную часть** поддержки идентификации и аутентификации доступа пользователя в систему. Ключевыми носителями могут служить персональные идентификаторы типа eToken, SafeNet eToken, JaCarta, ESMART Token, Avest Token, ruToken, а также – USB-накопители и дискеты.

В качестве ключевого носителя также может быть использован персональный идентификатор пользователя, расположенный в защищённом хранилище реестра Windows (далее – персональный идентификатор в реестре).

Клиентская часть СЗИ «Блокхост-сеть 2.0» обеспечивает локальную защиту рабочей станции от НСД к информации. После установки СЗИ «Блокхост-сеть К» администратору безопасности доступны следующие механизмы защиты:

- дискреционный и мандатный механизмы контроля доступа к информационным ресурсам рабочей станции в соответствии с заданными параметрами контекста безопасности;
- контроль целостности программ и данных;
- аудит и регистрация доступа к информационным ресурсам;
- очистка памяти и гарантированное удаление информационных ресурсов;

- контроль вывода документов на печать, маркировка документов;
- защита ввода и вывода информации на отчуждаемые физические носители;
- контроль запуска процессов;
- контроль доступа к сетевым ресурсам;
- временное разграничение доступа пользователей к рабочей станции;
- администрирование СЗИ с использованием интерфейса администратора.

Серверная часть СЗИ «Блокхост-сеть 2.0» выполняет функции централизованного управления удаленными рабочими станциями:

- удаленное администрирование клиентской части СЗИ «Блокхост-сеть 2.0» на рабочих станциях (объединенных в одноранговую или доменную сеть);
- удаленное ведение оперативного контроля.

Входящий в состав серверной части мандатный сервер, на основе мандатного (полномочного) механизма, обеспечивает разграничение доступа пользователей к защищаемой информации, содержащейся на удаленных рабочих станциях.

Входящая в состав серверной части система развертывания позволяет выполнять удаленную установку клиентских частей СЗИ «Блокхост-сеть 2.0» на рабочие станции из серверной консоли администрирования СЗИ.

Аппаратные средства, функционирующие в составе СЗИ «Блокхост-сеть 2.0», позволяют:

- хранить персональные данные для идентификации и аутентификации;
- хранить ключевую информацию СЗИ «Блокхост-сеть 2.0».

Программные средства защиты информации (клиентская и серверная части СЗИ), функционирующие в составе СЗИ «Блокхост-сеть 2.0», позволяют:

- обеспечить более надежную защиту входа в систему с помощью аппаратных средств идентификации пользователя;
- разграничивать доступ пользователей к ресурсам с помощью дискреционного и мандатного механизмов разграничения доступа;
- ограничить вход пользователей в систему по времени и дням недели или до определенной даты;
- обеспечить контроль информационного обмена с отчуждаемыми физическими носителями информации;
- обеспечить гарантированное удаление информации;
- санкционировать запуск программ с помощью механизмов разграничения доступа к запуску процессов;
- осуществлять контроль целостности необходимой информации;
- обеспечить очистку памяти после завершения работы приложений;
- контролировать вывод информации на печать, осуществлять маркировку документов;
- осуществлять мониторинг активности пользователей в системе – работу СЗИ в «мягком режиме»;
- осуществлять групповое администрирование;

- разграничить доступ пользователей к сетевым ресурсам;
- санкционировать доступ пользователей к администрированию СЗИ «Блокхост-сеть 2.0»;
- выполнять контроль событий, связанных с безопасностью защищаемой информации.

1.4. Персональные идентификаторы

Реализованный в СЗИ «Блокхост-сеть 2.0» механизм двухфакторной аутентификации позволяет усилить защищенность входа рабочей станции за счет использования, помимо аутентификационных данных пользователя, персональных идентификаторов:

- eToken (USB-брелок или смарт-карта);
- SafeNet eToken (USB-брелок или смарт-карта);
- JaCarta (JaCarta PRO, JaCarta ГОСТ, JaCarta PKI);
- ruToken;
- ESMART Token (USB-брелок или смарт-карта);
- Avest Token (AvBign);
- USB-накопитель;
- Дискета 3,5”;
- персональный идентификатор в реестре Windows.

Персональные идентификаторы eToken, SafeNet eToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, AvBign, ESMART Token и ruToken представляют собой компактные устройства в виде USB-брелка (eToken, SafeNet eToken, JaCarta ГОСТ, JaCarta PKI, ESMART Token SC – также в виде смарт-карты) с защищенной энергонезависимой памятью и используются для хранения ключевой информации и паролей.

Персональный идентификатор в реестре представляет собой ключ в защищённом хранилище реестра Windows локальной рабочей станции и содержит информацию, идентичную информации для других типов ключевых носителей.

Доступ к любому ключевому носителю осуществляется по PIN-коду (по умолчанию PIN-код для ruToken – «12345678», для eToken и SafeNet eToken – «1234567890», для JaCarta – «1234567890», для ESMART Token – «12345678», для AvBign – «12345678»). Для eToken, SafeNet eToken, ruToken, JaCarta PRO, JaCarta ГОСТ, ESMART Token и JaCarta PKI PIN-код задается с помощью специального программного обеспечения, поставляемого с идентификатором (драйверы для SafeNet eToken, драйверы для eSmart Token и драйверы JaCarta для ОС Windows 8/8.1/2012/2012R2 не входят в комплект поставки СЗИ). Для USB-накопителя, дискеты и персонального идентификатора в реестре PIN-код задается средствами СЗИ «Блокхост-сеть 2.0».

Проверка PIN-кода при использовании eToken, SafeNet eToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, ESMART Token, Avest Token и ruToken осуществляется внутренними механизмами идентификаторов, а при использовании дискеты, USB- накопителя и персонального идентификатора в реестре – на основе контрольной суммы СЗИ «Блокхост-сеть 2.0».

1.5. Механизмы, предназначенные для решения задач защиты информации

1.5.1. Механизм идентификации и аутентификации

Механизм идентификации и аутентификации реализует следующие функции:

- идентификацию и аутентификацию пользователя при входе его в систему;
- сопоставление пользователя с персональным идентификатором;
- запись пароля на парольную дискету и считывание его с дискеты;
- блокирование и разблокирование системы;
- смену пароля пользователя.

Идентификация и аутентификация пользователя при входе в систему предназначена для защиты локального компьютера от загрузки операционной системы незарегистрированным пользователем. Данный механизм предполагает наличие у пользователя его уникального регистрационного имени, пароля, ключевого носителя и PIN-кода к нему. Идентификация и аутентификация осуществляются на последнем этапе загрузки операционной системы, поэтому невозможно загрузить операционную систему, не пройдя процедуры идентификации и аутентификации. Исключением является загрузка операционной системы в режиме «Защищенный режим с поддержкой командной строки», который доступен только администратору безопасности.

Для идентификации и аутентификации пользователя при его входе в систему реализованы два способа парольной защиты:

- при входе в систему пользователь вводит пароль с клавиатуры;
- при входе в систему пароль пользователя считывается с персонального идентификатора (пароль в зашифрованном виде записывается на ключевой носитель средствами СЗИ).

В СЗИ «Блокхост-сеть 2.0» предусмотрено ограничение на минимальную длину пароля – **восемь** символов.

При успешном доступе пользователя в систему его идентификационное имя используется для контроля всех последующих действий.

Дополнительно может быть ограничен доступ и нахождение пользователя в системе по дням недели и по времени – с точностью до часа.

Сопоставление пользователя с персональным идентификатором происходит в процессе входа пользователя в систему. Возможность записи пароля на ключевой носитель, смены пароля пользователя, а также возможность заблокировать систему осуществляется после входа пользователя в систему, путем нажатия сочетания клавиш **<Ctrl>+<Alt>+<Del>** и выбора соответствующего пункта меню.

Действия пользователя для разблокирования системы аналогичны его действиям при входе в систему.

1.5.2. Дискреционный механизм контроля доступа к ресурсам

Субъектами доступа в СЗИ являются поименованные пользователи и процессы. Объектами доступа выступают следующие ресурсы:

- объекты файловой системы (логические диски, каталоги и файлы);
- порты (COM, LPT, USB) и подключаемые к ним устройства;
- процессы (файлы, запускаемые на исполнение).

Таким образом, дискреционный механизм контроля доступа к ресурсам включает:

- механизм контроля доступа к объектам файловой системы;
- механизм разграничения прав доступа к портам;
- механизм разграничения прав доступа на запуск процессов.

Администратор безопасности может изменять как список пользователей и контролируемых объектов защиты, так и права доступа пользователей к объектам.

1.5.3. Мандатный механизм контроля доступа к ресурсам

Мандатный механизм контроля доступа обеспечивает разграничение доступа субъектов (пользователей, процессов) к объектам (дискам, папкам, файлам) с помощью квалификационных меток – числовых значений уровня допуска субъекта или конфиденциальности объекта. Чем метка больше, тем выше уровень допуска субъекта или конфиденциальность объекта.

1.5.4. Механизм контроля печати

Механизм контроля печати осуществляет аудит процесса печати и маркировку конфиденциальных документов, выводимых на печать. Аудит печати подразумевает регистрацию всех фактов печати документов, в том числе и факты запрета печати в соответствии с настройками механизма контроля печати. Маркировка включает в себя вывод настраиваемого штампа в колонтитулах на страницах печатаемых документов. Специальный штамп может содержать следующие поля:

- дату/время распечатки;
- имя файла документа;
- уровень конфиденциальности документа;
- порядковый номер в формате «текущий номер страницы из общего числа листов»;
- имя пользователя, производившего печать документа;
- имя рабочей станции, с которой производилась печать документа;
- имя принтера, с которого производилась печать документа.

Механизм контроля печати имеет следующие ограничения:
1) запрещается включение механизма контроля печати СЗИ на рабочих станциях с установленным DLP-агентом Symantec Data Loss Prevention – при включении механизма контроля печати происходит аварийное завершение процесса explorer.exe;
2) для устойчивого функционирования АРМ с установленным СКЗИ «КриптоПро CSP», при использовании механизма контроля печати СЗИ, версия сборки СКЗИ должна быть 3.9.8293 или 4.0.9589 (Gauss) и выше;
3) механизмом контроля печати поддерживается работа с печатающими устройствами, для которых установлены драйвера поддержки PCL (работа механизма контроля печати с печатающими устройствами, для которых установлены драйвера поддержки PostScript не гарантируется – возможность печати на подобных устройствах может быть заблокирована);
4) в семействе Windows 8/8.1 не поддерживается работа с приложениями, использующими metro-интерфейс;

5) в режиме маркировки документов не поддерживается цветная печать – при печати цветного текста (изображения) вывод на печать происходит в черно-белом варианте;
6) блокируется возможность печати из браузера Mozilla Firefox;
7) блокируется возможность печати содержимого страницы браузера Internet Explorer (версия 11) при включенном контроле учетных записей (UAC);
8) печать на принтерах общего доступа возможна только при включении режима маркировки документов.

1.5.5. Механизм гарантированного удаления

Механизм гарантированного удаления запрещает удаление стандартным способом тех файлов, для которых определено гарантированное удаление. Удаление файлов происходит трехкратным затиранием содержимого по специальному алгоритму, исключающему считывание остаточной информации на диске после удаления.

1.5.6. Механизм очистки памяти

Механизм очистки памяти СЗИ «Блокхост-сеть 2.0» осуществляет очистку (обнуление) освобождаемых областей оперативной памяти ЭВМ и удаляемых данных на локальных дисках. Очистка осуществляется двукратной записью нулей в освобождаемую область памяти.

1.5.7. Механизм контроля целостности и гарантированного восстановления

Механизм контроля целостности выполняет проверку целостности контролируемых файлов по алгоритму CRC-32 и при обнаружении ошибок обеспечивает их восстановление.

Этот же механизм используется для контроля целостности и надежного восстановления свойств СЗИ после сбоев и отказов оборудования. При обнаружении ошибки выполняется восстановление контролируемых объектов из резервных копий, хранящихся в БД, после перезагрузки системы.

1.5.8. Механизм контроля целостности реестра

Механизм контроля целостности реестра выполняет проверку целостности разделов (ветвей), параметров (ключей) и значений параметров реестра Windows путем сравнения с эталоном и при обнаружении ошибки информирует об этом пользователя. Модуль контроля целостности реестра осуществляет контроль целостности объектов реестра Windows по следующим типам событий:

- переименование/удаление контролируемого раздела;
- добавление подраздела в контролируемый раздел;
- удаление существующего подраздела из контролируемого раздела;
- изменение названия подраздела в контролируемом разделе;
- добавление нового параметра в контролируемый раздел;
- изменение названия параметра в контролируемом разделе;
- удаление параметра в контролируемом разделе;
- изменение значения параметра в контролируемом разделе.

Модуль контроля целостности реестра реализован в виде отдельного программного приложения.

Описание работы с модулем контроля целостности реестра приведено в документе «СЗИ «Блокхост-сеть 2.0». Контроль целостности реестра. Руководство администратора безопасности».

1.5.9. Механизм регистрации событий и аудита

Механизм регистрации событий выполняет прием сообщений аудита от компонентов СЗИ «Блокхост-сеть 2.0». Журналы событий формируются из сообщений, поступающих при обращении к защищаемым ресурсам, а также при срабатывании всех механизмов защиты, встроенных в операционную систему. Также СЗИ позволяет отправлять сообщения аудита на внешний Syslog-сервер.

1.5.10. Механизм персонального экрана

Персональный экран реализует защиту ПК, подключенного к ЛВС, от НСД к его ресурсам из внешних источников, разграничение доступа пользователя ПК к ресурсам сети, а также – фильтрацию сетевого трафика.

1.5.11. Механизм администрирования СЗИ

Механизм администрирования обеспечивает настройку параметров работы СЗИ. Параметры СЗИ делятся на системные, которые задают правила доступа всех пользователей и индивидуальные, которые относятся к правилам доступа конкретных пользователей. Для удобства работы предусмотрен режим ввода настроек с использованием шаблонов.

После запуска консоли администрирования СЗИ администратор безопасности может выполнять следующие действия:

- создание, изменение, удаление субъектов (пользователей и процессов), их уровней доступа, паролей пользователей с возможностью установки для пользователей различных шаблонов настроек доступа;
- назначение объектам уровней конфиденциальности;
- установка контролируемых объектов (файлы, папки, диски, COM-, LPT-, USB-порты) для конкретных субъектов с указанием атрибутов доступа;
- установка замкнутой программной среды;
- формирование списков процессов запрещенных для запуска;
- формирование списка файлов, целостность которых требуется контролировать;
- делегирование прав доступа по администрированию СЗИ пользователям (такие пользователи должны быть включены в группу администраторов текущей рабочей станции);
- формирование списка процессов для контроля печати и настройка колонтитулов для выводимой информации;
- формирование режимов работы и набора правил доступа для персонального экрана.

С помощью модуля интерфейса администратора производится настройка параметров системы защиты, сохранение их в БД настроек и посылка команд другим модулям с тем, чтобы они обновили свои настройки. Действия по изменению настроек фиксируются в журналах аудита.

1.6. Общая архитектура СЗИ «Блокхост-сеть 2.0»

Общая архитектура СЗИ «Блокхост-сеть 2.0» представлена на рисунке 1.2.

Программную часть СЗИ «Блокхост-сеть 2.0» можно разделить на:

- ядро, выполняющее непосредственно функции защиты информации от несанкционированного доступа;
- программы, обеспечивающие пользовательский интерфейс СЗИ «Блокхост-сеть 2.0»;
- вспомогательные программные библиотеки и служебные программы (установка/удаление СЗИ «Блокхост-сеть 2.0»).

Ядро комплекса взаимодействует с остальной частью программного обеспечения с использованием внутренних интерфейсов, представленных в специальных форматах. Надежность защиты информации от несанкционированного доступа полностью определяется качеством работы ядра СЗИ «Блокхост-сеть 2.0» и не зависит от других компонентов программного обеспечения. Корректность взаимодействия ядра СЗИ «Блокхост-сеть 2.0» и остальной части программного обеспечения обеспечивается применением внутренних интерфейсов, не допускающих передачу исполняемых программных кодов и технологией проектирования, а также не допускающей использования в составе программного обеспечения исполняемых кодов, модифицирующих коды и данные ядра СЗИ «Блокхост-сеть 2.0».

Входными данными для работы модуля аутентификации являются списки зарегистрированных пользователей и их пароли, хранимые в БД настроек СЗИ, синхронизированные с БД пользователей, зарегистрированных в операционной системе Windows. При включении компьютера этот модуль начинает работать на последнем этапе загрузки операционной системы. Все попытки пройти аутентификацию записываются в журнал аудита. При успешном доступе пользователя в систему его идентификационное имя фиксируется в БД настроек СЗИ, считывается модулем диспетчера доступа и используется для контроля всех последующих его действий.

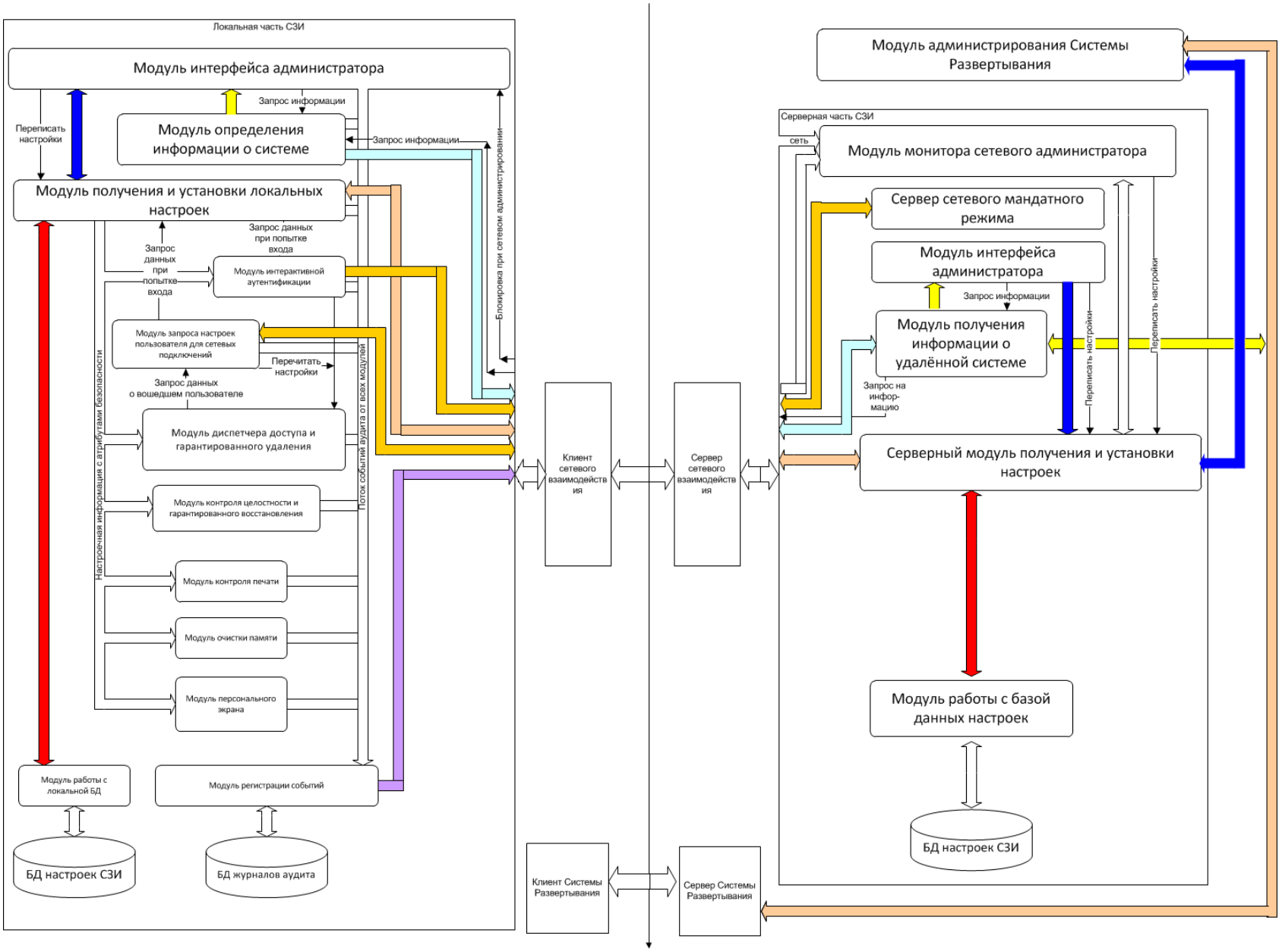


Рисунок 1.2. Общая архитектура СЗИ «Блокхост-сеть 2.0»

Модуль диспетчера доступа является драйвером файловой системы и загружается до запуска графической оболочки ОС. Драйвер запускается после прохождения пользователем аутентификации и начинает контролировать доступ к защищаемым объектам на основе информации из БД настроек СЗИ. Все обращения к защищаемым ресурсам контролируются и фиксируются в БД журналов аудита модулем регистрации событий.

Модуль контроля целостности и гарантированного восстановления и модуль регистрации событий являются сервисами (службами) ОС Windows, запускаются при загрузке системы и постоянно находятся в памяти до перезагрузки компьютера. Модули используют для своей работы настройки СЗИ и фиксируют в журналах аудита нарушение целостности поставленных на контроль файлов.

Модуль персонального экрана стартует при загрузке ОС. Модуль загружается после драйвера NDIS, но до регистрации сетевых протоколов. Проверка старта персонального экрана может быть выполнена вручную с помощью команды ***sc query DrvFltIP*** (для всех ОС Windows).

При входе пользователя в систему драйверу персонального экрана от модуля идентификации и аутентификации приходит конфигурация настроек, согласно которой выполняется дальнейшая фильтрация сетевого трафика. Драйвер персонального экрана регистрируется на этапе инициализации как драйвер-фильтр интерфейса NDIS 6, настраиваются функции обратного вызова, которые гарантируют присоединение фильтра к любому существующему или вновь появляющемуся в системе сетевому адаптеру. В дальнейшем для каждого такого адаптера фильтром обрабатывается любая сетевая активность указанного устройства. Регистрация трафика выполняется согласно опциям ***Общих настроек*** профиля ПЭ, а так же опции ***Аудит*** для каждого отдельно взятого правила. Контроль целостности программной и информационной части персонального экрана выполняется модулем контроля целостности (GIS.Client.IntegrityChecker.exe), а так же с помощью ЭП.

Каждый драйвер ПЭ подписан доверенным сертификатом компании ООО «Газинформсервис», который включен в список доверенных распространителей системного ПО компании Verisign и Microsoft. Корректность проверки ЭП гарантирует целостность программной и информационной части ПЭ. Проверка ЭП выполняется автоматически средствами ОС при запуске драйвера. Драйвер, подпись которого не была проверена или целостность исполняемого образа которого была нарушена, не будет загружен ОС. Резервная копия исполняемого образа создается в папке *C:\BlockHost\Backup* при установке СЗИ «Блокхост-сеть 2.0». Процедура восстановления после сбоев и отказов оборудования, обеспечивающая восстановление свойств ПЭ, гарантируется спецификацией интерфейса NDIS 6 и является архитектурной особенностью. При нарушении целостности драйвера персонального экрана администратор безопасности может восстановить его следующим образом:

Заново установить драйвер персонального экрана из папки *C:\BlockHost\Backup\BlockHost\bppfw*. Для этого необходимо:

1) открыть окно **«Центр управления сетями и общим доступом»** (***Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом***) и в нем нажать на ссылку ***Подключение по локальной сети***;
2) в открывшемся окне **«Состояние-Подключение по локальной сети»** (рис. 1.3) нажать кнопку ***Свойства***.

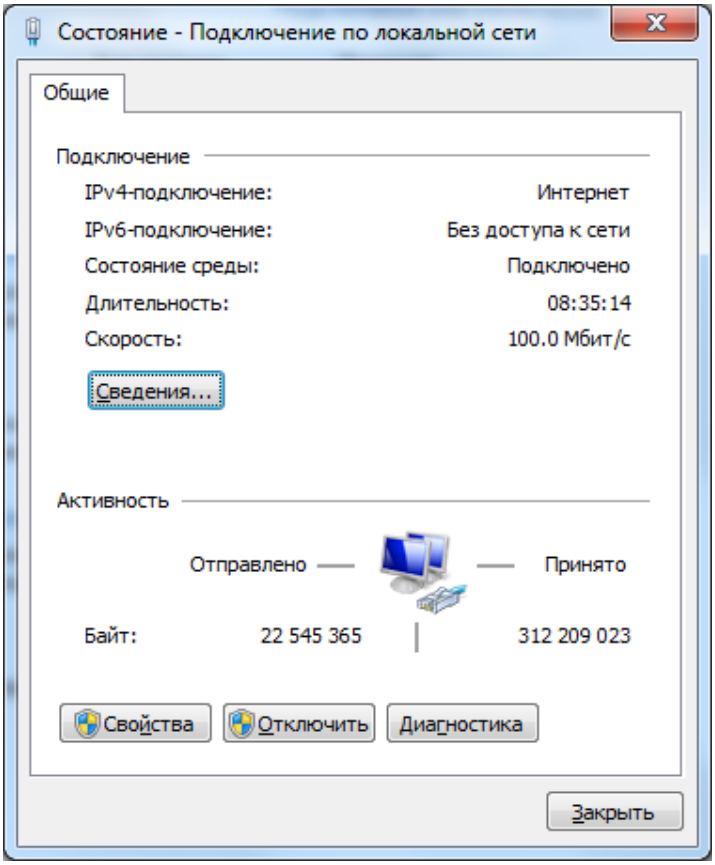


Рисунок 1.3. Окно «Состояние-Подключение по локальной сети»

3) в открывшемся окне **«Подключение по локальной сети - свойства»** выделить компонет ***Клиент для сетей Microsoft*** и нажать кнопку ***Установить*** (рис. 1.4):

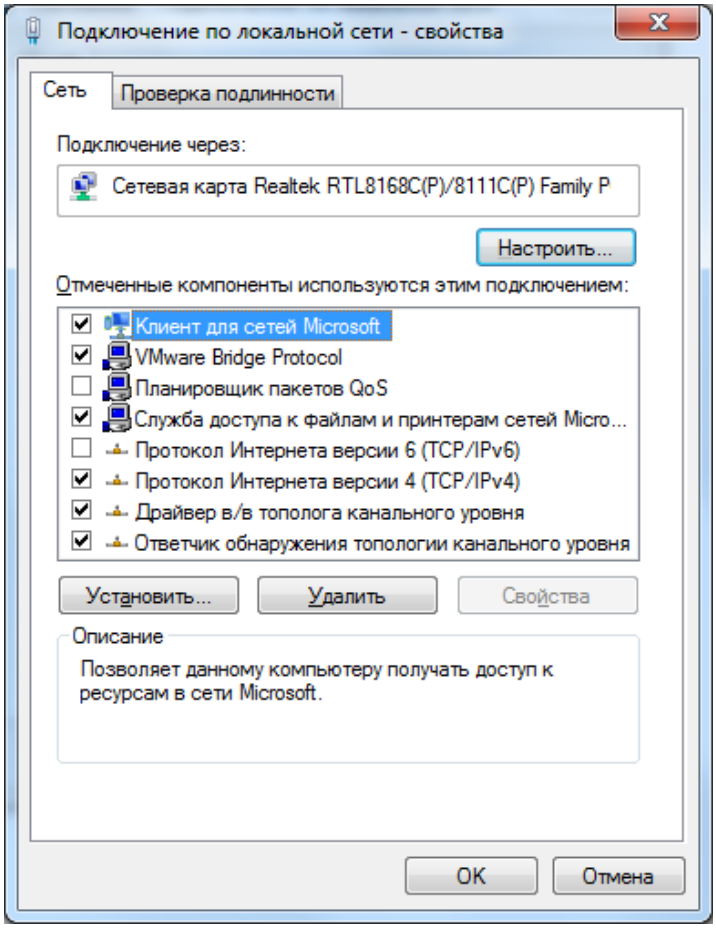


Рисунок 1.4. Выбор пункта «Установить»

4) в открывшемся окне **«Выбор сетевых компонентов»** выделить тип сетевого компонента ***Служба*** и нажать кнопку ***Добавить***:

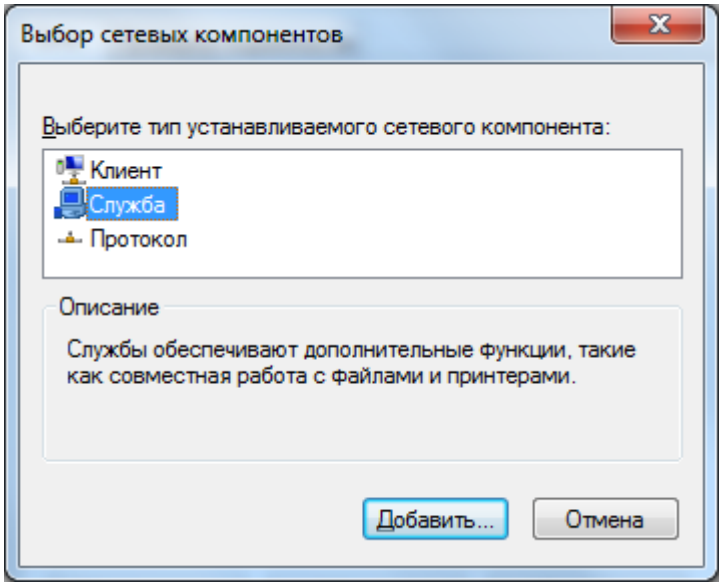


Рисунок 1.5. Выбор компонента «Служба»

5) в окне выбора сетевой службы нажать кнопку ***Установить с диска*** (рис. 1.6):

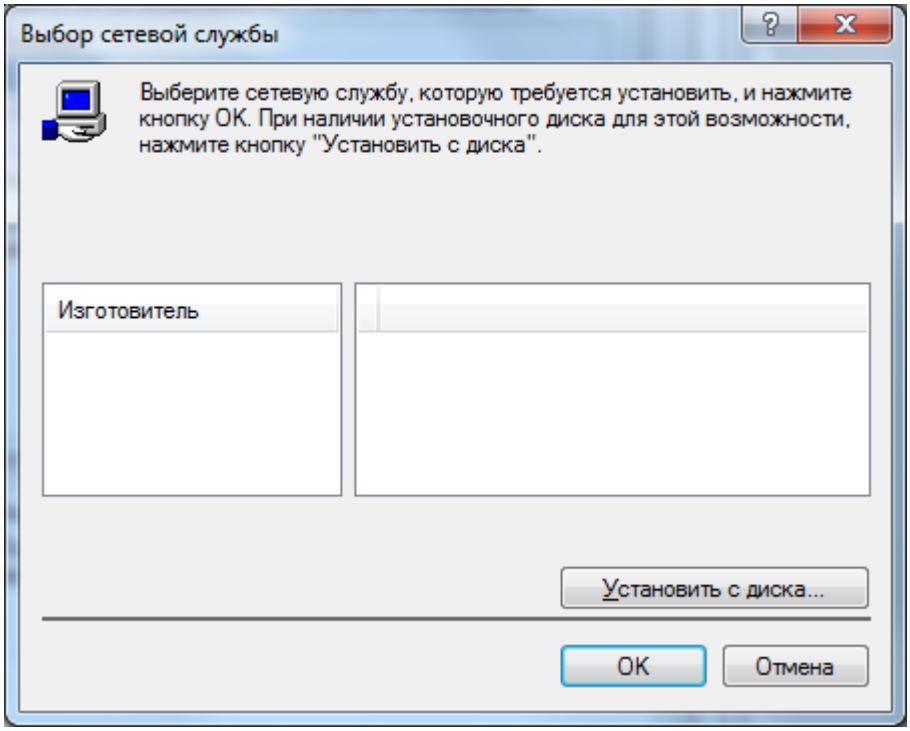


Рисунок 1.6. Установка драйвера

6) в открывшемся окне **«Установка с диска»** нажать кнопку ***Обзор***, в окне **«Поиск файла»** выбрать в папке *C:\BlockHost\Backup\BlockHost\bppfw* файл *DrvFltIP.inf* и нажать кнопку ***OK***.

Аудит сетевого трафика может выполняться, как посредством записи соответствующих событий в системный журнал с помощью службы диспетчера аудита (GIS.Client.LogDispatcher.exe), так и их отправкой на Syslog-сервер.

С помощью модуля интерфейса администратора (локального и серверного) производится настройка параметров системы защиты и сохранение их в БД настроек. Для того чтобы новые настройки СЗИ вступили в силу, необходимо сменить сеанс пользователя. Действия администратора безопасности по изменению настроек СЗИ фиксируются в журналах аудита.

Модуль определения информации о системе получает данные о локальных ресурсах машины, списках пользователей, запущенных процессах и обслуживает запросы на получение данной информации как от локального модуля интерфейса администратора, так и удаленные запросы.

Модуль получения информации об удаленной системе перенаправляет запросы о доступных ресурсах локальной машины модулю определения информации о системе данной локальной станции. Так же он обрабатывает информацию о подключении и отключении клиентских станций, информируя об этом модуль интерфейса администратора для разрешения/блокирования возможности их администрирования.

Модуль запроса настроек пользователя для сетевых подключений обрабатывает запросы модуля диспетчера доступа на загрузку настроек вошедших сетевых пользователей или запуска процессов от имени пользователя, не вошедшего интерактивно. Модуль обрабатывает запрос о текущем мандате работы пользователей на рабочей станции, что необходимо для организации сетевого мандатного режима.

Модуль очистки памяти контролирует работающие процессы и очищает память при завершении процесса, поставленного на контроль.

Модуль получения и установки настроек (локальный и серверный) является диспетчером, которому направляются запросы получения рабочих параметров при загрузке системы, входе нового пользователя или перезапуске модулей.

Модуль работы с базой данных (локальный и серверный) обрабатывает запросы на получение, сохранение настроек, кодирование и раскодирование файла конфигурации параметрами работы системы и разграничениями пользователей.

В модуль регистрации событий собираются все события аудита от модулей СЗИ, которые в свою очередь сохраняются в базе данных журналов аудита. Так же производится фильтрация событий аудита для выявления событий из определенного перечня, которые отправляются модулю монитора сетевого администратора для сигнализации о нарушениях безопасности.

Модуль контроля печати блокирует возможность печати на установленный виртуальный принтер и отслеживает отправку пользователем документа на другие установленные принтеры. Когда пользователь отправляет какой-либо документ на принтер, то определяется имя пользователя, домен (если есть), к которому принадлежит пользователь, процесс, который производит печать, и принтер, на который производится печать. После этого задание переправляется на виртуальный принтер, на котором производится проверка полномочий печати и добавление колонтитулов на странице печатаемой информации.

Модули клиента и сервера сетевого взаимодействия предназначены для защищенного удаленного управления разграничением полномочий пользователей на удаленных рабочих станциях. Они осуществляют передачу данных по протоколу TCP/IP, взаимную аутентификацию, аутентификацию локальной станции и сервера удаленного управления СЗИ. Так же по защищенному каналу они осуществляют конфиденциальный обмен данными, управление потоками данных для различных модулей СЗИ.

Модуль монитора сетевого администратора сигнализирует сетевому администратору о попытках нарушения безопасности, о подключении, о входе пользователей на локальные станции.

Сервер сетевого мандатного режима хранит список работающих машин и мандаты вошедших пользователей, что необходимо для осуществления сетевого мандатного режима.

2. Условия применения СЗИ «Блокхост-сеть 2.0»

2.1. Требования к аппаратной конфигурации

СЗИ «Блокхост-сеть 2.0» устанавливается на компьютеры с процессорами, имеющими архитектуру x86 и AMD64. Для корректной работы СЗИ «Блокхост-сеть 2.0» к аппаратной конфигурации компьютера предъявляются требования, приведенные в таблице 2.1.

Таблица 2.1 – Требования к аппаратной конфигурации ПК

Тактовая частота процессора	Объем оперативной памяти	Объем свободного места на жестком диске	Режим видео, не менее
Определяются требованиями операционной системы			800x600, 256 цветов

Для функционирования персональных идентификаторов необходимо:

- USB-порт – при использовании идентификаторов eToken, SafeNet eToken (USB-ключ или смарт-карта), ruToken, JaCarta (USB-ключ и смарт-карта), Avest Token, ESMART Token (USB-ключ и смарт-карта) или USB-накопителя;
- дисковод гибких дисков – при использовании идентификаторов на дискетах.

2.2. Требования к составу установленного программного обеспечения

Допускается установка СЗИ «Блокхост-сеть 2.0» на компьютеры, функционирующие под управлением операционных систем:

1) клиентская часть СЗИ:
   - 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 Vista Business SP2 (32-разрядная);
   - Windows Vista Business SP2 (64-разрядная);
   - Windows 7 Home Basic SP1 (32-разрядная);
   - Windows 7 Home Basic SP1 (64-разрядная);
   - Windows 7 Home Premium SP1 (32-разрядная);
   - Windows 7 Home Premium SP1 (64-разрядная);
   - Windows 7 Professional SP1 (32-разрядная);
   - Windows 7 Professional SP1 (64-разрядная);
   - Windows 7 Enterprise SP1 (32-разрядная);
   - Windows 7 Enterprise SP1 (64-разрядная);

- Windows 7 Ultimate SP1 (32-разрядная);
- Windows 7 Ultimate SP1 (64-разрядная);
- Windows 8/8.1 Core (32-разрядная);
- Windows 8/8.1 Core (64-разрядная);
- Windows 8/8.1 Professional (32-разрядная);
- Windows 8/8.1 Professional (64-разрядная);
- Windows 8/8.1 Enterprise (32-разрядная);
- Windows 8/8.1 Enterprise (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).

2) серверная часть СЗИ:

- 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).

В составе установленного программного обеспечения необходимы следующие компоненты:

- .NET Framework 2.0 (при установке клиентской и серверной частей СЗИ);
- .NET Framework 4.0 (при установке серверной части СЗИ);
- обновление NDP40-KB2468871 для .NET Framework 4.0 (при установке серверной части СЗИ)
- драйверы для устройств eToken и SafeNet eToken (любой из вариантов):
  - SafeNet Authentication Client 8.2. Подходит для всех поддерживаемых ОС, в комплект поставки СЗИ не входит.
  - eToken RTE 3.66 (или eToken PKI Client 5.1 SP1) – при использовании персональных идентификаторов eToken PRO, eToken NG-FLASH, eToken NG-OTP;
  - eToken PKI Client 5.1 SP1 – при использовании персональных идентификаторов eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken PRO (Java), eToken GT (Java), eToken PRO (Java) SC, eToken PRO SC;
- драйверы для устройств ruToken (при использовании персональных идентификаторов ruToken S, ruToken Lite, ruToken Web, ruToken ЭЦП, ruToken ЭЦП Flash);
- драйверы «Единый клиент JaCarta»для устройств JaCarta (при использовании персональных идентификаторов JaCarta);

- драйверы «ESMART PKI Client» для устройств ESMART Token (при использовании (персональных идентификаторов ESMART Token USB 64K и ESMART Token SC 64K);
- драйверы AvBignDriver, устанавливаемые в составе пакета Avest CSP Bign, для поддержки персональных идентификаторов AvBign;
- СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2 – при организации входа пользователей в ОС с помощью сертификатов.

Драйверы для устройств eToken (eToken PKI Client 5.1 SP1 и eToken RTE 3.66), JaCarta (кроме драйверов для ОС Windows 8/8.1/2012/2012R2) и ruToken, а также .Net Framework поставляются на одном диске с СЗИ «Блокхост-сеть 2.0». SafeNet Authentication Client 8.2, драйверы JaCarta для ОС Windows 8/8.1/2012/2012R2, драйверы для устройств ESMART Token и Avest Token в комплект поставки не входят.

При установке СЗИ «Блокхост-сеть 2.0» на ПК под управлением ОС Windows 7/2008R2/8/8.1/2012/2012R2 также должна быть включена платформа Microsoft .NetFramework 3.5.

Перед началом установки СЗИ на ОС Windows 8/8.1/2012/2012R2 необходимо отключить встроенный антивирус ОС (Windows Defender).

В некоторых случаях для корректного функционирования СЗИ необходимо понизить уровень контроля учетных записей (UAC) в ОС Windows (вплоть до полного отключения) (рис. 2.1). Для изменения параметров UAC необходимо войти в ОС под учетной записью встроенного администратора.

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности и контролируемых рабочих станциях должны быть открыты 999 TCP-порт и 5555 UDP-порт.

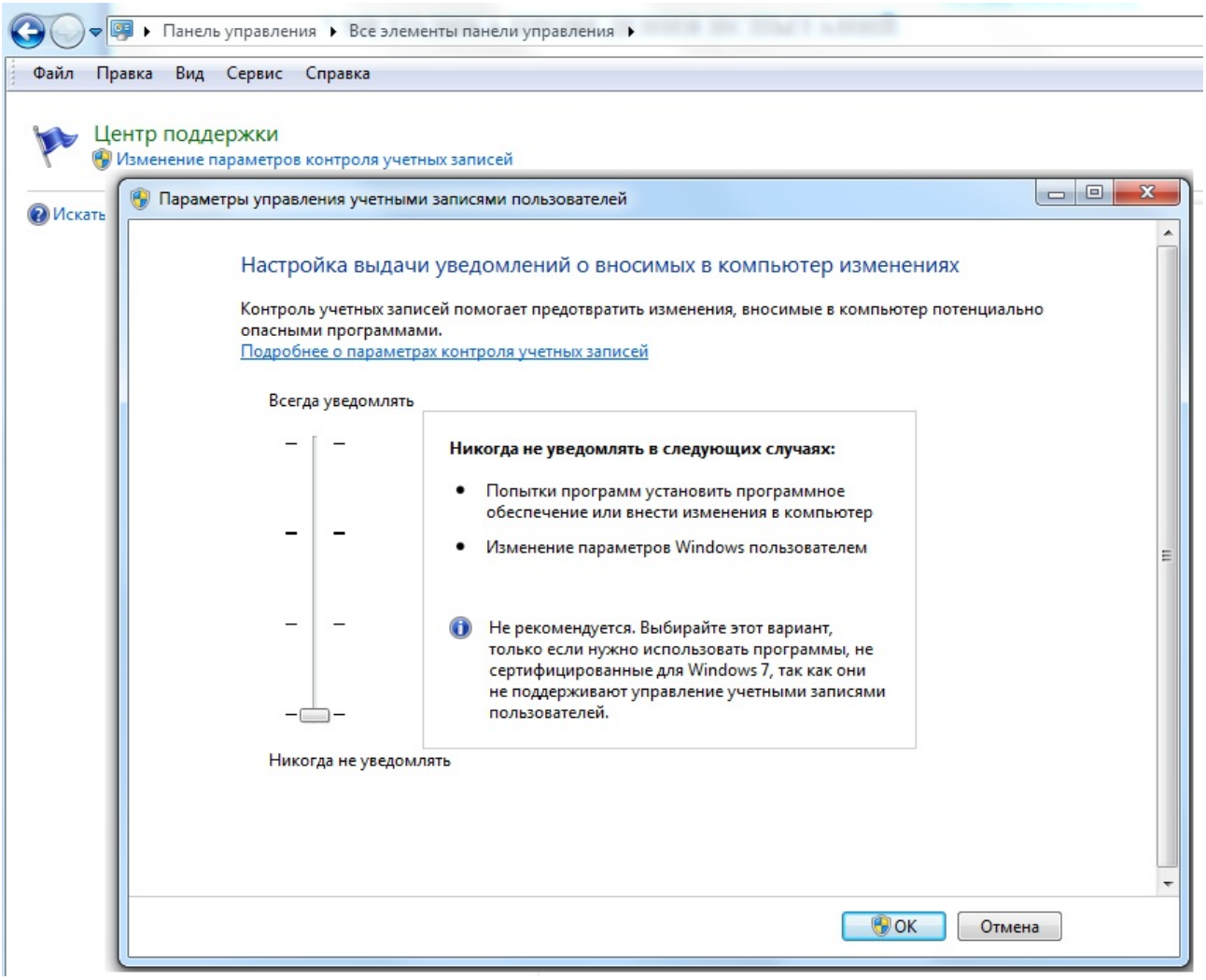


Рисунок 2.1. Изменение уровня контроля UAC

3. Подготовка СЗИ «Блокхост-сеть 2.0» к работе

3.1. Запуск СЗИ «Блокхост-сеть 2.0»

СЗИ «Блокхост-сеть 2.0» включает в себя локальную и серверную консоли администрирования. Локальная консоль администрирования позволяет выполнять настройку СЗИ «Блокхост-сеть 2.0» непосредственно на рабочей станции. Серверная консоль администрирования позволяет выполнять удаленное администрирование СЗИ с рабочего места администратора безопасности.

Первый запуск серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» должен осуществляться от имени учетной записи встроенного администратора, и может быть произведен сразу после установки СЗИ или после перезагрузки ОС с предъявлением персонального идентификатора, указанного при установке СЗИ. Последующие запуски серверной консоли СЗИ должны осуществлять зарегистрированные в СЗИ пользователи, входящие в группу администраторов ОС Windows сервера СЗИ и которым делегированы права запуска консоли администрирования СЗИ. Обязательным условием для работы в серверной консоли СЗИ является вход в систему администраторов СЗИ со значением мандатной метки равным **1**.

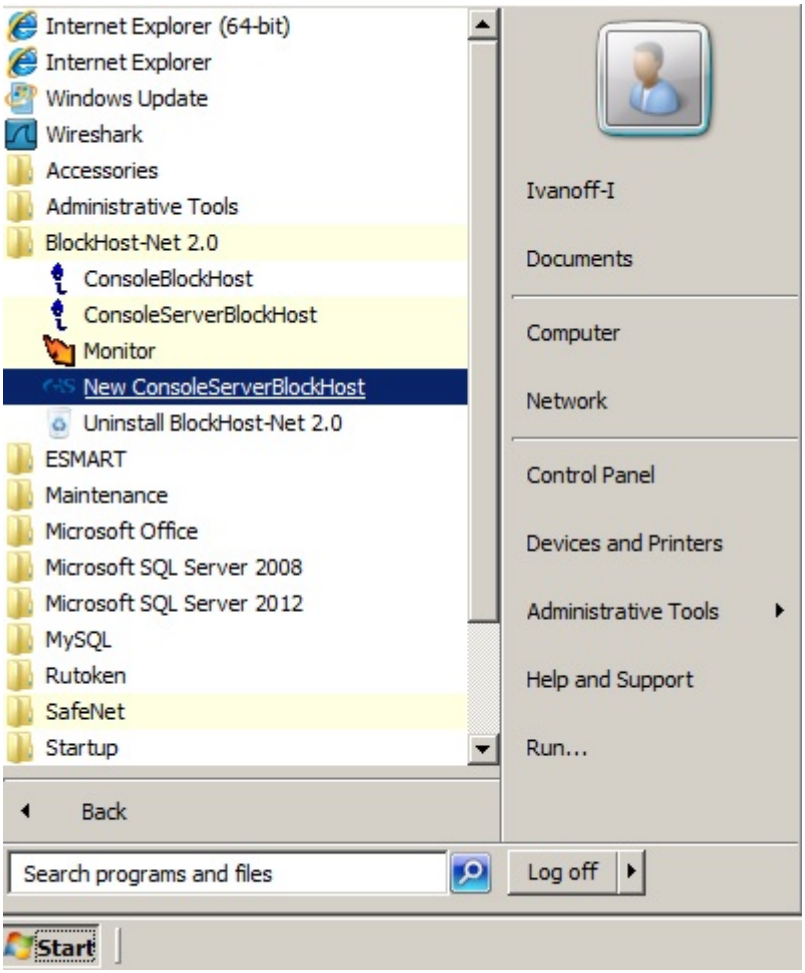


Рисунок 3.1. Меню вызова серверной консоли администрирования СЗИ в ОС Windows Server 2008R2

Запуск серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» осуществляется из меню ***Пуск →Все программы →BlockHost-Net 2.0 →New***

ConsoleServerBlockHost (рис. 3.1). Запуск серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» при использовании ОС Windows 2012/2012R2 приведен на рисунке 3.2.

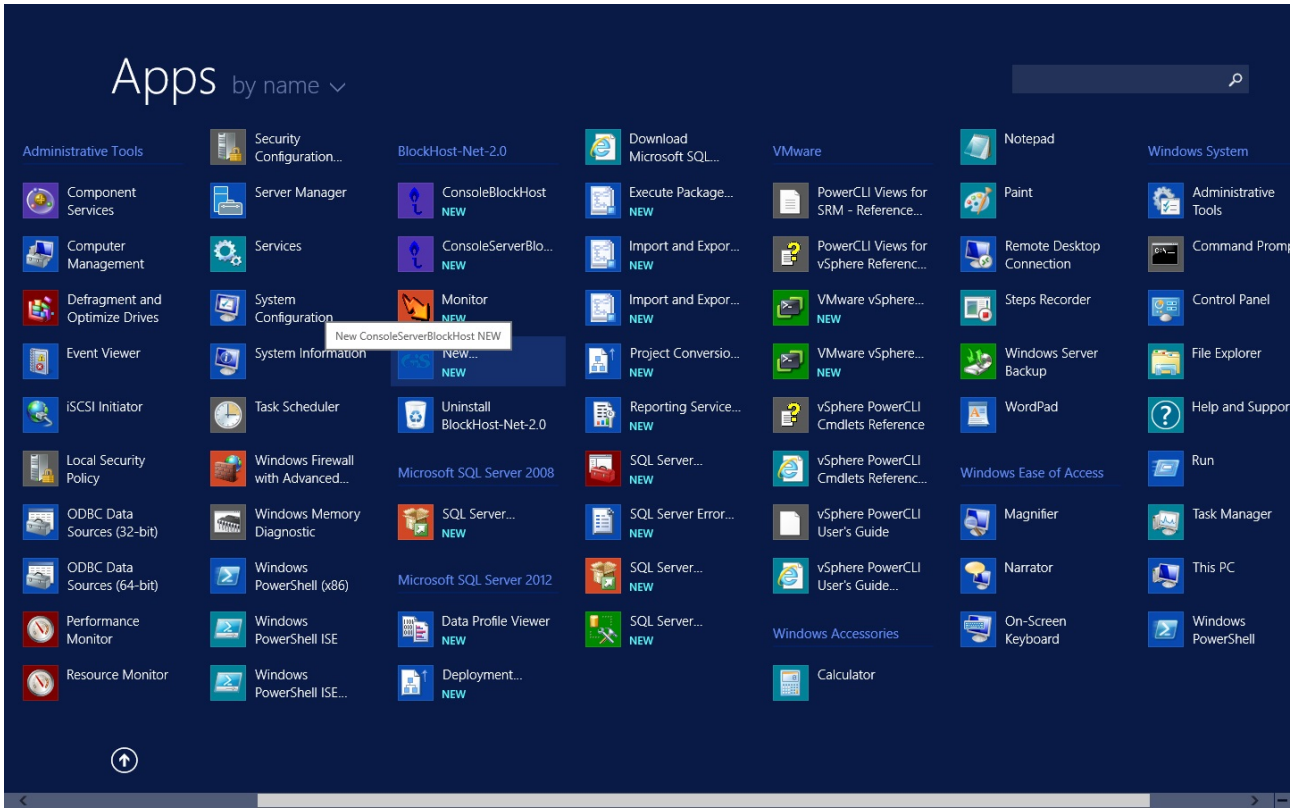


Рисунок 3.2. Меню вызова серверной консоли администрирования СЗИ в ОС Windows Server 2012

3.2. Серверная консоль администрирования СЗИ «Блокхост-сеть 2.0»

Серверная консоль администрирования СЗИ предназначена для:

- осуществления настроек механизмов разграничения доступа и защиты информации на контролируемых рабочих станциях;
- осуществления настроек серверной части СЗИ;
- отображения информации о контролируемых рабочих станциях, пользователях, объектах, стоящих на контроле настройках механизмов защиты информации;
- отображения аудита работы механизмов СЗИ для всех пользователей на каждой из контролируемых рабочих станциях.

Серверная консоль позволяет выполнять централизованное управление удаленными рабочими станциями с рабочего места администратора безопасности.

В окне серверной консоли администрирования СЗИ (рис. 3.3) расположены следующие элементы:

- главное меню,
- элементы управления – кнопки,
- дочерние окна:
  - сервера – **«Список машин», «Лог», «Токены сервера»**,
  - клиента – **«Настройки машины», «Токены <имя_клиента>»**;

Содержимое и заголовок окна **«Токены…»** изменяется в зависимости от того, какая рабочая станция или группа выбрана в окне **«Список машин»** (подробнее см. п. 3.2.2.3 настоящего руководства).

- вкладка **Основная панель настроек клиентов.**

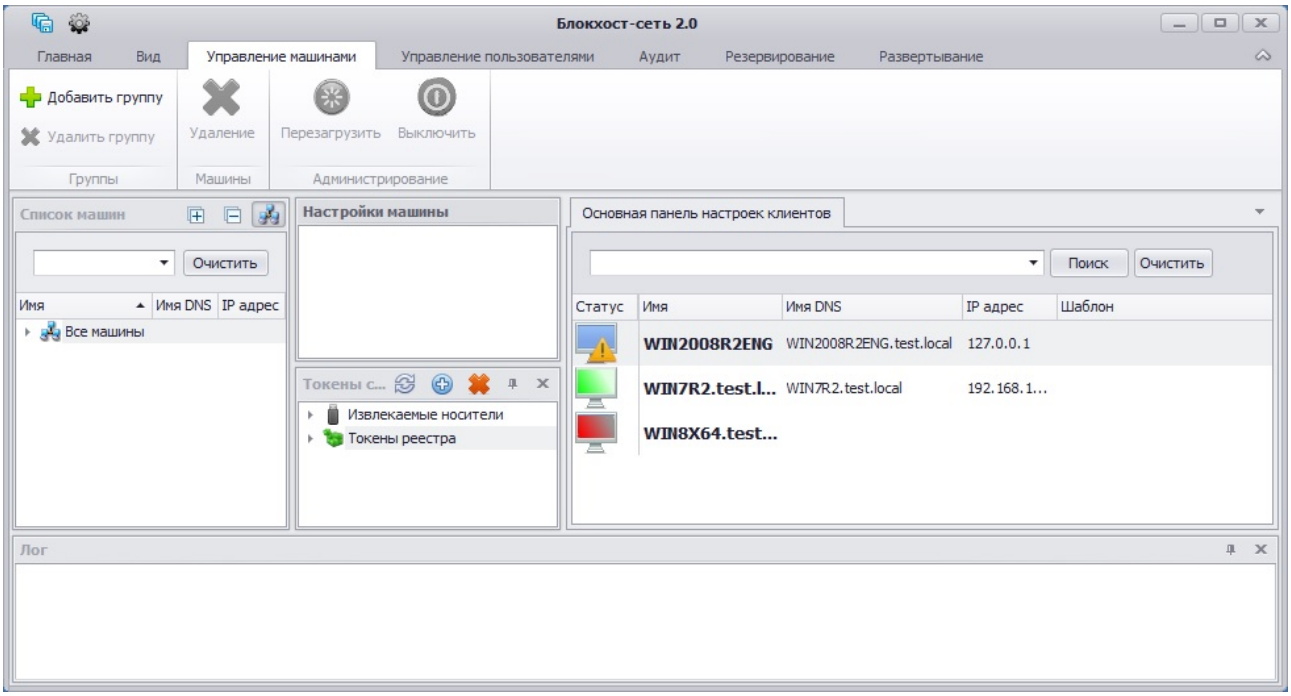


Рисунок 3.3. Серверная консоль администрирования СЗИ «Блокхост-сеть 2.0»

Настройки механизмов СЗИ «Блокхост-сеть 2.0» в серверной консоли отображаются отдельно для каждой контролируемой рабочей станции.

Из серверной консоли СЗИ «Блокхост-сеть 2.0 также возможно удаленное управление контролируемыми рабочими станциями (пункты главного меню ***Управление машинами***):

- перезагрузить рабочую станцию;
- выключить рабочую станцию.

3.2.1. Меню серверной консоли администрирования СЗИ «Блокхост-сеть 2.0»

3.2.1.1. Основные операции меню серверной консоли СЗИ «Блокхост-сеть 2.0»

Меню расположено в верхней части консоли и предназначено для управления СЗИ «Блокхост-сеть 2.0». Меню позволяет выполнять следующие операции:

- создание и удаление групп;
- удаление рабочих станций из списка контролируемых текущим сервером СЗИ;
- удаленное управление контролируемыми рабочими станциями;
- управление пользователями контролируемых рабочих станций;
- просмотр и сохранение сообщений аудита СЗИ контролируемых рабочих станций;
- добавление рабочих станций в список контролируемых текущим сервером СЗИ;
- установка клиентской части СЗИ на удаленные рабочие станции

- резервное копирование и восстановление настроек текущего сервера СЗИ и контролируемых им рабочих станций;
- сохранение произведенных настроек СЗИ «Блокхост-сеть 2.0» для текущей рабочей станции;
- сохранение произведенных настроек СЗИ «Блокхост-сеть 2.0» для всех контролируемых рабочих станций;
- отмена произведенного действия с помощью пункта ***Главная →Отменить все изменения***.

Необходимо сохранять произведенные изменения в настройках СЗИ контролируемых рабочих станций перед выходом из серверной консоли администрирования.

3.2.1.2. Резервное копирование и восстановление настроек сервера СЗИ

Резервное копирование настроек сервера СЗИ подразумевает сохранение в зашифрованном файле (файле с расширением *.set*) списка рабочих станций, контролируемых данным сервером (подключенных к данному серверу), настроек сетевого взаимодействия сервера СЗИ и контролируемых текущим сервером СЗИ рабочих станций, настроек клиентской части сервера СЗИ.

Резервное копирование настроек может понадобиться для:

- создания резервной копии настроек сервера (если по какой-либо причине произошла потеря настроек данного сервера, их можно будет восстановить);
- переноса настроек с одного сервера безопасности на другой (т.е. можно скопировать и перенести список контролируемых рабочих станций сервера).

Для выполнения резервного копирования настроек сервера СЗИ необходимо в серверной консоли администрирования СЗИ:

1) выбрать пункт меню ***Резервирование →Резервирование настроек сервера***;
2) в открывшемся окне **«Сохранение настроек»** (рис. 3.4):

- в поле ***Пароль*** ввести пароль, с использованием которого будет зашифрован файл настроек сервера СЗИ;
- нажав на кнопку ***Выбор пути*** указать, в открывшемся стандартном окне Windows **«Сохранить как»**, каталог размещения и имя файла, в котором будут зарезервированы настройки;
- нажать кнопку ***Сохранить***.

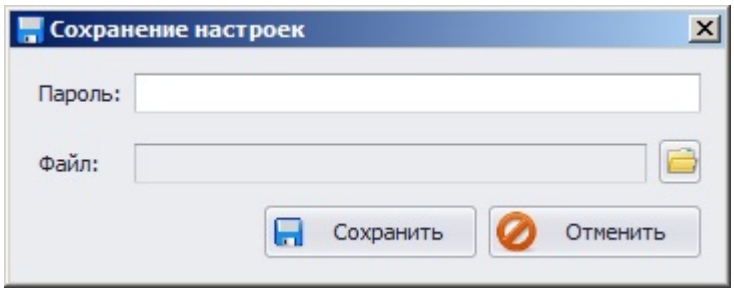


Рисунок 3.4. Окно сохранения настроек сервера СЗИ

В результате в указанном каталоге будет создан файл, в котором в зашифрованном виде будут записаны текущие настройки сервера СЗИ.

При необходимости восстановления настроек сервера СЗИ администратору безопасности в серверной консоли администрирования текущего сервера СЗИ необходимо:

1) выбрать пункт меню ***Резервирование →Восстановление настроек сервера***;

2) подтвердить восстановление настроек клиентской части СЗИ на текущем сервере СЗИ (рис. 3.5);

В случае нажатия на кнопку ***Нет*** (***No***) в окне подтверждения восстановления настроек клиентской части сервера СЗИ операция восстановления настроек сервера СЗИ будет прекращена, и настройки текущего сервера СЗИ останутся без изменений.

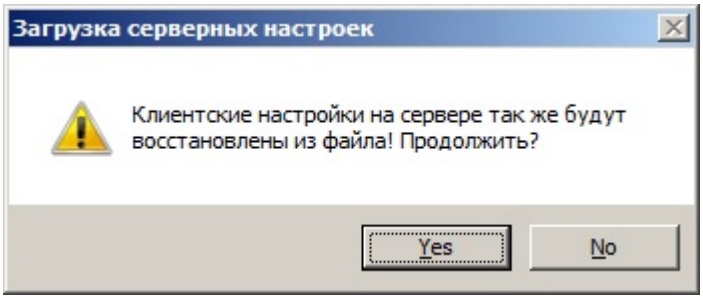


Рисунок 3.5. Подтверждение восстановления настроек клиентской части СЗИ

3) в открывшемся окне **«Восстановление настроек»**:

- ввести пароль, при помощи которого был зашифрован файл настроек;
- указать имя и каталог размещения файла, в котором были зарезервированы настройки. Указать имя файла настроек можно введя полный путь к файлу в поле ***Файл*** вручную, или нажав кнопку ***Выбор пути***, указать файл в открывшемся стандартном окне Windows **«Открыть»**;
- из выпадающего списка поля ***Носитель*** выбрать ключевой носитель, с использованием которого производилась установка СЗИ «Блокхост-сеть 2.0» и ввести PIN-код доступа к нему в соответствующее поле;
- нажать кнопку ***Восстановить***:

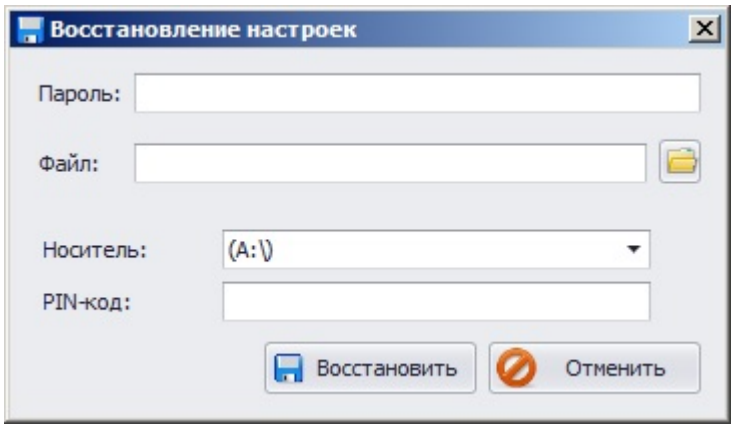


Рисунок 3.6. Окно восстановления настроек сервера СЗИ

В результате на текущем сервере СЗИ будут восстановлены все настройки серверной части СЗИ и список контролируемых рабочих станций-клиентов СЗИ, выбрав пункт меню ***Главная →Сохранить все.***

Для вступления измененных настроек СЗИ в силу необходимо перегрузить ОС.

При переносе настроек с одного сервера безопасности на другой действия по восстановлению настроек нужно производить на сервере, на который переносятся настройки СЗИ.

3.2.1.3. Резервное копирование и восстановление настроек СЗИ рабочей станции

Резервное копирование настроек СЗИ контролируемой рабочей станции подразумевает сохранение в зашифрованном файле текущих настроек механизмов СЗИ данной рабочей станции (подключенной к данному серверу).

Резервное копирование настроек СЗИ контролируемой рабочей станции выполняется в зашифрованный на пароле файл настроек (*.set) с помощью пункта меню ***Резервирование →Резервирование настроек клиента*** серверной консоли СЗИ.

Для выполнения резервного копирования настроек СЗИ рабочей станции необходимо в серверной консоли администрирования:

1) выделить в окне **«Список машин»** рабочую станцию, настройки СЗИ которой будут резервироваться;
2) выбрать пункт меню ***Резервирование →Резервирование настроек клиента***;
3) в открывшемся окне **«Сохранение настроек»** (см. рис. 3.4):

- в поле ***Пароль*** ввести пароль, с использованием которого будет зашифрован файл настроек сервера СЗИ;
- нажав на кнопку ***Выбор пути*** указать, в открывшемся стандартном окне Windows **«Сохранить как»**, каталог размещения и имя файла, в котором будут зарезервированы настройки;
- нажать кнопку ***Сохранить***.

В результате в указанном каталоге будет создан файл, в котором в зашифрованном виде будут записаны текущие настройки СЗИ рабочей станции.

При необходимости восстановления настроек СЗИ рабочей станции следует в серверной консоли администрирования:

1) выделить в окне **«Список машин»** рабочую станцию, настройки СЗИ которой будут восстанавливаться;
2) выбрать пункт меню ***Резервирование →Восстановление настроек клиента***;
3) в открывшемся окне **«Восстановление настроек»** (рис. 3.7):

- в поле ***Пароль*** ввести пароль, с использованием которого был зашифрован файл настроек рабочей станции-клиента СЗИ;
- указать имя и каталог размещения файла, в котором были зарезервированы настройки. Указать имя файла настроек можно введя полный путь к файлу в поле ***Файл*** вручную, или нажав кнопку ***Выбор пути***, указать файл в открывшемся стандартном окне Windows **«Открыть»**;
- нажать кнопку ***Восстановить***.

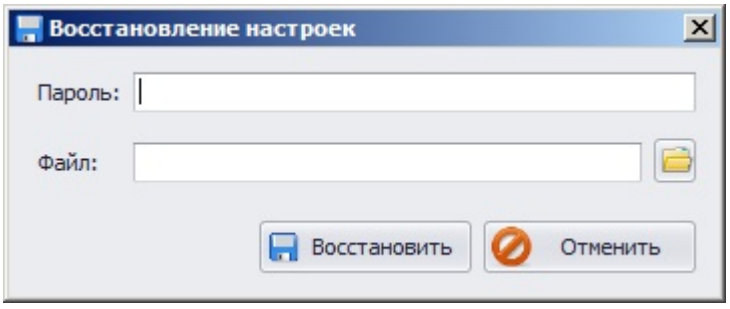


Рисунок 3.7. Окно восстановления настроек СЗИ на контролируемой рабочей станции

Запрещается при помощи механизма резервного копирования настроек СЗИ переносить настройки СЗИ с одной контролируемой рабочей станции на другую.

3.2.2. Дочерние окна консоли администрирования

Все дочерние окна консоли администрирования СЗИ можно переместить в любую часть основного окна консоли. Для перемещения окна необходимо захватить его заголовок левой кнопкой мыши и переместить на необходимый элемент расположения:

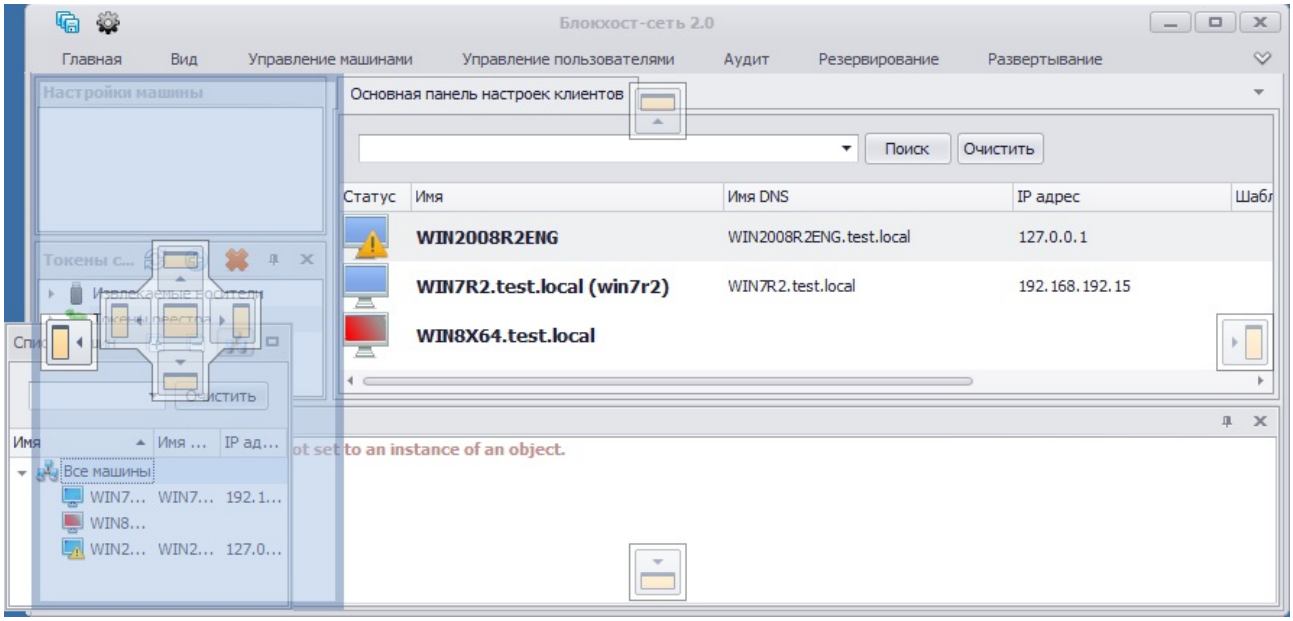


Рисунок 3.8. Перемещение дочерних окон в окне консоли администрирования

При нажатии на кнопку ***Скрывать автоматически*** окна **«Токены…»** и **«Лог»** можно свернуть – при этом вкладка, при наведении указателя мыши на которую окно раскроется, будет привязана к левой (для окна **«Токены…»**) или нижней (для окна **«Лог»**) границе окна консоли администрирования СЗИ.

Для отображения или закрытия дочернего окна необходимо, соответственно, установить или снять флажок напротив имени соответствующего окна в меню ***Вид*** (рис. 3.9). Для закрытия окон **«Токены…»** и **«Лог»** можно также воспользоваться кнопкой закрытия окна, которая располагается в правом верхнем углу окна.

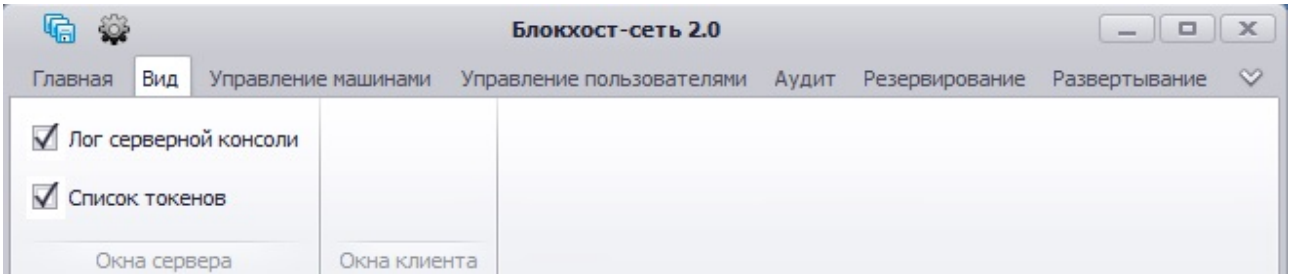


Рисунок 3.9. Меню «Вид» серверной консоли администрирования СЗИ

Переход между окнами (вкладками) серверной консоли администрирования СЗИ возможен с использованием «горячих» клавиш. После нажатия комбинации клавиш **<Ctrl>+<Tab>** открывается окно перехода между окнами (вкладками) серверной консоли администрирования СЗИ (рис. 3.10). Для перехода в нужное окно или вкладку необходимо при нажатой клавише **<Ctrl>** стрелками «вправо» или «влево» выбрать необходимую категорию: окно или вкладку, а затем стрелками «вверх», «вниз» или клавишей **<Tab>** выбрать нужную вкладку или окно.

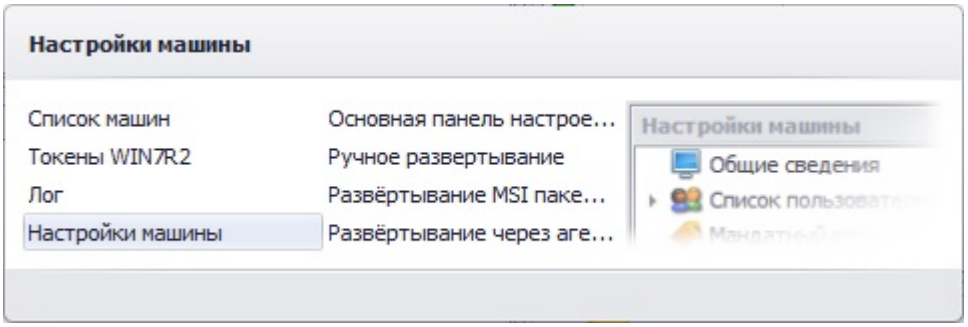


Рисунок 3.10. Перемещение между окнами (вкладками) с использованием «горячих» клавиш

Внутри окон (вкладок) серверной консоли также возможно использование «горячих» клавиш. Использование сочетания клавиш **<Ctrl>+** стрелка «вправо» или «влево» позволит, соответственно, развернуть или свернуть узел (список машин, настройки СЗИ, деревья файловых объектов, usb-устройства) в выбранном окне консоли.

3.2.2.1. Окно «Список машин»

В окне **«Список машин»** (рис. 3.11) отображаются все рабочие станции, контролируемые на текущем сервере безопасности СЗИ. Рабочие станции могут быть добавлены в список контролируемых данным сервером СЗИ различными, реализованными в меню ***Развертывание***, способами: ***Развертывание MSI пакетов***, ***Ручное развертывание***, ***Развертывание через агента*** (подробнее о формировании списка контролируемых рабочих станций на сервере СЗИ см. подраздел 3.3 настоящего документа).

В окне **«Список машин»** расположены следующие элементы управления:

- кнопка ***Показывать группы*** – предназначена для отображения созданных администратором безопасности групп рабочих станций;
- кнопки ***Раскрыть все узлы*** и ***Свернуть все узлы*** – предназначены, соответственно, для раскрытия списка сгруппированных рабочих станций или отображения только групп рабочих станций;
- поле ввода – предназначено для ввода значения критерия отбора рабочих станций из списка. Фильтрация рабочих станций в окне осуществляется автоматически – сразу же после ввода значения фильтра. Для осуществления корректной фильтрации рабочих станций необходимо, чтобы все группы рабочих станций были раскрыты – перед вводом критерия отбора в поле ввода необходимо нажать кнопку ***Раскрыть все узлы***;
- кнопка ***Очистить*** – очищает поле ввода от введенного значения фильтра.

Окно **«Список машин»** по умолчанию расположено в левой части окна консоли администрирования СЗИ.

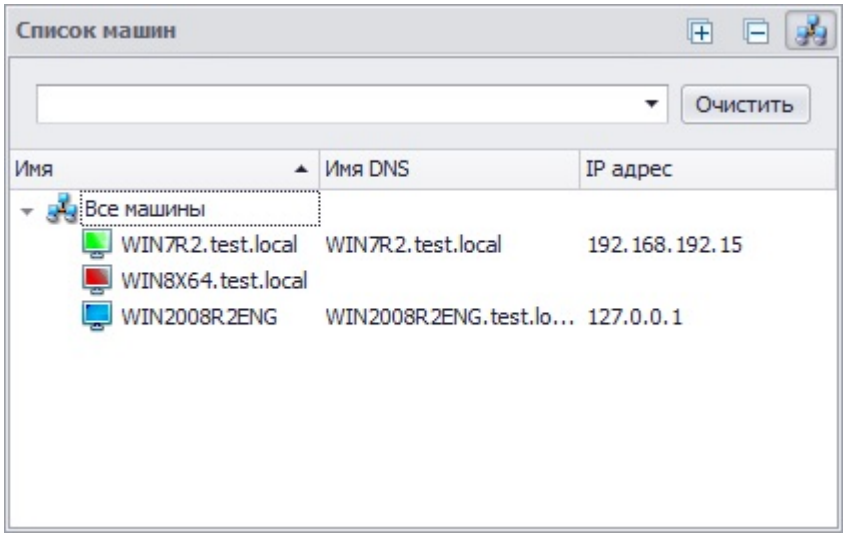


Рисунок 3.11. Окно «Список машин» серверной консоли администрирования СЗИ

3.2.2.2. Окно «Настройки машины»

В окне **«Настройки машины»** отображены настраиваемые механизмы разграничения доступа и защиты информации выбранной в окне **«Список машин»** рабочей станции:

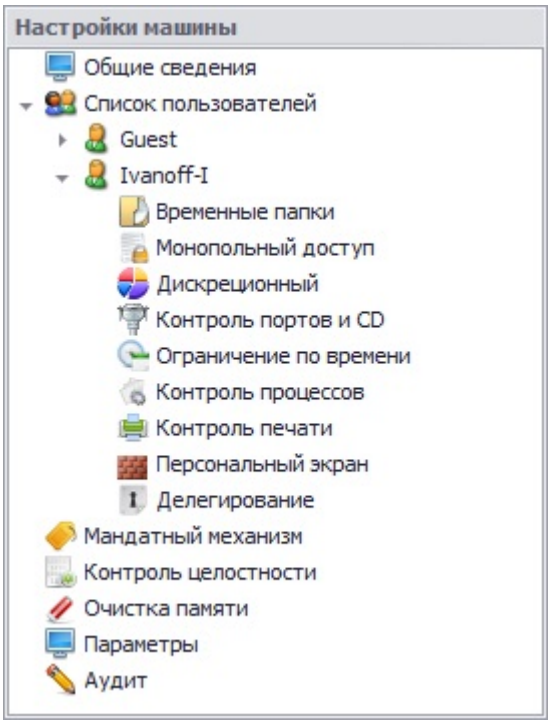


Рисунок 3.12. Окно «Настройки машины» серверной консоли администрирования СЗИ

3.2.2.3. Окно «Токены»

Заголовок и содержимое окна **«Токены»** (рис. 3.13) зависит от того, какой объект выделен в окне **«Список машин»**. Если в окне **«Список машин»** выделена группа (например, ***Все машины***), то заголовок окна **«Токены…»** принимает вид **«Токены сервера»**, а в окне отображаются, сгруппированные по типам, все подключенные к серверу СЗИ персональные идентификаторы. А если в окне **«Список машин»** выделена контролируемая рабочая станция, то заголовок окна **«Токены…»** принимает вид **«Токены <имя_рабочей_станции>»**, а в окне отображаются, сгруппированные по типам, все подключенные к контролируемой рабочей станции персональные идентификаторы.

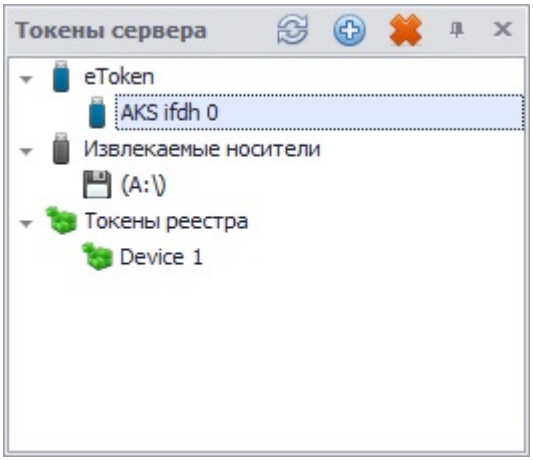


Рисунок 3.13. Окно «Токены…» серверной консоли администрирования СЗИ

В окне **«Токены…»** расположены следующие элементы управления:

- кнопка ***Обновить*** – позволяет обновить список подключенных к рабочей станции (серверу СЗИ) персональных идентификаторов;
- кнопка ***Создать токен в реестре*** – служит для создания персонального идентификатора в реестре ОС Windows, выбранной в окне **«Список машин»** рабочей станции;
- кнопка ***Удалить токен из реестра*** – служит для удаления персонального идентификатора в реестре ОС Windows, выбранной в окне **«Список машин»** рабочей станции.

При выборе носителя в окне **«Токены сервера»** возможна настройка его параметров во вкладке **Настройки токена** серверной консоли администрирования СЗИ (подробнее о настройке параметров персонального идентификатора во вкладке **Настройки токена** см. п. 6.2.5 «Механизм идентификаторов входа» настоящего руководства).

3.2.2.4. Окно «Лог»

В окне **«Лог»** отображается результат выполняемых администратором действий. Все сообщения выводимые в окно «Лог» также регистрируются в файле *short_log.log*, расположенном в каталоге *C:\BlockHost\ServerBPShell.New\Log*.

В случае запуска серверной консоли из командной строки с ключом ***-trace***, в окно **«Лог»** будут выводиться все информационные сообщения СЗИ. Также в этом случае все сообщения СЗИ будут записываться в файл *full_log.log*, расположенный в каталоге размещения программы (*C:\BlockHost\ServerBPShell.New\Log*).

3.2.3. Основная панель настроек клиентов

Основная панель настроек клиентов находится в правой части консоли администрирования и представляет собой вкладку, в которой отображаются настройки того механизма СЗИ, который выбран в окне **«Настройки машины»**. **Основная панель настроек клиентов** в зависимости от выбранного механизма СЗИ имеет различные элементы управления и вид отображаемой информации. На рисунке 3.14 приведен вид вкладки для настройки механизма контроля целостности и дискреционного разграничения доступа.

При отображении в **Основной панели настроек клиентов** списка пользователей удаленной рабочей станции, работающий в данный момент на ней пользователь, выделяется зеленым цветом.

Дерево ресурсов (список объектов файловой системы), расположенное в нижней части **Основной панели настроек клиентов** (см. рис. 3.13), предназначено для отображения ресурсов рабочей станции, к которым может быть применен механизм разграничения доступа или защиты информации, выбранный в окне **«Настройки машины»**. При необходимости применения настроек выбранного механизма к какому-либо объекту дерева ресурсов, администратору безопасности необходимо левой кнопкой мыши выбрать этот объект, после чего перетащить его в область настроек, не отпуская нажатую кнопку мыши.

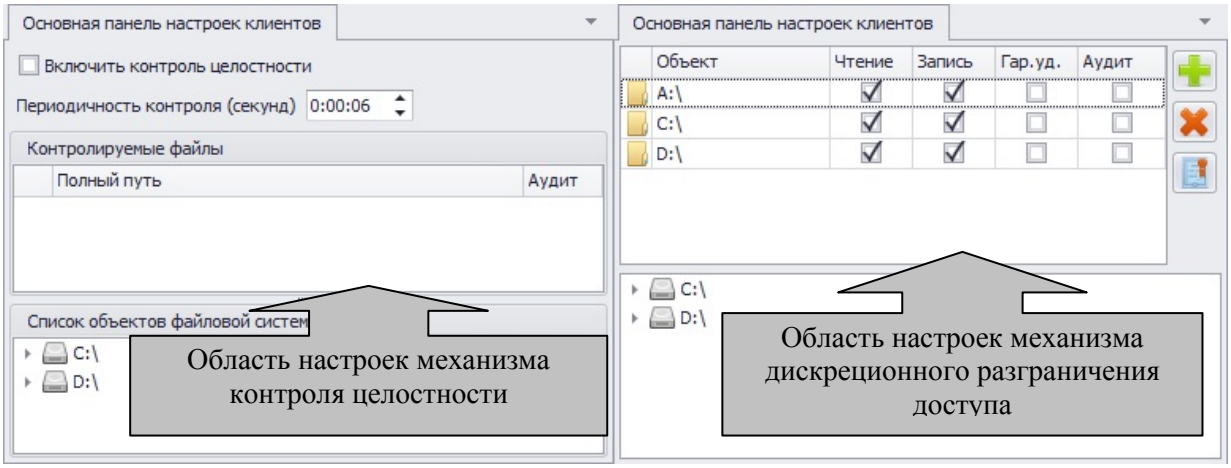


Рисунок 3.14. Настройки механизмов СЗИ в Основной панели настроек клиентов

Отображение списка объектов (ресурсов), находящихся в **Основной панели настроек клиентов**, можно настроить при помощи их группировки, отображения/скрытия столбцов, устанавливая критерии фильтра отбора объектов. Для настройки отображения списка объектов (ресурсов) служит контекстное меню, которое можно вызвать, щелкнув правой кнопкой мыши на имени любой колонки (столбца) в **Основной панели настроек клиентов**. Количество параметров настройки отображения объектов может различаться в зависимости от выбора настраиваемого механизма СЗИ, объекты которого отображены в **Основной панели настроек клиентов**. На рисунке 3.15 показано контекстное меню настройки отображения при выборе механизма настройки параметров пользователей (***Список пользователей***):

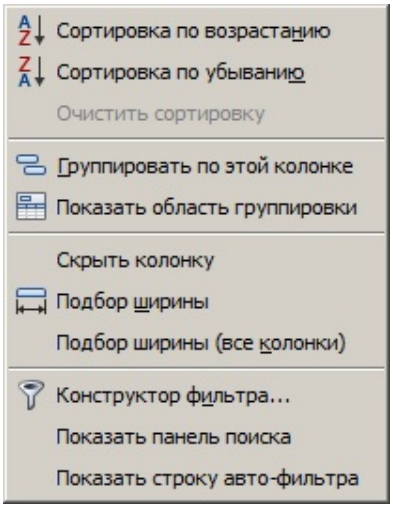


Рисунок 3.15. Контекстное меню настройки отображения списка объектов (ресурсов)

При помощи контекстного меню можно выполнить следующие настройки отображения списка объектов (ресурсов):

Сортировка по возрастанию, ***Сортировка по убыванию*** – позволяет отсортировать список объектов по возрастанию или убыванию (соответственно) по значению колонки, на которой было вызвано контекстное меню;

Очистить сортировку – возвращает отображение списка объектов к параметрам по умолчанию;

Группировать по этой колонке – осуществляется группировка списка объектов по значениям выбранной колонки. Имя колонки переносится в область группировки.

Показать область группировки – над заголовками колонок открывается область группировки, в которую можно перетащить левой кнопкой мыши заголовок колонки, устанавливая таким образом порядок группировки списка отображаемых объектов;

Скрыть колонку – скрывает отображение колонки, на которой было вызвано контекстное меню;

Подбор ширины – устанавливает ширину колонки, на которой было вызвано контекстное меню, в соответствии с ее содержимым;

Подбор ширины (все колонки) – устанавливает ширину всех колонок в соответствии с их содержимым;

Показать панель поиска – над именами колонок открывается поле ввода критериев отбора объектов из списка и кнопки ***Поиск*** и ***Очистить***. Проверка соответствия введенной в поле ввода маске осуществляется по значениям сразу всех колонок.

Конструктор фильтра – открывается окно **«Конструктор фильтра»** (рис. 3.16), в котором можно задать параметры, в соответствии с которыми будут отображены объекты.

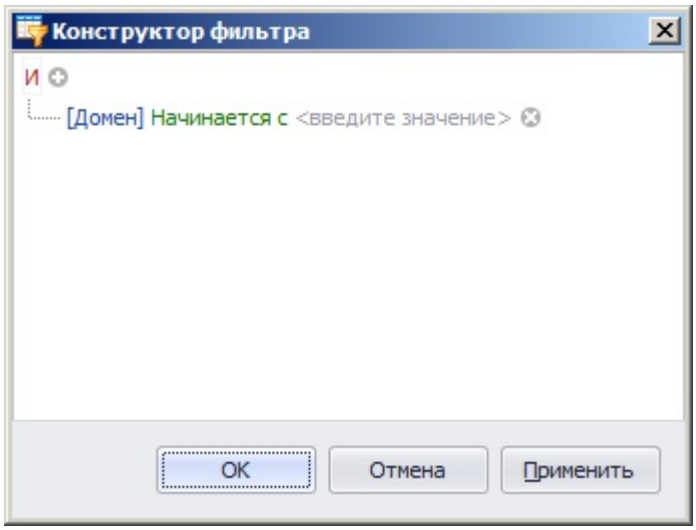


Рисунок 3.16. Окно конструктора фильтра отображения списка объектов

В окне **«Конструктор фильтра»** можно задать несколько условий фильтрации отображаемых в **Основной панели настроек клиентов** объектов. При помощи логических операторов **И**, **ИЛИ**, **НЕ И**, **НЕ ИЛИ** можно задать отношения между группами фильтров. Нажатие левой кнопкой мыши на логический оператор открывает контекстное меню, в котором можно изменить логический оператор, добавить новое условие фильтра, добавить новую группу условий или полностью очистить фильтр. Нажатие левой кнопкой мыши на имя колонки открывает контекстное меню, в котором можно изменить колонку, для которой устанавливается фильтр. Нажатие левой кнопкой мыши на оператор условия также открывает контекстное меню, в котором можно изменить этот оператор.

3.3. Формирование списка контролируемых рабочих станций

3.3.1. Алгоритм создания списка контролируемых рабочих станций

Для централизованного администрирования СЗИ «Блокхост-сеть 2.0» администратору безопасности необходимо:

1. Определить группу рабочих станций, которые будут централизованно управляться:

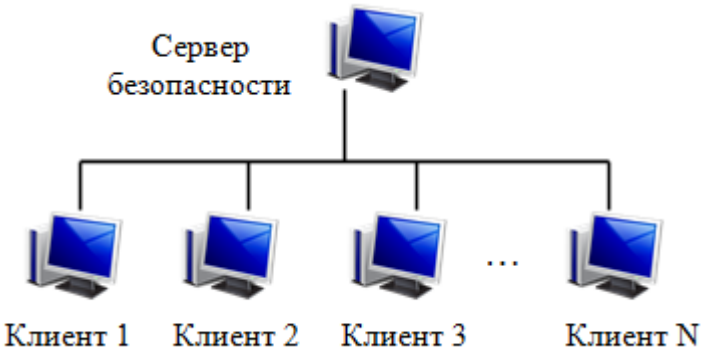


Рисунок 3.17. Группа рабочих станций

2. Установить серверную часть СЗИ «Блокхост-сеть 2.0» на рабочее место администратора безопасности (рис. 3.18) и с использованием ключевого носителя администратора и выполнить:

- сетевые настройки сервера СЗИ;
- создание списка защищаемых рабочих станций;
- генерацию ключей взаимной аутентификации клиентских и серверной частей СЗИ.

Процедура установки сервера СЗИ «Блокхост-сеть 2.0» на рабочее место администратора безопасности описана в руководстве по установке СЗИ «Блокхост-сеть 2.0».

Рисунок 3.18. Установка и настройка серверной части СЗИ на рабочем месте администратора

3. Установить клиентские части СЗИ «Блокхост-сеть 2.0» на защищаемые рабочие станции (локально или из серверной консоли администрирования СЗИ):

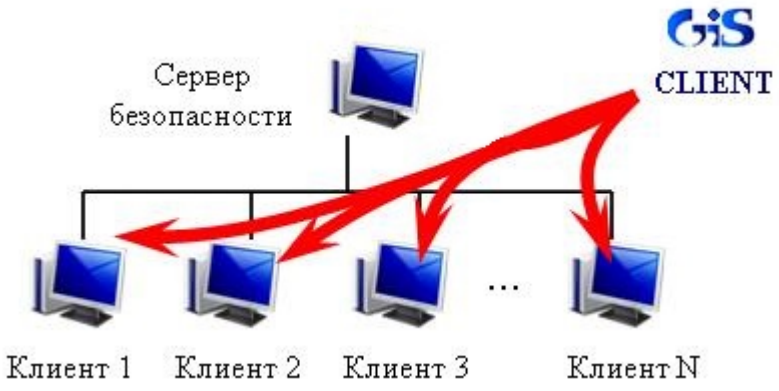


Рисунок 3.19. Рабочие станции, подключенные к серверу

При локальной установке клиентских частей СЗИ «Блокхост-сеть 2.0» на защищаемые рабочие станции администратор безопасности должен использовать один ключевой носитель (далее – ключевой носитель администратора). Данный ключевой носитель позволит выполнять локальное администрирование клиентской части СЗИ «Блокхост-сеть 2.0», создание и удаленное администрирование группы рабочих станций.

4. При ручной генерации рабочих станций в серверной консоли администрирования СЗИ экспортировать выполненные на сервере СЗИ настройки на отчуждаемый носитель:

Рисунок 3.20. Экспорт настроек на носитель

5. Импортировать и загрузить настройки на каждую из рабочих станций, сгенерированных в серверной консоли администрирования СЗИ:

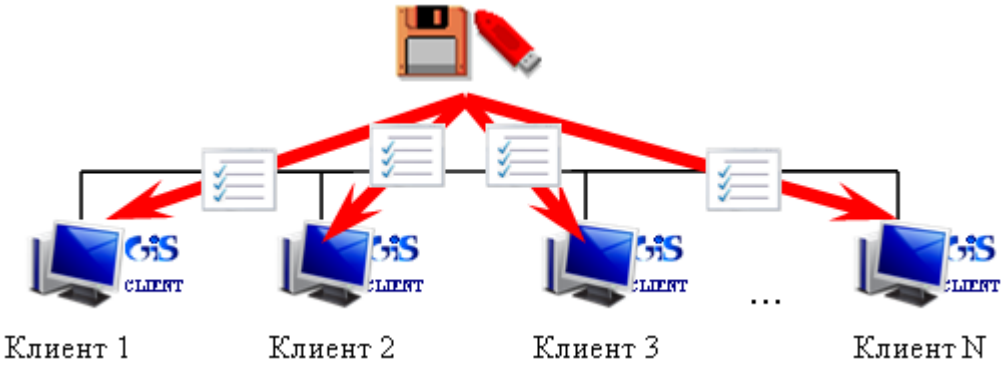


Рисунок 3.21. Импорт и загрузка настроек на защищаемые рабочие станции

При определении списка контролируемых рабочих станций администратору безопасности необходимо учесть, что при существовании пользователей с одинаковыми именами (в одноранговой сети) их одновременный доступ к ресурсам будет невозможен.

6. В результате безопасность информации на защищаемых рабочих станциях будет контролироваться сервером СЗИ:

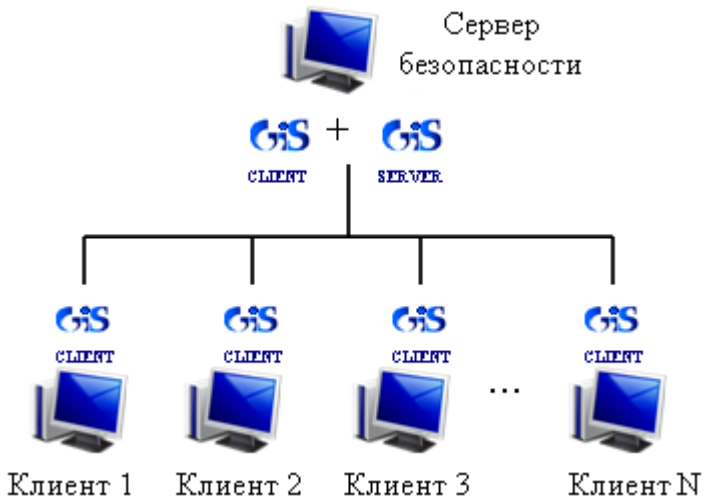


Рисунок 3.22. Контроль безопасности рабочих станций сервером СЗИ

3.3.2. Настройка серверной части СЗИ «Блокхост-сеть 2.0»

Настройка параметров сетевого взаимодействия сервера СЗИ с рабочими станциями, контролируемыми текущим сервером, выполняется администратором в серверной консоли СЗИ «Блокхост-сеть 2.0» в следующей последовательности:

1. В серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» нажать кнопку ***Настройка параметров сервера*** , расположенную в левом верхнем углу окна программы;
2. В открывшейся вкладке **Параметры сервера** (рис. 3.23) доступны для изменения следующие параметры:

- ***Идентификатор машины по умолчанию*** – в данном поле указывается идентификатор сервера СЗИ, с использованием которого будет устанавливаться подключение клиента к серверу СЗИ. Для возможности изменения данного параметра необходимо отметить пункт ***Редактировать***, расположенный за полем ввода идентификатора сервера;
- ***Пароль подключения клиента*** – в данном поле указывается пароль для подключения клиента к серверу СЗИ;
- ***Сетевой интерфейс сервера*** – в полях ***Имя (IP)*** и ***Порт*** указывается IP-адрес и номер TCP-порта сервера СЗИ, по которым будет происходить подключение клиентов СЗИ. Для возможности изменения данного параметра необходимо отметить пункт ***Редактировать***, расположенный за полем ввода номера порта сервера;
- ***Групповой адрес*** – в полях ***Имя (IP)*** и ***Порт*** указывается IP-адрес и номер UDP-порта групповой рассылки, осуществляемой сервером на контролируемые рабочие станции, в формате **<IP-адрес>:<порт>**. Изменять его не следует. В случае необходимости изменения данного параметра следует отметить пункт ***Редактировать***, расположенный за полем ввода номера порта клиента СЗИ;
- в области *Управление лицензиями* указаны сведения об используемых на сервере СЗИ лицензиях: количество используемых серверных лицензий, общее

и оставшееся количество клиентов, которых можно подключить к серверу СЗИ с использованием установленных серверных лицензий.

Для добавления новой лицензии необходимо ввести серийный номер и код лицензии в соответствующие поля и нажать кнопку ***Добавить***.

Для удаления используемой на сервере СЗИ лицензии необходимо выделить ее в списке используемых лицензий и нажать кнопку ***Удалить***.

3. Для сохранения изменений параметров сервера СЗИ нажать кнопку ***Сохранить*** во вкладке **Параметры сервера**.

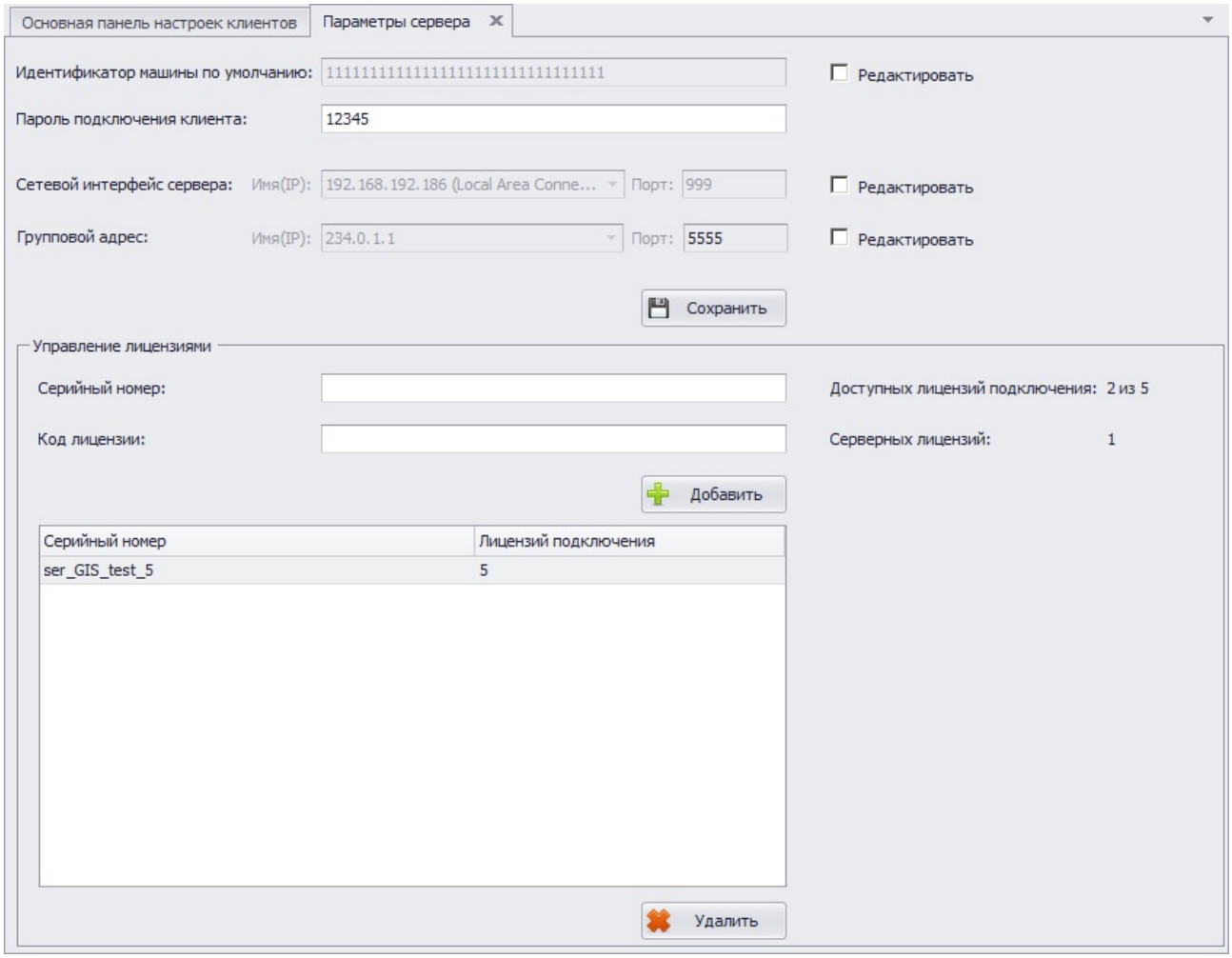


Рисунок 3.23. Настройка параметров сервера

3.3.3. Порядок формирования списка контролируемых рабочих станций

В серверной консоли СЗИ «Блокхост-сеть 2.0» можно добавить на текущий сервер СЗИ рабочие станции на контроль несколькими способами:

- из вкладки **Развертывание MSI пакетов**;
- из вкладки **Ручное развертывание**;
- из вкладки **Развертывание через агента**.

В общем случае процесс формирования списка контролируемых рабочих станций одинаков при добавлении их на сервер СЗИ из любой вкладки. Различие состоит лишь в способе распространения настроек серверной части СЗИ на эти рабочие станции. При наличии особенностей формирования списка контролируемых станций в какой-либо из вкладок, это будет отмечено особо.

Общий алгоритм действий администратора безопасности по формированию списка контролируемых рабочих станций включает в себя следующие шаги:

1. В серверной консоли СЗИ открыть одну из вкладок: **Развертывание MSI пакетов**, **Ручное развертывание** или **Развертывание через агента**. Открытие вкладки осуществляется путем выбора соответствующего пункта главного меню **Развертывание**:

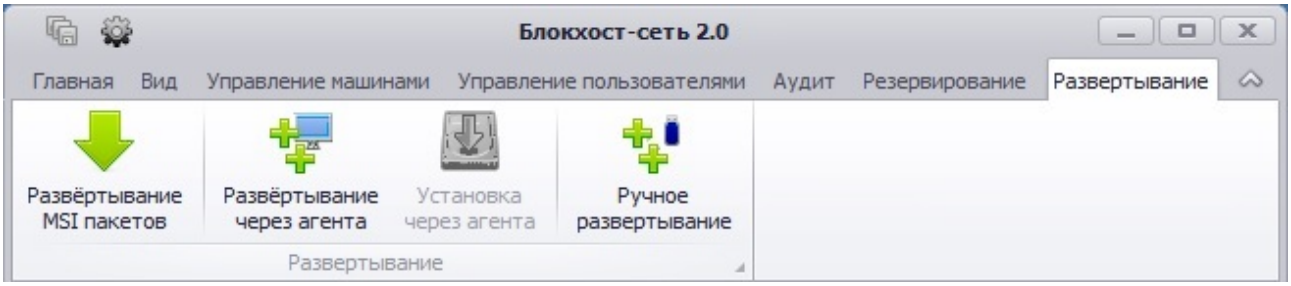


Рисунок 3.24. Меню «Развертывание»

Пункты меню ***Ручное развертывание***, ***Развертывание MSI пакетов*** и ***Развертывание через агента*** становятся активными в том случае, если в окне **«Список машин»** выделена группа, в которую будут добавлены новые рабочие станции. Пункт меню ***Установка через агента*** становится активным, если на сервер СЗИ добавлены рабочие станции из вкладки **Развертывание через агента**.

2. Сформировать в открытой вкладке список добавляемых на сервер СЗИ рабочих станций;

3. Добавить рабочие станции из сформированного списка на сервер СЗИ, нажав кнопку ***Добавить рабочие станции*** во вкладке **Ручное развертывание** или кнопку ***Добавить рабочие станции для развертывания*** во вкладке **Развертывание через агента**. Из вкладки **Развертывание MSI пакетов** рабочие станции будут добавлены в список контролируемых на сервере СЗИ после завершения на них процесса инсталляции клиентской части СЗИ и успешного запуска служб СЗИ.

3.3.3.1 Описание способов формирования на сервере СЗИ списка рабочих станций

Во вкладке **Ручное развертывание** (рис. 3.25) возможны четыре варианта формирования списка рабочих станций, которые будут контролироваться текущим сервером СЗИ:

- создать одну рабочую станцию;
- создать несколько рабочих станций с одинаковым префиксом;
- выбрать рабочие станции из списка объектов Active Directory;
- выбрать рабочие станций на основе данных сервера DNS.

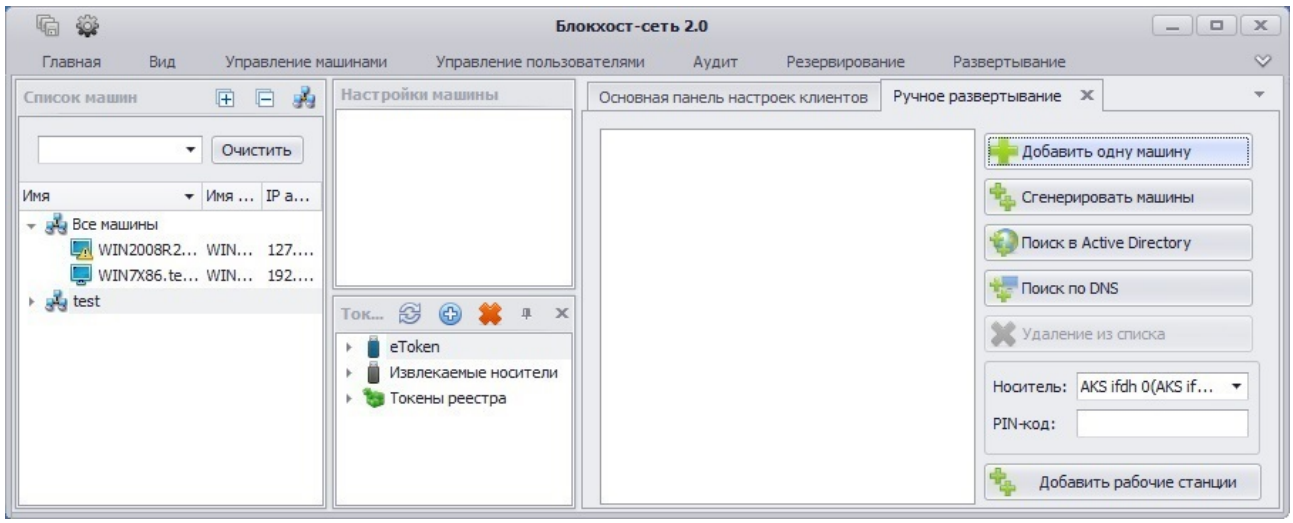


Рисунок 3.25 Вкладка «Ручное развертывание»

Во вкладках **Развертывание через агента** (рис. 3.26) и **Развертывание MSI пакетов** (рис. 3.27), в отличие от вкладки **Ручное развертывание**, отсутствуют варианты генерации машин (одной или диапазона), но добавлена возможность поиска рабочих станций в подсети по IP-адресу:

- выбор рабочих станций на основе IP-адреса;
- выбор рабочих станций из списка объектов Active Directory;
- выбор рабочих станций на основе данных сервера DNS.

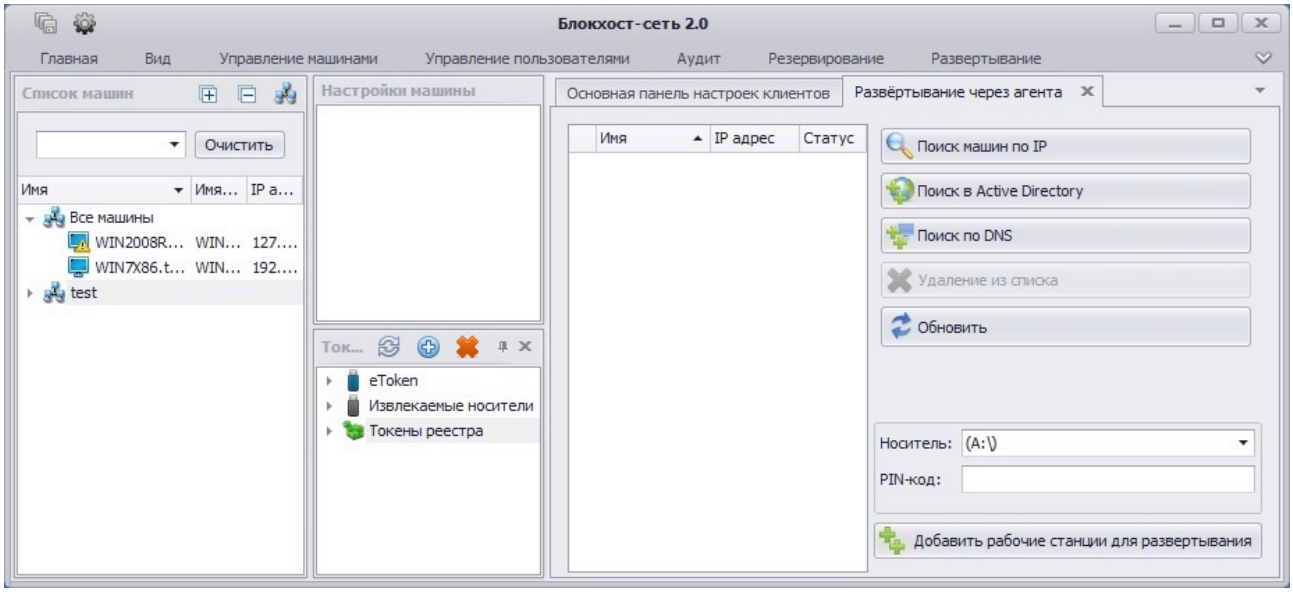


Рисунок 3.26. Вкладка «Развертывание через агента»

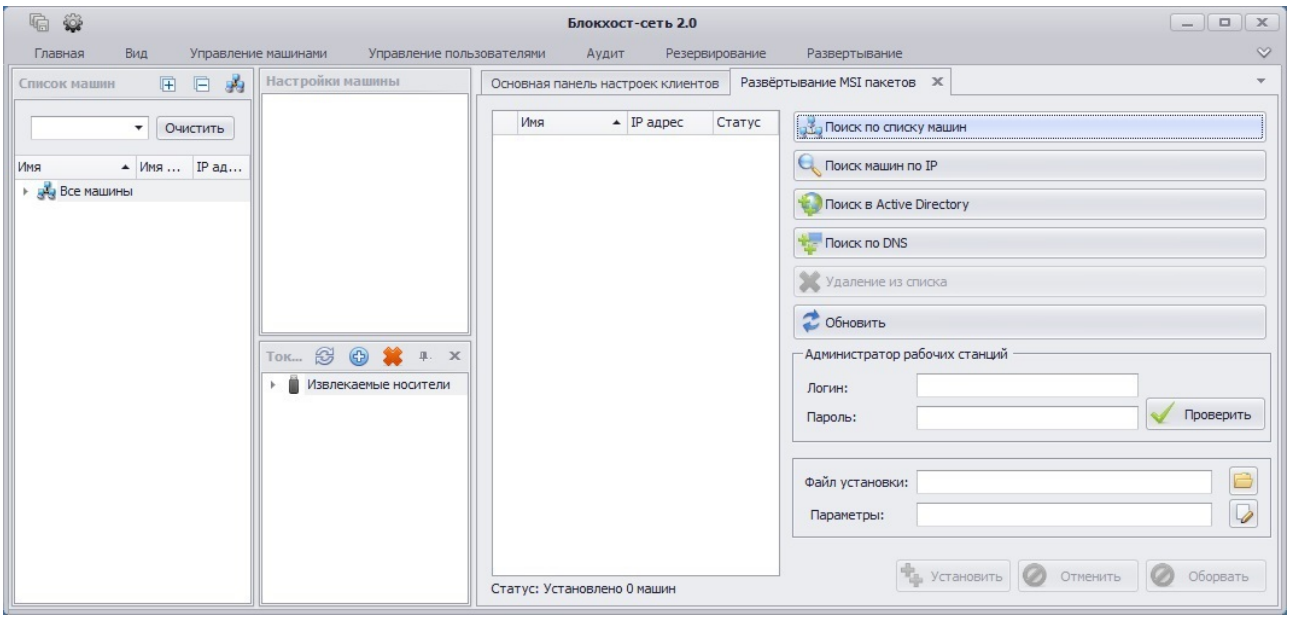


Рисунок 3.27. Вкладка «Развертывание MSI пакетов»

Кнопка ***Поиск по списку машин***, расположенная во вкладке **Развертывание MSI пакетов**, предназначена для формирования во вкладке списка рабочих станций – клиентов СЗИ, уже зарегистрированных на текущем сервере, для установки на них обновлений программного обеспечения СЗИ.

Дальнейшая работа по формированию списка рабочих станций и их добавления на сервер СЗИ осуществляется из соответствующей вкладки.

3.3.3.2 Генерация рабочих станций в серверной консоли СЗИ

В СЗИ «Блокхост-сеть 2.0» идентификация рабочей станции на сервере СЗИ происходит с использованием значений идентификатора рабочей станции (*Machine ID*) и имени рабочей станции на сервере СЗИ (*Name Value*). Процесс генерации рабочей станции на сервере СЗИ подразумевает под собой создание объекта (рабочей станции) и присвоение ему уникального идентификатора и имени. Идентификатор создаваемому объекту присваивается автоматически. Имя администратор безопасности назначает сам, в соответствии с принятыми в организации правилами. Значения идентификаторов и имен контролируемых рабочих станций хранится в зашифрованном виде в файле настроек: на сервере СЗИ (*ServerSettingsEncoded.set*), на локальной рабочей станции (*SettingsEncoded.set*)

Генерация контролируемых рабочих станций в серверной консоли СЗИ возможна во вкладке **Ручное развертывание**:

1. Для генерации одной рабочей станции нажать кнопку ***Добавить одну машину*** (см. рис. 3.25). В результате рабочая станция с именем *Machine 1* появится в соответствующей вкладке (префикс *Machine* используется по умолчанию и может быть изменен в окне **«Добавление диапазона клиентов»** (см. рис. 3.28)). Для изменения имени созданной рабочей станции следует один раз щелкнуть по нему левой кнопкой мыши – оно сразу будет выделено, – и ввести необходимое имя контролируемой рабочей станции.

2. Для генерации сразу нескольких рабочих станций необходимо нажать кнопку ***Сгенерировать машины*** (см. рис. 3.25). В результате откроется окно **«Добавление диапазона клиентов»** (рис. 3.28), в котором в поле ***Шаблон имени клиентов*** следует ввести общую часть имени генерируемых рабочих станций (по умолчанию используется префикс *Machine*) и задать необходимое количество генерируемых машин в поле ***Количество***

клиентов. После того, как все поля заполнены необходимо нажать кнопку ***Добавить***. В результате в соответствующей вкладке появится заданное количество рабочих станций.

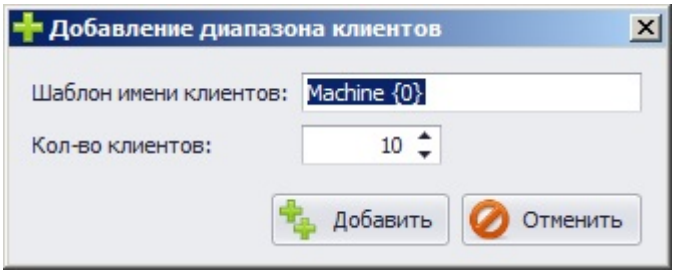


Рисунок 3.28 Окно «Добавление диапазона клиентов»

При вводе общей части имени клиентов СЗИ в окне **«Добавление диапазона клиентов»** следует учесть, что символы **{0}** должны присутствовать и оставаться неизменными в шаблоне имени рабочей станции. Изменять можно шаблон имени до и после этих символов. Например: *NWR{0}spb, CFO{0}msk, BUX{0}*.

Не допускается использовать символы фигурных скобок **{}** в качестве составляющих имени рабочей станции.

При выполнении нескольких операций генерации рабочих станций с использованием единого префикса, нумерация генерируемых станций начинается с последнего номера имени сгенерированной рабочей станции, имеющей аналогичный префикс.

3.3.3.3 Выбор рабочих станций из списка объектов Active Directory

Для добавления на сервер СЗИ рабочих станций из списка объектов Active Directory следует во вкладках **Развертывание MSI пакетов**, **Ручное развертывание** или **Развертывание через агента** нажать кнопку ***Поиск в Active Directory*** (см. рис. 3.25 – 3.27), в результате откроется окно **«Добавление клиентов из Active Directory»** (рис. 3.29). В окне **«Добавление клиентов из Active Directory»** необходимо выбрать требуемый домен, щелкнув по его имени левой кнопкой мыши, и авторизоваться в нем, для чего ввести логин и пароль пользователя домена в соответствующие поля открывшегося окна (рис. 3.30), затем нажать кнопку ***Подключить***.

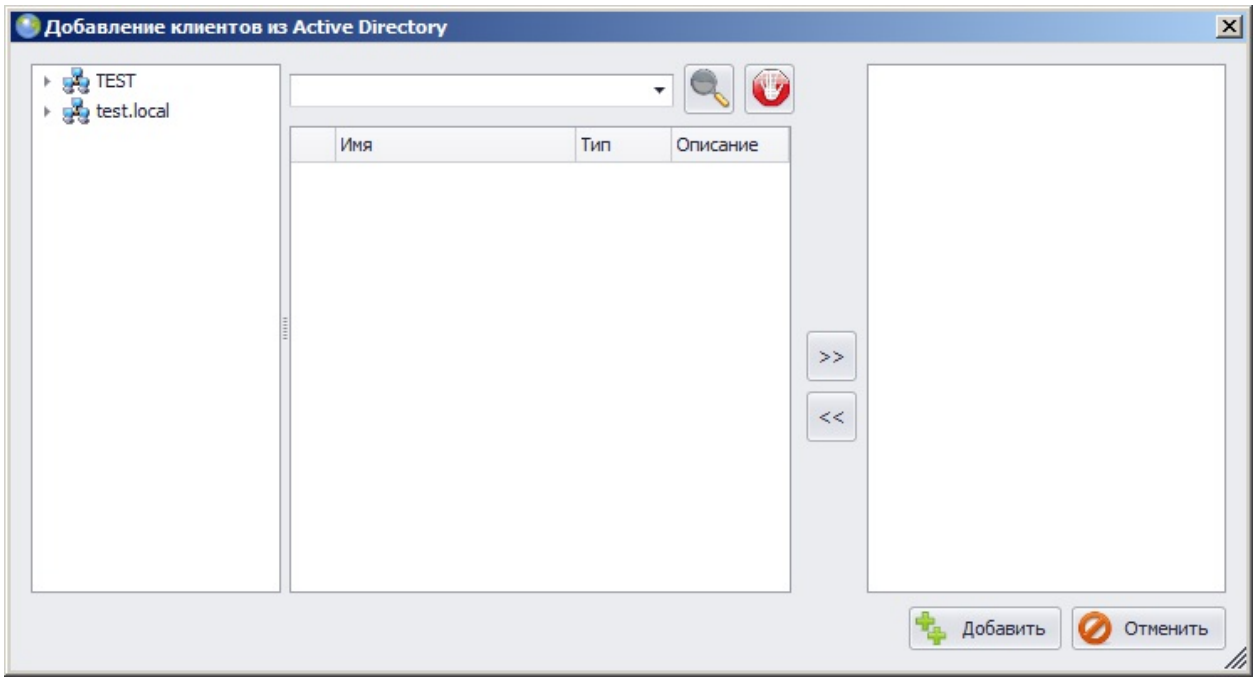


Рисунок 3.29. Окно поиска рабочих станций в структуре Active Directory

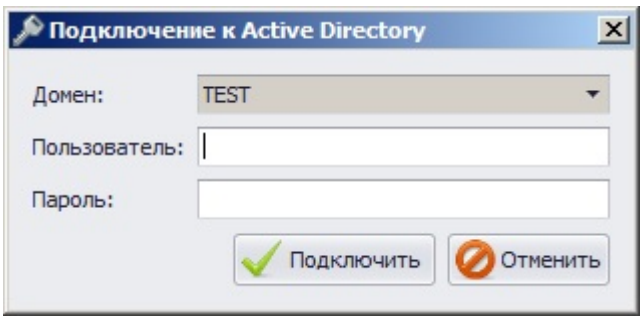


Рисунок 3.30. Окно «Подключение к Active Directory»

В отобразившейся в окне **«Добавление клиентов из Active Directory»** структуре объектов Active Directory выделить контейнер, содержащий добавляемые рабочие станции (в примере на рис. 3.31 – это контейнер ***Computers***), в средней части окна выделить необходимые рабочие станции (для выделения нескольких рабочих станций можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и с помощью кнопки >> переместить их в правую часть окна, затем нажать кнопку ***Добавить***.

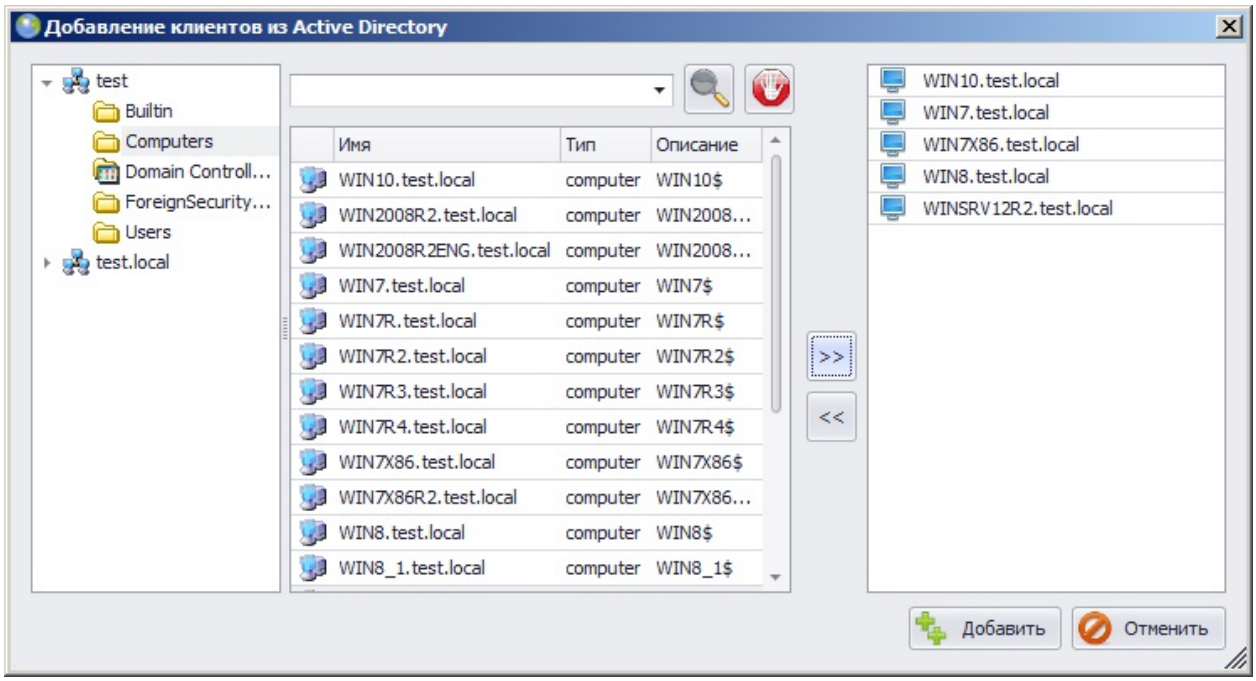


Рисунок 3.31. Сформированный список рабочих станций в окне выбора из AD

В результате выбранные рабочие станции появятся во вкладке, из которой производился процесс выбора рабочих станций из списка объектов Active Directory.

3.3.3.4 Поиск рабочих станций на основе данных сервера DNS

Для выбора рабочих станций на основе данных сервера DNS необходимо во вкладках **Развертывание MSI пакетов**, **Ручное развертывание** или **Развертывание через агента** нажать кнопку ***Поиск по DNS*** (см. рис. 3.25 – 3.27), в результате откроется окно **«Добавление клиентов на основе DNS-имен»** (рис. 3.32), в котором отображаются все включавшиеся за время работы сервера DNS рабочие станции. В списке доступных для выбора следует выбрать необходимые рабочие станции (для выделения нескольких рабочих станций можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и при помощи кнопок управления (>> и <<) сформировать список для добавления на сервер СЗИ, затем нажать кнопку ***Добавить***.

Использование параметра ***Поиск по DNS*** подразумевает наличие не более 100 рабочих станций в домене.

Значение, введенное в поле ввода окна **«Добавление клиентов на основе DNS-имен»**, позволяет осуществить фильтрацию списка найденных рабочих станций.

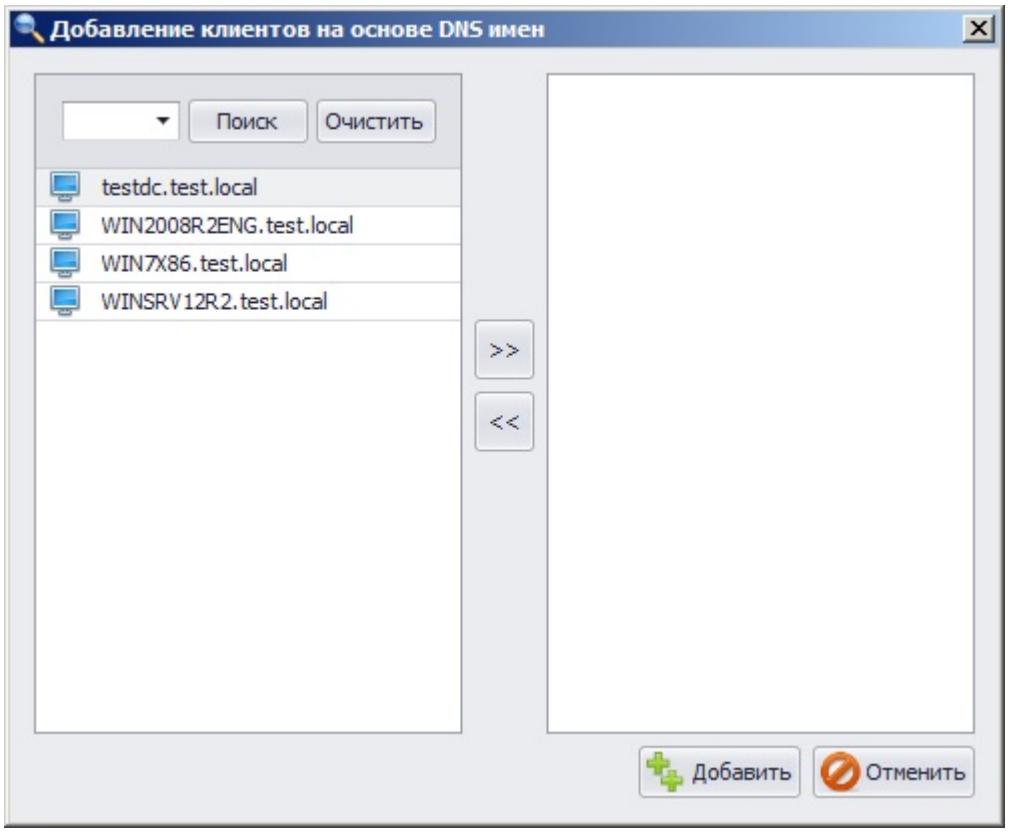


Рисунок. 3.32 Окно «Добавление клиентов на основе DNS имен»

В результате выбранные рабочие станции появятся во вкладке, из которой был запущен процесс выбора рабочих станций на основе данных сервера DNS.

3.3.3.5 Поиск рабочих станций по IP-адресу

Возможность выбора рабочих станций сети на основе их IP-адреса есть во вкладках **Развертывание через агента** и **Развертывание MSI пакетов**.

Для поиска компьютеров в подсети администратору безопасности необходимо в серверной консоли администрирования:

1. Перейти во вкладку **Развертывание через агента (Развертывание MSI пакетов)**;
2. Нажать кнопку ***Поиск машин по IP***;
3. В открывшемся окне **«Поиск машин с агентом развертывания»** (рис. 3.33) или **«Поиск машин в сети»** (для вкладок **Развертывание через агента** и **Развертывание MSI пакетов**, соответственно. Окна поиска рабочих станций по IP-адресу, открываемые из этих вкладок, различаются между собой только заголовками):
   - в поле ***Адрес подсети*** ввести IP-адрес (либо диапазон IP-адресов в формате 192.168.0.* или 192.168.0.1-50);

     В случае ввода неверного IP-адреса (диапазона IP-адресов) рядом с полем ввода появится пиктограмма ошибки, а в окне **«Лог»** появится сообщение *Неверный формат адреса рассылки*.

- нажать кнопку ***Поиск***.

> В окне **«Поиск машин в сети»** осуществляется поиск всех включенных в момент выполнения запроса рабочих станций сети. В окне **«Поиск машин с агентом развертывания»** осуществляется поиск только тех рабочих станций, на которых работает агент системы развертывания СЗИ.

- После успешного завершения поиска выделить в списке найденных рабочих станций необходимые и нажать кнопку ***Добавить***.

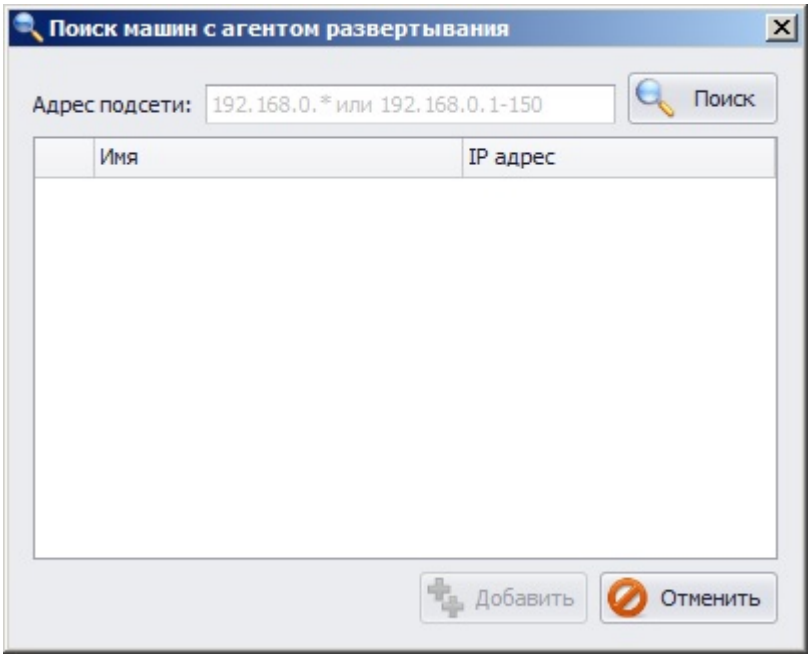


Рисунок 3.33. Окно поиска машин с агентом развертывания

В результате выбранные рабочие станции появятся во вкладке, из которой был запущен процесс поиска рабочих станций по IP-адресу.

3.3.3.6 Добавление рабочих станций на сервер СЗИ

Для добавления на сервер СЗИ, найденных или сгенерированных рабочих станций, необходимо во вкладке **Ручное развертывание** нажать кнопку ***Добавить рабочие станции***, а во вкладке **Развертывание через агента** – кнопку ***Добавить рабочие станции для развертывания***. В результате, добавленные рабочие станции отобразятся в окне **«Список машин».**

> Во вкладках **Ручное развертывание** и **Развертывание через агента** перед добавлением рабочих станций на сервер СЗИ, необходимо подключить к серверу ключевой носитель, на который будут записаны ключи взаимной аутентификации, и ввести PIN-код доступа к нему.

Из вкладки **Развертывание MSI пакетов** рабочие станции автоматически добавляются в список контролируемых сервером СЗИ сразу после завершения установки на них клиентской части СЗИ.

3.3.4. Экспорт сетевых настроек

Настройка сетевых параметров рабочих станций, добавляемых в группу контролируемых, выполняется администратором безопасности в серверной консоли СЗИ «Блокхост-сеть 2.0» в следующей последовательности:

1. В окне **«Список машин»** выделить пункт ***Все машины***;
2. В меню ***Развертывание*** выбрать пункт ***Ручное развертывание*** (рис. 3.24). Откроется вкладка **Ручное развертывание** (рис. 3.25);
3. Во вкладке **Ручное развертывание** сформировать список рабочих станций, для которых будет производиться экспорт параметров сетевого взаимодействия (подробнее о создании списка контролируемых рабочих станций см. подраздел 3.3.3 настоящего руководства);
4. Подключить к серверу СЗИ ключевой носитель, на который будет осуществлен экспорт сетевых настроек и ключей аутентификации клиента, и выбрать его из выпадающего списка поля ***Носитель***;

1. Для экспорта сетевых настроек сервера СЗИ и ключей аутентификации клиента может быть использован носитель, отличный от того, с которым производилась установка серверной и клиентских частей СЗИ.
2. Следует учесть, что, если при установке серверной части СЗИ в качестве ключевого носителя был использован персональный идентификатор в реестре Windows, то для экспорта сетевых настроек сервера безопасности необходимо использовать другой вид носителя, например, eToken. Персональный идентификатор в реестре не предназначен для переноса настроек и может применяться только на той рабочей станции, на которой он был создан.

5. В поле ***PIN-код*** ввести PIN-код доступа к выбранному носителю;
6. Для записи сетевых настроек и ключей взаимной аутентификации удаленных рабочих станций на выбранный ключевой носитель нажать кнопку ***Добавить рабочие станции***.

После этого сетевые настройки и ключи взаимной аутентификации сервера СЗИ и рабочих станций будут созданы и экспортированы на ключевой носитель администратора, а в окне **«Список машин»** появятся рабочие станции, список которых был сформирован во вкладке **Ручное развертывание**.

Необходимо учитывать, что количество генерируемых ключей аутентификации клиентов СЗИ ограничено размерами носителя (например, на eToken Pro 32K можно сгенерировать ключи аутентификации приблизительно для 100 машин). Если необходимо подключать к серверу СЗИ большее количество машин, то по мере подключения рабочих станций к серверу СЗИ можно добавлять ключи аутентификации для новых машин на тот же самый носитель, либо использовать дополнительный носитель, в остальном процедура экспорта сетевых настроек сервера и ключей аутентификации клиента аналогична.

3.3.5. Импорт сетевых настроек на рабочие станции

Импорт сетевых настроек осуществляется непосредственно на рабочих станциях с ключевого носителя, на который из вкладки **Ручная генерация** серверной консоли администрирования СЗИ выполнялся экспорт сетевых настроек и ключей аутентификации клиента. Для импорта сетевых настроек администратор безопасности должен выполнить следующие действия:

1. Подключить к рабочей станции, для которой осуществляется импорт настроек, ключевой носитель администратора, на который были экспортированы сетевые настройки;
2. Войти в ОС от имени учетной записи встроенного администратора и запустить локальную консоль администрирования СЗИ «Блокхост-сеть 2.0»;

3. В локальной консоли администрирования СЗИ выбрать пункт ***Сетевые настройки*** раскрыв дерево списка объектов (***Рабочие станции →localhost → Сетевые настройки***);

Если данный пункт отсутствует в локальной консоли, значит при установке клиентской части СЗИ «Блокхост-сеть 2.0» не была введена сетевая лицензия или вход в ОС был осуществлен не от имени учетной записи встроенного администратора. Для добавления сетевой лицензии необходимо в локальной консоли администрирования выбрать пункт меню ***? → О программе***, и в открывшемся окне (рис. 3.34), напротив поля ***Серийный номер сетевой установки*** нажать кнопку ***Сменить***. В появившемся окне ввести код сетевой лицензии и код активации.

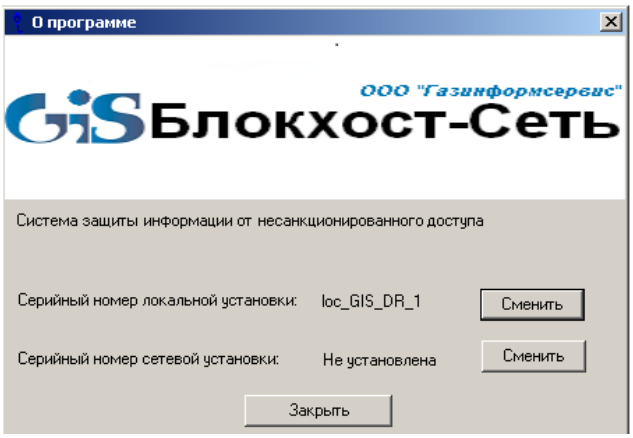


Рисунок 3.34. Пункт меню «О программе»

4. В области настроек в выпадающем списке поля ***Вид носителя*** выбрать тип ключевого носителя и ввести PIN-код доступа к нему в поле ***PIN-код*** (рис. 3.35);

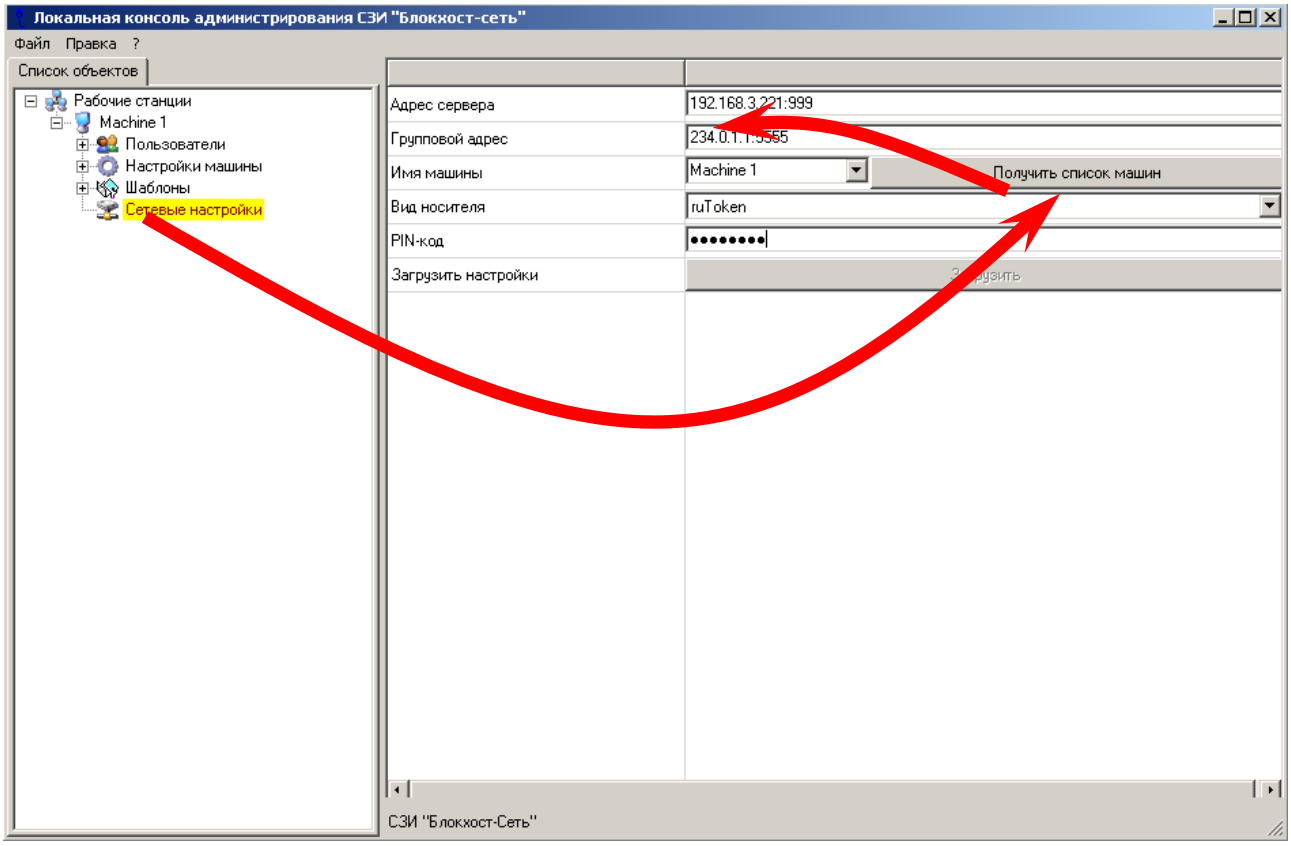


Рисунок 3.35. Импорт сетевых настроек

5. В области настроек нажать кнопку ***Получить список машин***;

6. Из выпадающего списка поля ***Имя машины*** выбрать имя сгенерированной, во вкладке **Ручное развертывание** серверной консоли, рабочей станции;

7. Загрузить настройки сервера СЗИ и рабочей станции, нажав кнопку ***Загрузить***;

Поля ***Адрес сервера*** и ***Групповой адрес*** заполняются автоматически на основе информации, содержащейся на ключевом носителе администратора (подробнее об этих параметрах см. п. 3.3.2 настоящего руководства). В дальнейшем, в ходе администрирования СЗИ «Блокхост-сеть 2.0» администратор безопасности может изменить значения в указанных полях (данная операция может потребоваться, если в сети параметры IP-адресации определяются автоматически).

8. Сохранить произведенные настройки с помощью пункта меню ***Файл →Сохранить настройки*** (либо с помощью сочетания клавиш <**Ctrl**>+<**S**>);

9. Аналогичные действия выполняются на всех рабочих станциях, которые необходимо подключить к серверу СЗИ.

3.4. Удаленная установка СЗИ «Блокхост-сеть 2.0»

В серверной консоли администрирования СЗИ существует возможность установки программного обеспечения (в частности, компонентов СЗИ «Блокхост-сеть 2.0») на удаленные рабочие станции с использованием дистрибутива поставляемого в виде файлов установщика Windows (*.msi*). Корректная установка ПО на удаленные рабочие станции из серверной консоли администрирования СЗИ происходит, если выполняются следующие условия:

- на удаленной рабочей станции должен быть включен ***Общий доступ к файлам и принтерам***. Включение ***Общего доступа к файлам и принтерам*** осуществляется в **Центре управления сетями и общим доступом** (пункт ***Изменить дополнительные параметры общего доступа***) для используемого сетевого профиля;
- msi-файл дистрибутива устанавливаемого программного обеспечения является «монолитным», то есть не требует в процессе инсталляции наличия в одном каталоге с установщиком дополнительных файлов дистрибутива ПО (*.cab*, *.zip* и др.);
- файл-установщик поддерживает «тихую установку», то есть установка программного обеспечения на удаленной рабочей станции должна производиться без участия пользователя и в скрытом (без диалоговых окон мастера установки) режиме.

Установка программного обеспечения из серверной консоли администрирования СЗИ заключается в последовательном выполнении следующих шагов:

- открыть вкладку **Развертывание MSI пакетов**;
- сформировать список рабочих станций сети, на которые будет осуществляться установка ПО;
- ввести идентификационные данные пользователя (члена группы **Администраторы** удаленной рабочей станции), от имени которого будет производиться установка;
- указать размещение файла-дистрибутива (файла-установщика с расширением *.msi) и, при необходимости, ввести параметры установки программного

обеспечения в соответствующее поле ввода;

- загрузить файл-установщик ПО на удаленную рабочую станцию, выполнив соответствующую команду в серверной консоли администрирования СЗИ.

3.4.1. Установка клиентской части СЗИ «Блокхост-сеть 2.0»

Для установки клиентской части СЗИ «Блокхост-сеть 2.0» на удаленные рабочие станции из серверной консоли администратору безопасности необходимо:

1. В окне **«Список машин»** выделить пункт ***Все машины***;
2. Выбрать пункт главного меню ***Развертывание →Развертывание MSI пакетов*** (см. рис. 3.24) – откроется вкладка **Развертывание MSI пакетов**:

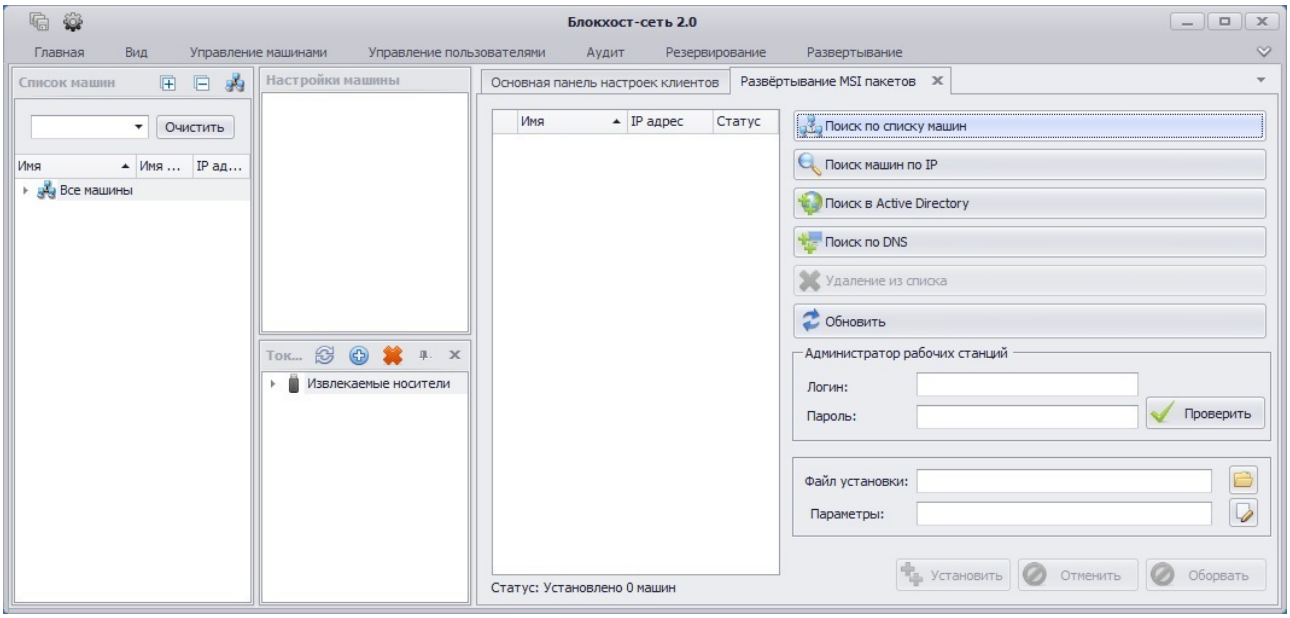


Рисунок 3.36. Вкладка «Развертывание MSI пакетов»

3. Сформировать список рабочих станций для установки клиентской части СЗИ (подробнее о способах формирования списка рабочих станций см. подраздел 3.3.3 настоящего руководства).

   После добавления рабочих станций в список для установки клиентской части СЗИ, они отобразятся во вкладке **Развертывание MSI пакетов** (рис. 3.37). Рабочие станции, недоступные в настоящий момент для установки будут иметь статус *Не в сети* и подсвечены красным цветом.

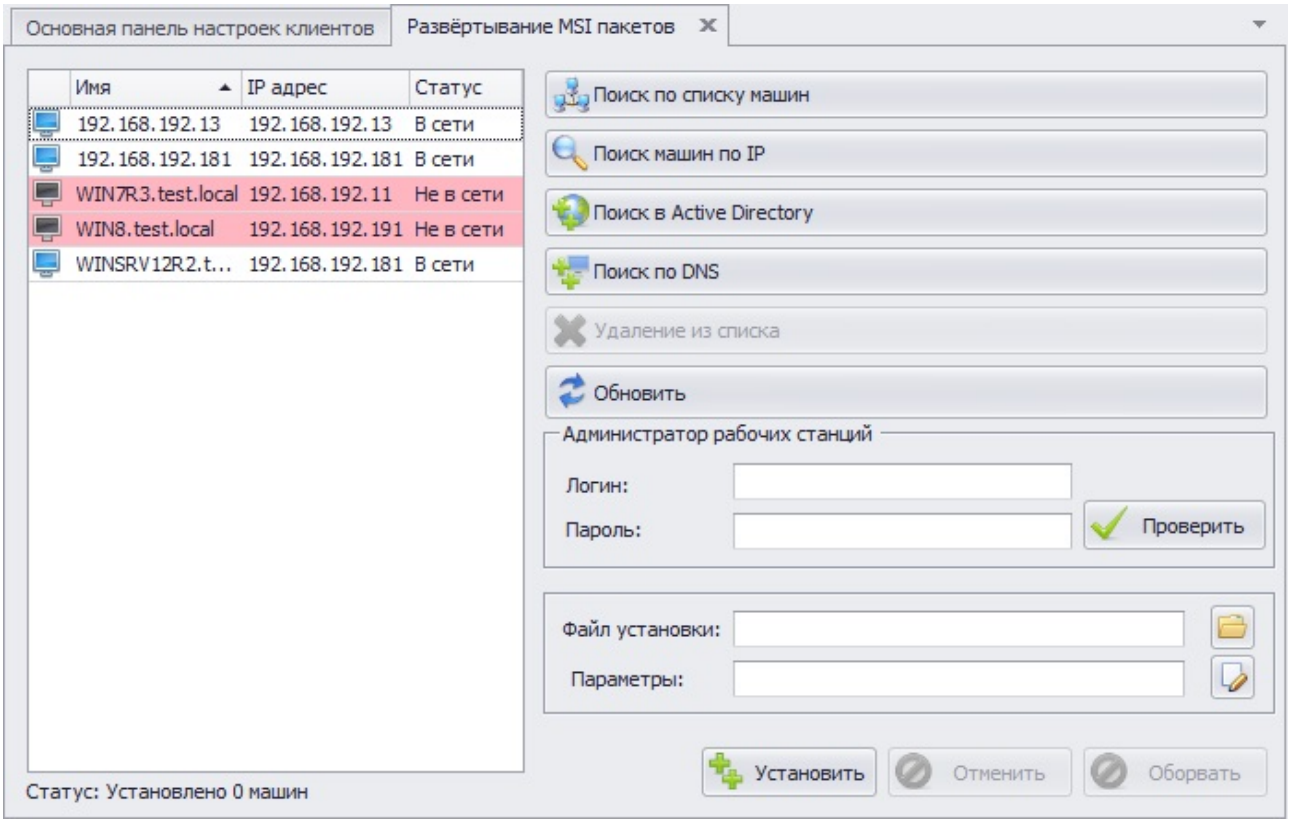


Рисунок 3.37. Статус рабочих станций во вкладке «Развертывание MSI пакетов»

4. Установка программного обеспечения на рабочие станции из серверной консоли СЗИ осуществляется от имени пользователя, входящего в группу **Администраторы** удаленной рабочей станции. Для авторизации на удаленной рабочей станции необходимо ввести в поля ***Логин*** и ***Пароль*** соответствующие данные пользователя, от имени которого будет происходить установка;

Пользователь может быть как локальный, так и доменный. В случае использования учетной записи пользователя домена, логин такого пользователя следует вводить с указанием имени домена, например: *Domain_name\user_name*.

При авторизации в ОС Windows 7/8/8.1/2012/2012R2 на удаленной рабочей станции от имени **локального** пользователя, входящего в группу администраторов (за исключением учетной записи встроенного администратора), на удаленной рабочей станции должен быть отключен параметр локальной политики безопасности ***Контроль учетных записей: все администраторы работают в режиме одобрения администратором***. В противном случае попытка доступа к рабочей станции из консоли администрирования СЗИ закончится ошибкой, а в поле ***Статус*** рабочей станции появится запись *Отсутствует доступ* (при операции проверки введенных данных авторизации администратора рабочей станции) или *Проблема при копировании файла установщика* (при попытке установки СЗИ на рабочую станцию).

5. В поле ***Файл установки*** указать полный путь к файлу-установщику клиентской части СЗИ *BlockHost-Net-2.0-Client v.<№ версии> x32.msi* или *BlockHost-Net-2.0-Client v.<№ версии> x64.msi*. Это можно сделать введя полный путь к файлу в данное поле вручную, или, нажав на кнопку ***Выбрать файл*** , указать размещение файла дистрибутива клиентской части СЗИ в открывшемся стандартном окне Windows **«Открыть»**.

6. В поле ***Параметры*** ввести необходимые для установки клиентской части СЗИ параметры: лицензию на использование СЗИ на удаленных рабочих станциях, идентификатор сервера СЗИ и пароль для подключения к нему удаленной рабочей станции, параметры подключения клиента СЗИ к серверу и др. Ввести необходимые параметры можно двумя способами:

   a) вручную – список параметров, их описание, возможные значения и значения по умолчанию приведены в табл. 3.1. Ввод параметров осуществляется через пробел. Например: *SERVER_ADDRESS=192.168.119.90:999 PIN=12345 LOC=код_лицензии LOCKEY=ключ_активации NET=код_лицензии NETKEY = ключ_активации MACHINE_ID=11111111111111111111111111111111 NET_KEY=12345 SOFTMODE=1 REBOOT=ReallySuppress /L*V "C:\<имя_файла_установщика>"*. В случае отсутствия параметров конфигурации клиента в поле ***Параметры***, они принимают значения по умолчанию.

   b) воспользоваться механизмом автозаполнения параметров – нажать кнопку ***Параметры по умолчанию***  , расположенную справа от поля ***Параметры***. В открывшемся окне **«Генерация командной строки инсталлятора»** (рис. 3.38) администратору безопасности доступны для изменения следующие параметры:

   - ***PIN токена*** – PIN-код доступа к создаваемому в процессе инсталляции клиентской части СЗИ персональному идентификатору в реестре Windows удаленной рабочей станции;

     При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] ` { } ( ) < >.

   - ***Syslog сервер*** – IP-адрес и номер UDP-порта Syslog-сервера, на который будут передаваться сообщения о работе СЗИ на контролируемой РС;
   - ***Перезагрузка после установки*** – параметр отвечает за перезагрузку рабочей станции сразу после установки клиентской части СЗИ. При его активации, рабочая станция будет перезагружена в процессе установки клиентской части СЗИ. Снятый параметр позволит избежать перезагрузки после установки СЗИ;
   - ***Дополнительные пользователи*** – при помощи кнопок ***Добавление дополнительных пользователей*** и ***Удаление дополнительных пользователей*** можно сформировать список пользователей домена, которые автоматически будут включены в список пользователей рабочей станции по окончании процесса установки на нее клиентской части СЗИ.

     По умолчанию в окне **«Генерация командной строки инсталлятора»** активирован недоступный для редактирования параметр ***Мягкий режим работы клиента*** (параметр *SOFTMODE=1* в командной строке). В результате на контролируемой рабочей станции СЗИ, сразу после установки, будет работать в ***Мягком режиме*** (подробнее о ***Мягком режиме*** работы СЗИ см. п. 6.2.4 настоящего руководства).

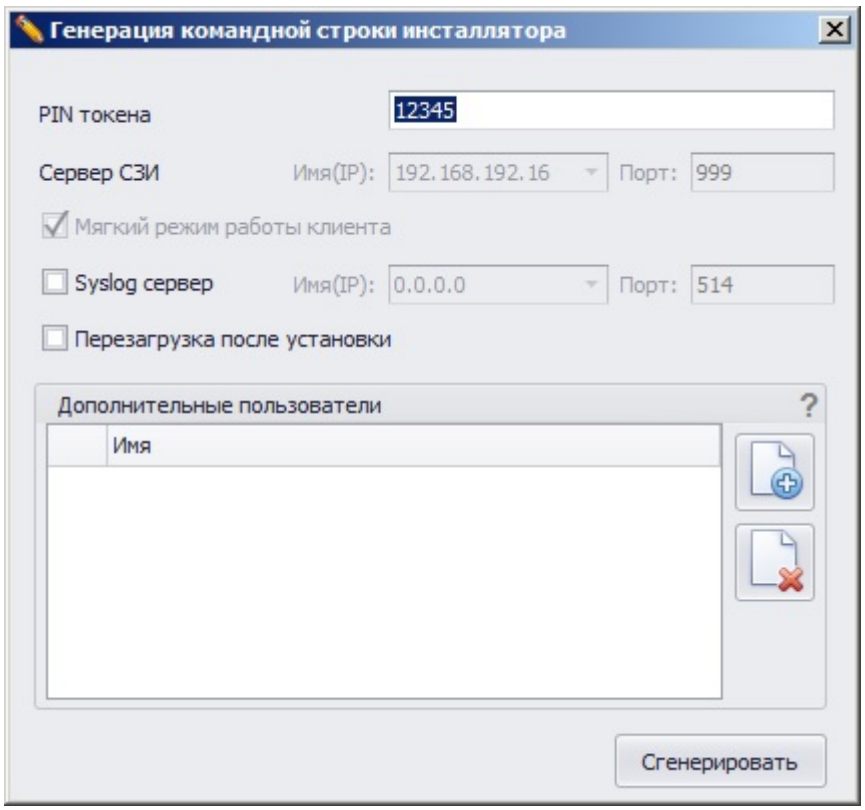


Рисунок 3.38. Окно задания параметров командной строки инсталлятора

Для генерации командной строки, с указанными в окне **«Генерация командной строки инсталлятора»** параметрами, нажать кнопку ***Сгенерировать***. В результате в поле ***Параметры*** вкладки **Развертывание MSI пакетов**, помимо указанных в окне **«Генерация командной строки инсталлятора»** параметров, будут добавлены значения используемых на сервере СЗИ локальной и сетевой лицензий, параметры сервера и клиента СЗИ, используемые по умолчанию, и необходимые клиенту СЗИ для первичного подключения к серверу, а также параметр командной строки с именем файла-журнала для аудита процесса инсталляции клиентской части СЗИ.

7. Для проверки корректности введенных идентификационных данных администратора удаленной рабочей станции следует нажать кнопку ***Проверить***. В случае успешной проверки запись в поле ***Статус*** рабочей станции изменится на *Успешная аутентификация*, а в случае ошибки введенных данных – запись в поле ***Статус*** изменится на *Отсутствует доступ*. Для устранения ошибки необходимо ввести верные данные идентификации и повторно нажать кнопку ***Проверить***.

   Процесс повторной проверки проходит только для рабочих станций, не прошедших проверку.

8. После заполнения поля ***Параметры*** нажать кнопку ***Установить*** для запуска процесса установки клиентской части СЗИ. Во время процесса установки во вкладке **Развертывание MSI пакетов** доступна только кнопка ***Отменить***. Процесс установки клиентской части СЗИ на удаленную рабочую станцию отображается в поле ***Статус***. В случае положительного результата установки

клиентской части СЗИ статус рабочей станции примет значение *Установка успешно завершена* (рис. 3.39).

Копирование файла-установщика с сервера СЗИ осуществляется в общий каталог *admin$* удаленной рабочей станции. Затем из этой папки система развертывания СЗИ средствами ОС Windows осуществляет запуск интерпретатора командной строки с командой вида:

```
msiexec /i [путь до файла] /quiet [параметры],
```

где:

`[путь до файла]` – локальный путь до файла-установщика на удаленной машине, то есть туда куда система его скопировала.

`[параметры]` – список параметров установки, указанных в виде строки, которые взяты из поля ***Параметры*** вкладки **Развертывание MSI пакетов** серверной консоли администрирования СЗИ.

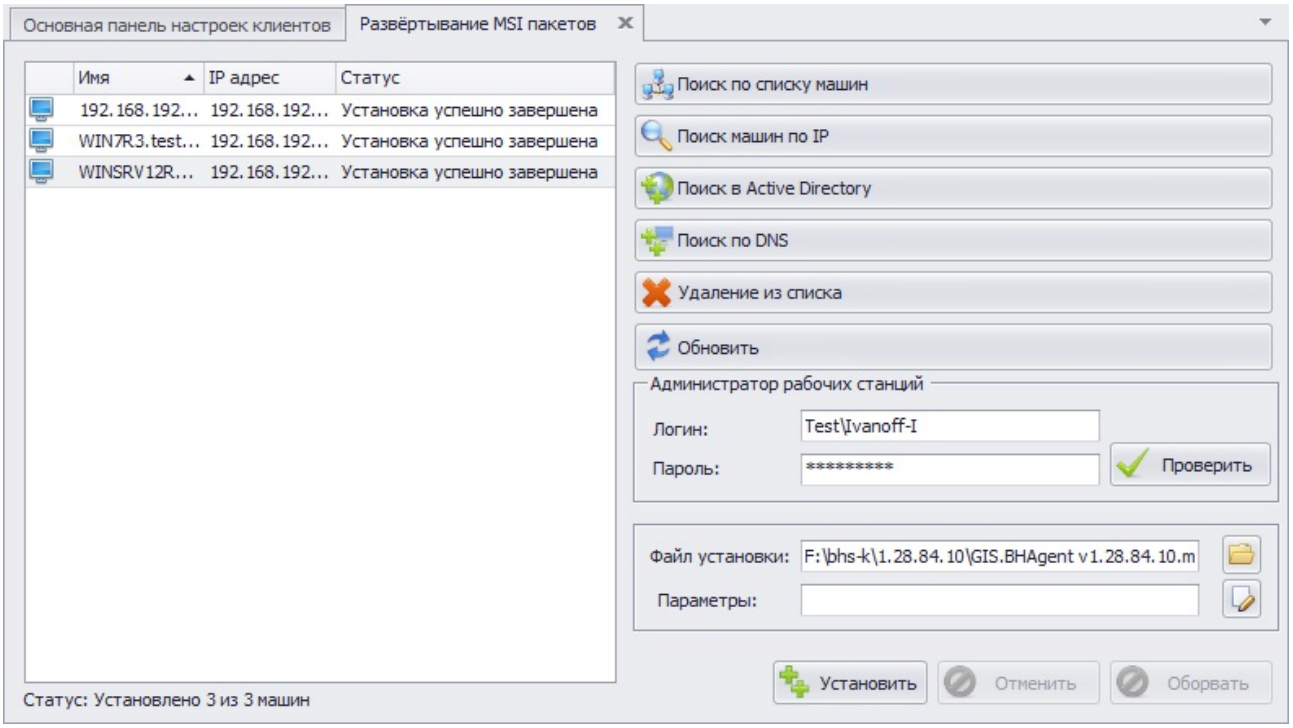


Рисунок 3.39. Отображение результата установки клиентской части СЗИ на удаленные PC

В случае необходимости отмены установки клиентской части СЗИ в процессе ее установки из консоли администрирования СЗИ следует нажать кнопку ***Отменить***. Значение в поле ***Статус*** изменится на *Отмена установки пользователем*, а на удаленной рабочей станции произойдет корректный возврат к состоянию ОС до начала процесса установки клиентской части СЗИ.

В случае установки клиентской части СЗИ на несколько рабочих станций (список которых сформирован во вкладке **Развертывание MSI пакетов**) нажатие на кнопку ***Отменить*** приведет к отмене установки СЗИ на всех находящихся в списке рабочих станциях.

Таблица 3.1. Параметры конфигурации клиента СЗИ

Наименование параметра	Назначение	Возможные значения
SERVER_ADDRESS	IP адрес и порт взаимодействия сервера СЗИ в формате IP-adress:Port	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке **Параметры сервера**. По умолчанию 192.198.1.1:999

Наименование параметра	Назначение	Возможные значения
PIN	PIN-код доступа к ключевому носителю	При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] ` { } ( ) < >
LOC	Код локальной лицензии	По умолчанию не задан
LOCKEY	Ключ активации локальной лицензии	По умолчанию не задан
NET	Код сетевой лицензии	По умолчанию не задан
NETKEY	Ключ активации сетевой лицензии	По умолчанию не задан
MACHINE_ID	Идентификатор рабочей станции, на которую будет устанавливаться СЗИ	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке **Параметры сервера**. По умолчанию не задан.
NET_KEY	Пароль подключения клиента к серверу СЗИ	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке **Параметры сервера.**
REBOOT	Параметр перезагрузки	ReallySuppress – перезагрузка подавляется (по умолчанию); Force – по окончании инсталляции СЗИ выполняется перезагрузка рабочей станции
SOFTMODE	Работа СЗИ в мягком режиме	1 – мягкий режим включен (по умолчанию); отсутствие параметра – мягкий режим отключен.
USERS	Список SID-ов пользователей, указанных через запятую.	При отсутствии параметра, в список пользователей будут добавлены все локальные пользователи рабочей станции, а также пользователи домена, профиль которых существует на рабочей станции.
SYSLOG_SERVER	IP адрес и порт взаимодействия с внешним syslog-сервером в формате IP-adress:Port	По умолчанию не задан.
/L*V	Параметр командной строки установщика Windows, указывающий на необходимость вывода подробных сведений процесса инсталляции СЗИ в указанный файл	По умолчанию имя файла-журнала соответствует имени файла-установщика СЗИ с расширением .log.

3.4.2. Установка клиентской части СЗИ «Блокхост-сеть 2.0» с использованием агента системы развертывания

Установка клиентской части СЗИ на рабочие станции с использованием агента системы развертывания состоит из следующих этапов:

- установка агента системы развертывания СЗИ на рабочие станции;
- формирование в серверной консоли СЗИ списка рабочих станций для развертывания на них клиента СЗИ и добавление их на сервер СЗИ;

- настройка рабочих станций, подготовленных к развертыванию;
- установка клиентской части СЗИ на подготовленные рабочие станции.

3.4.2.1 Установка агента системы развертывания СЗИ

Установка агента системы развертывания СЗИ на рабочие станции может осуществляться как локально – непосредственно на рабочей станции, так и удаленно: из консоли управления СЗИ или с применением групповых политик.

При локальной установке агента системы развертывания СЗИ необходимо запустить на рабочей станции файл дистрибутива *GIS.BHAgent_<№ версии>.msi*. и затем последовательно пройти все шаги мастера установки.

Для установки агента системы развертывания из серверной консоли администрирования СЗИ необходимо:

1. Сформировать во вкладке **Развертывание MSI пакетов** список рабочих станций, на которые будет установлен агент системы развертывания (подробнее о способах формирования списка рабочих станций см. подраздел 3.3.3 настоящего руководства);
2. Ввести в соответствующие поля вкладки **Развертывание MSI пакетов** имя и пароль пользователя, входящего в группу **Администраторы** удаленной рабочей станции (подробнее см. п. 4 подраздела 3.4.1 настоящего руководства);
3. В поле ***Файл установки*** вкладки **Развертывание MSI пакетов** (см. рис. 3.39) указать полный путь к файлу-установщику агента системы развертывания *GIS.BHAgent v<№ версии>.msi*. Это можно сделать введя в данное поле полный путь к файлу вручную, или, нажав на кнопку ***Выбрать файл***  , указать размещение файла в открывшемся стандартном окне Windows **«Открыть»**. Поле ***Параметры*** при установке агента системы развертывания можно оставить пустым;
4. Проверить корректность введенных идентификационных данных администратора удаленной рабочей станции (подробнее см. п. 7 подраздела 3.4.1 настоящего руководства);
5. Для запуска процесса установки агента системы развертывания нажать кнопку ***Установить*** во вкладке **Развертывание MSI пакетов** консоли управления. Во время процесса установки во вкладке **Развертывание MSI пакетов** доступна только кнопка ***Отменить***. Процесс установки агента на удаленную рабочую станцию отображается в поле ***Статус***. В случае успешного завершения процесса установки агента статус рабочей станции примет значение *Установка успешно завершена*.

По окончании процесса установки (удаленной или локальной) агента системы развертывания СЗИ произойдет запуск службы, отвечающей за работу агента, и рабочая станция будет готова к операции развертывания клиентской части СЗИ.

3.4.2.2 Добавление рабочих станций с агентом системы развертывания на сервер СЗИ

Для добавления рабочих станций, на которые планируется установить клиентскую часть СЗИ «Блокхост-сеть 2.0» с использованием агента системы развертывания, на сервер СЗИ необходимо в серверной консоли СЗИ выполнить следующие действия:

1. В окне **«Список машин»** выделить группу, в которую будут добавлены рабочие станции (в примере на рис. 3.40 выделена группа ***Все машины***);
2. Выбрать пункт главного меню ***Развертывание → Развертывание через агента*** (см. рис. 3.24) – откроется вкладка **Развертывание через агента**:

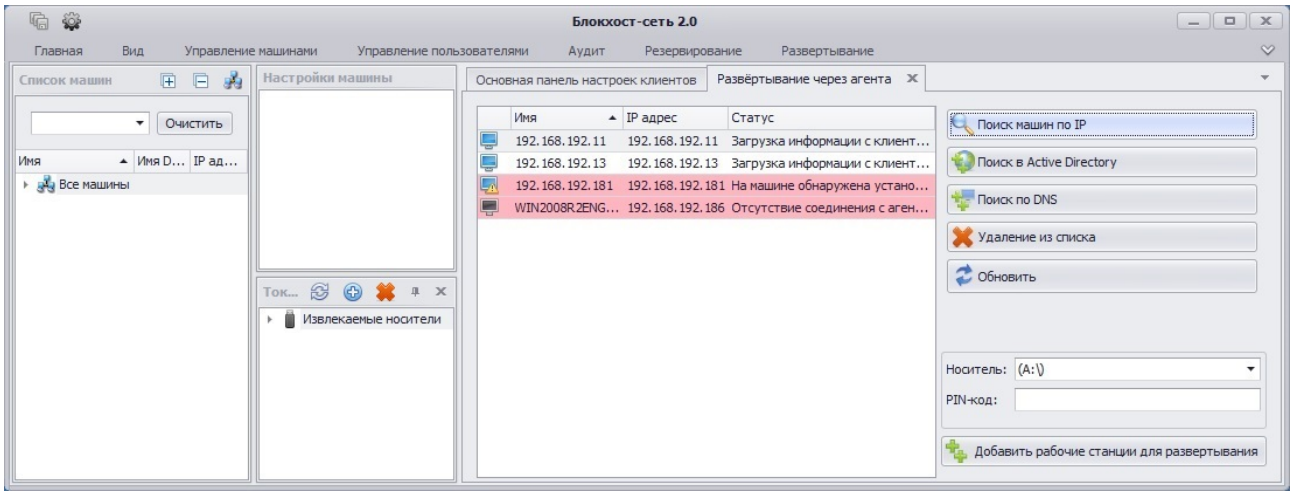


Рисунок 3.40. Вкладка «Развертывание через агента»

3. Во вкладке **Развертывание через агента** сформировать список рабочих станций для развертывания на них клиента СЗИ (подробнее о способах формирования списка рабочих станций см. подраздел 3.3.3 настоящего руководства).

   Во вкладке **Развертывание через агента** в графе *Статус* для добавленных рабочих станций может отображаться следующая информация:

   - *Загрузка информации с клиентской машины завершена* – рабочая станция готова к добавлению на сервер СЗИ и для инсталляции на ней клиентской части;
   - *Отсутствие соединения с агентом на клиентской машине* – на рабочей станции не установлен агент системы развертывания СЗИ или остановлена его служба (*GIS.BlockPost.Deployment.Service*). Добавить такую рабочую станцию на сервер СЗИ из вкладки **Развертывание через агента** невозможно;
   - *На машине обнаружена установленная консоль* – на рабочей станции уже установлена клиентская часть СЗИ. Добавить такую рабочую станцию на сервер СЗИ из вкладки **Развертывание через агента** невозможно;
   - *Отсутствие сетевого соединения с клиентской машиной* – рабочая станция в настоящее время находится не в сети. Добавить такую рабочую станцию на сервер СЗИ из вкладки **Развертывание через агента** невозможно.

   Рабочие станции недоступные для добавления на сервер СЗИ будут подсвечены красным цветом.

При формировании списка рабочих станций по их IP-адресу (нажата кнопка ***Поиск машин по IP***), в окне **«Поиск машин с агентом развертывания»** осуществляется поиск только тех рабочих станций, на которых запущена служба агента системы развертывания (*GIS.BlockPost.Deployment.Service*).

Для удаления рабочей станции из списка необходимо выделить ее (для выделения нескольких рабочих станций можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и нажать на кнопку ***Удаление из списка***.

Кнопка ***Обновить*** во вкладке **Развертывание через агента** (рис. 3.36) предназначена для обновления статуса рабочих станций добавленных для развертывания СЗИ.

4. Затем из выпадающего списка поля ***Носитель*** выбрать электронный идентификатор (предварительно подключив его к серверу безопасности), на который будут записаны ключи взаимной идентификации сервера и клиента СЗИ, и который будет присвоен встроенной учетной записи локального администратора удаленной рабочей станции, а в поле ***PIN-код*** ввести PIN-код доступа к этому носителю.

В качестве электронного идентификатора встроенного администратора удаленной рабочей станции рекомендуется использовать USB-накопитель (флешку). Для удобства работы администратора безопасности СЗИ встроенным учетным записям администраторов ОС на контролируемых рабочих станциях может быть присвоен **один и тот же USB-накопитель (флешка).**

5. Для завершения операции добавления рабочих станций на сервер СЗИ нажать кнопку ***Добавить рабочие станции для развертывания***. При успешном завершении операции добавления пиктограмма рабочей станции появится в окне **«Список машин»** серверной консоли (рис. 3.41), в окне **«Лог»** появится сообщение *Сохранены настройки сервера*, а указанный ключевой носитель будет присвоен в качестве персонального идентификатора учетной записи встроенного администратора удаленной рабочей станции.

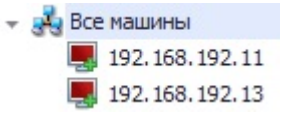


Рисунок 3.41 Рабочие станции, добавленные для развертывания СЗИ

Если во вкладке **«Развертывание через агента»** указано несколько рабочих станций, параметры выбора ключевого носителя для учетной записи встроенного администратора применятся сразу ко всем этим станциям.

3.4.2.3 Формирование списка пользователей на рабочих станциях, подготовленных к развертыванию с использованием агента СЗИ

После того, как рабочие станции, на которые планируется установить клиентскую часть СЗИ «Блокхост-сеть 2.0», были добавлены на сервер СЗИ, можно стразу приступить к установке на них клиентской части СЗИ. Однако перед этим рекомендуется создать список пользователей, которые будут допущены к работе на контролируемой рабочей станции.

Для формирования списка пользователей, допущенных к работе на контролируемой рабочей станции, необходимо в серверной консоли управления СЗИ выполнить следующие действия:

1. В окне **«Список машин»** раскрыть пункт ***Все машины*** и выбрать добавленную для развертывания рабочую станцию, для которой будет формироваться список пользователей (рис. 3.42).

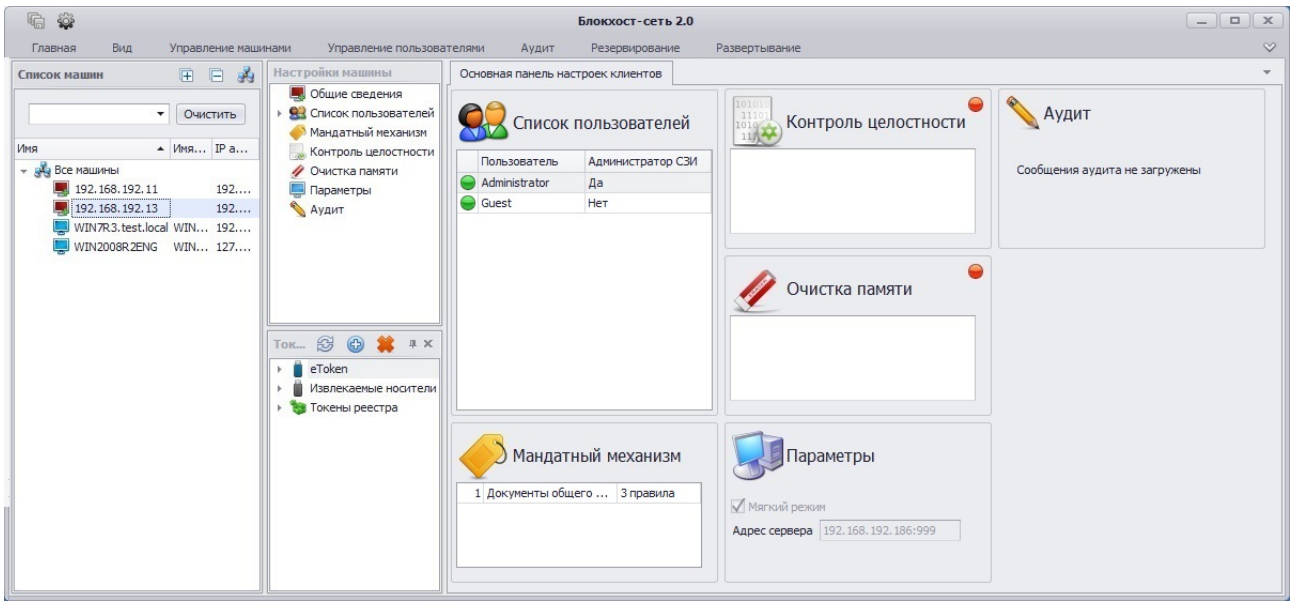


Рисунок 3.42. Выбор PC для формирования списка пользователей

2. В окне **«Настройки машины»** выделить параметр ***Список пользователей*** и в главном меню ***Управление пользователями*** выбрать пункт ***Добавление пользователей***:

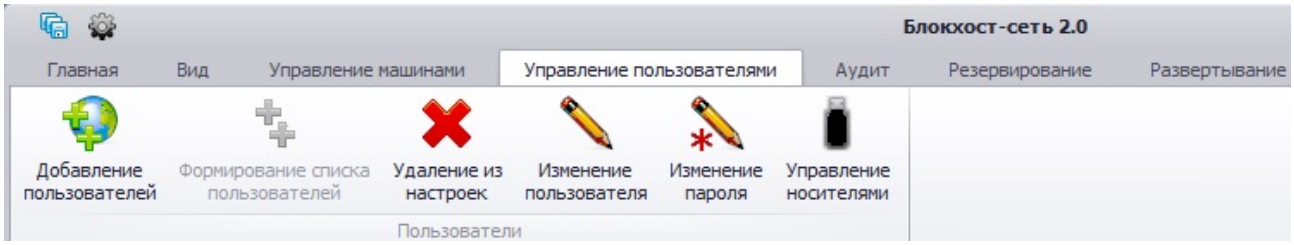


Рисунок 3.43. Меню «Управление пользователями»

3. В открывшемся окне **«Добавление пользователей»** (рис. 3.44):
   - сформировать список добавляемых пользователей (подробно процесс выбора учетных записей пользователей рассмотрен в разделе 5.2. «Добавление пользователей в СЗИ «Блокхост-сеть 2.0» настоящего руководства);
   - задать необходимые параметры добавляемых в СЗИ пользователей (ключевой носитель, из списка подключенных к серверу СЗИ, PIN-код доступа к нему и тип входа пользователя на рабочую станцию);
   - нажать кнопку ***Добавить***.

В случае выбора сразу нескольких учетных записей, параметры, указанные в окне **«Добавление пользователей»** (ключевой носитель и тип входа), присваиваются каждому из списка добавляемых пользователей. Всем добавленным пользователям по умолчанию присваивается мандатная метка со значением **1**.

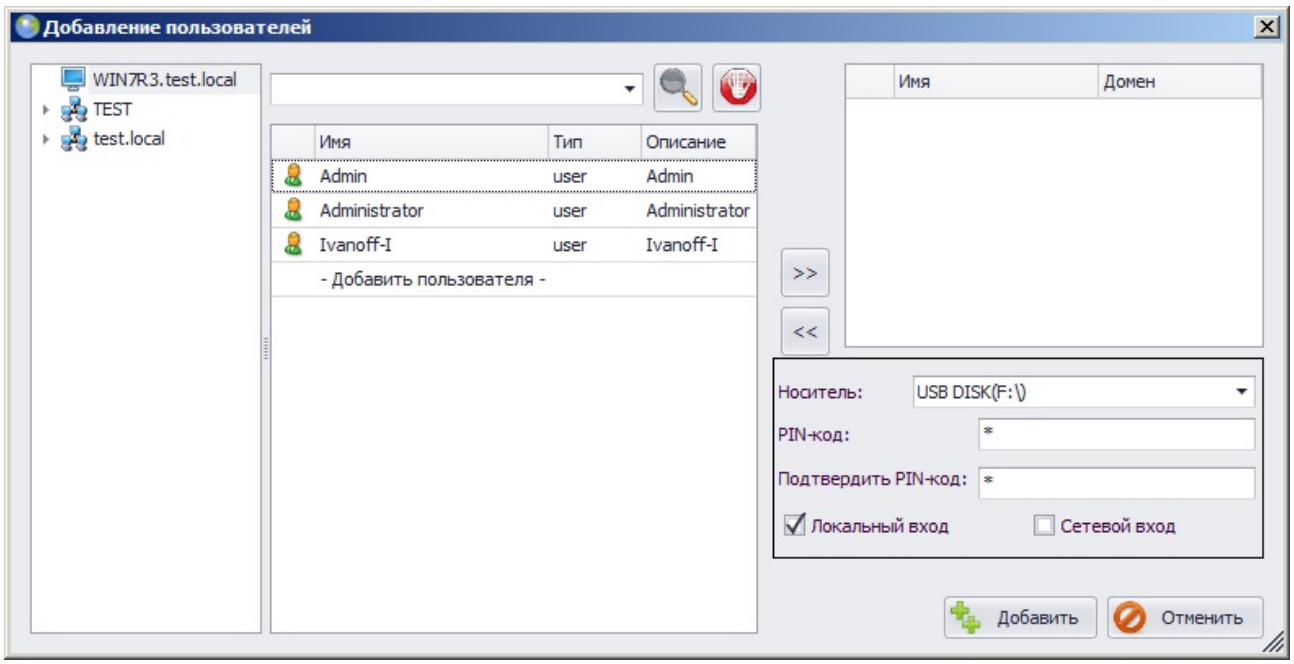


Рисунок 3.44. Окно «Добавление пользователей»

4. Учетная запись добавленного в СЗИ пользователя отобразится в ***Основной панели настроек клиентов*** консоли администрирования СЗИ «Блокхост-сеть 2.0»:

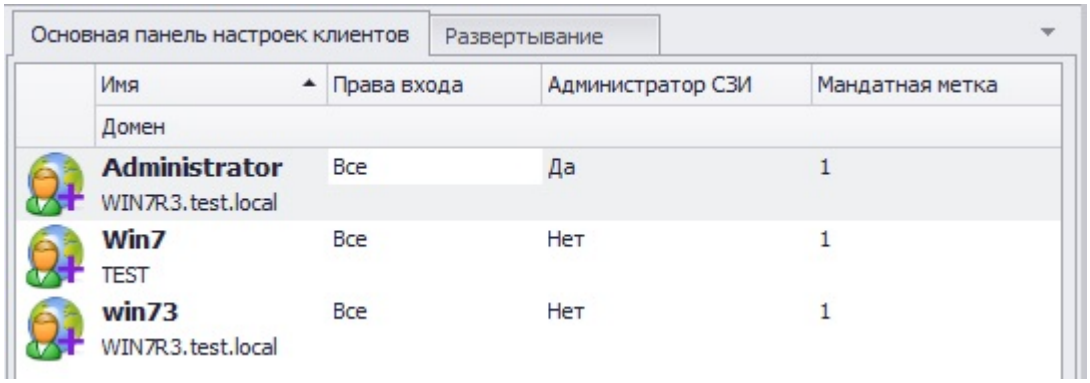


Рисунок 3.45. Отображение добавленного пользователя в консоли администрирования СЗИ

Процесс формирования списка пользователей необходимо выполнять **отдельно для каждой рабочей станции**.

В **Основной панели настроек клиентов** в списке пользователей рабочей станции до начала процесса установки СЗИ на рабочую станцию существует возможность изменения основных параметров учетной записи пользователя (имя, пароль, тип входа, значение мандатной метки, назначение персонального идентификатора). Подробнее редактирование параметров учетной записи пользователя в серверной консоли администрирования СЗИ рассмотрено в разделе 5.3 «Редактирование параметров пользователей» настоящего руководства.

3.4.2.4 Удаленная установка клиентской части СЗИ «Блокхост-сеть 2.0»

Следующим шагом является удаленная установка клиентской части СЗИ «Блокхост-сеть 2.0» на рабочие станции, подготовленные к развертыванию СЗИ. Для начала процесса установки клиентской части СЗИ на удаленные рабочие станции необходимо:

1. В окне **«Список машин»** выделить группу (например, группу по умолчанию ***Все машины***);

2. В главном меню ***Развертывание*** выбрать пункт ***Установка через агента*** (см. рис. 3.24);
3. В открывшемся окне **«Управление развертыванием»** (рис. 3.46) будет отображен список подготовленных к установке СЗИ рабочих станций, для начала процесса установки клиентской части СЗИ на все подготовленные к развертыванию компьютеры нажать кнопку ***Развернуть***. Ход установки СЗИ для каждой рабочей станции из списка отображается в окне **«Управление развертыванием»** в поле *Состояние процесса установки* (см. рис. 3.48).

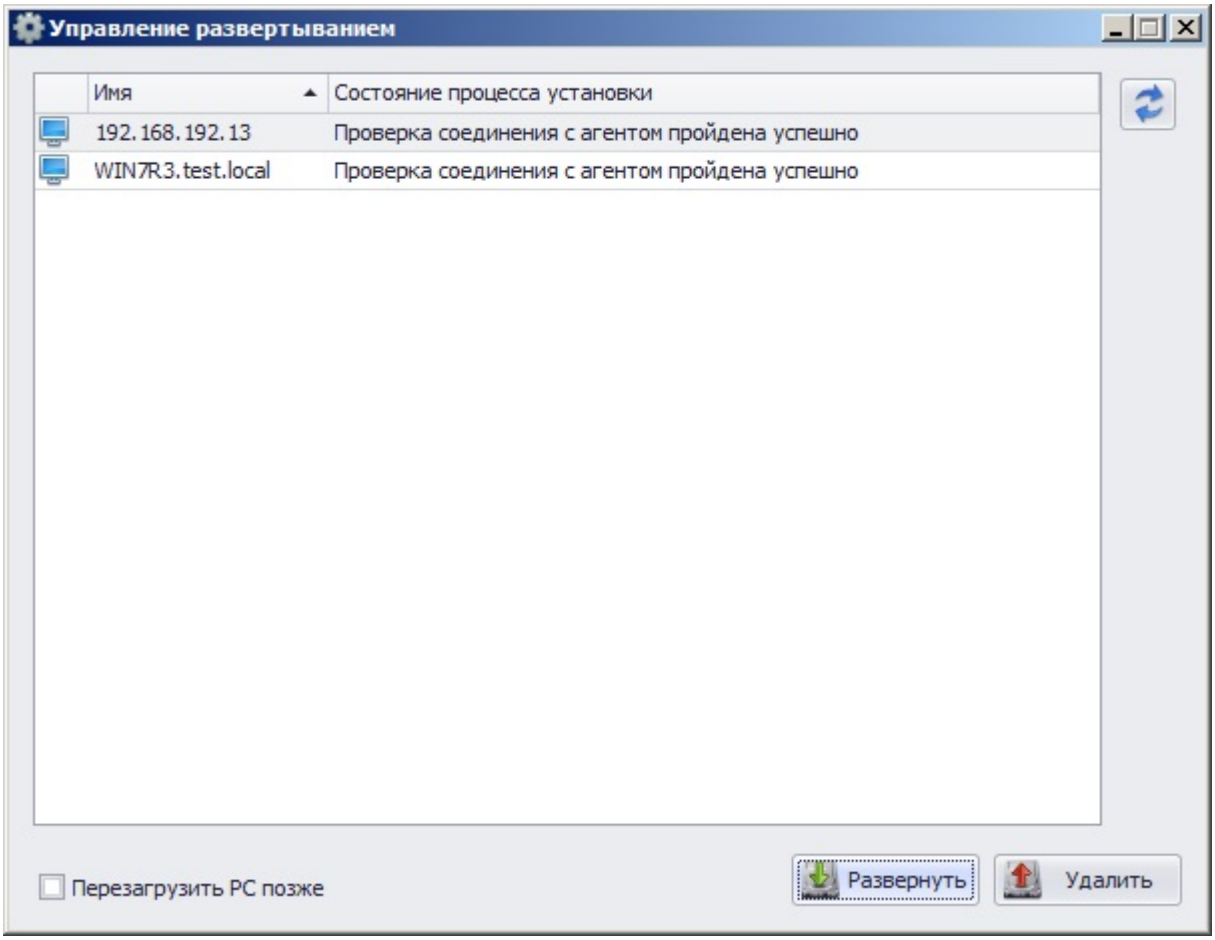


Рисунок 3.46. Окно «Управление развертыванием»

Установка параметра ***Перезагрузить PC позже*** в окне **«Управление развертыванием»** позволит отменить перезагрузку удаленных рабочих станций после установки на них клиентской части СЗИ «Блокхост-сеть 2.0».

Следует учитывать, что рабочие станции станут доступны для настройки механизмов СЗИ из серверной консоли администрирования только после их перезагрузки. Перезагрузка может быть выполнена как сразу после окончания инсталляции клиентской части СЗИ, так и позднее самим пользователем локально на рабочей станции или администратором безопасности из серверной консоли администрирования СЗИ (пункт меню ***Управление машинами →Перезагрузить*** или пункт контекстного меню рабочей станции ***Перезагрузить***).

Если параметр ***Перезагрузить PC позже*** не установлен, то в процессе установки СЗИ рабочие станции будут автоматически перезагружены. По окончании процесса установки СЗИ на рабочей станции появится окно с предупреждением о предстоящей перезагрузке (рис. 3.47). За время до начала перезагрузки пользователь рабочей станции должен сохранить все несохраненные данные, чтобы избежать их потери.

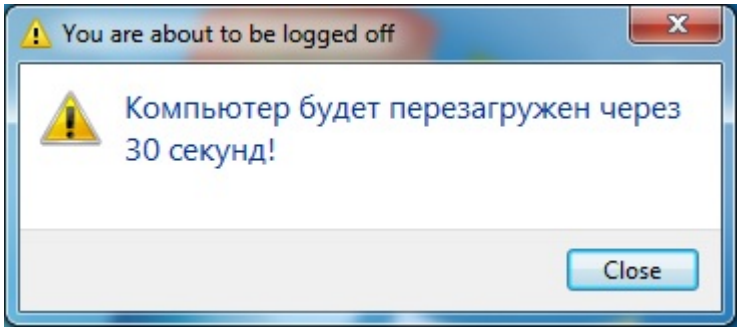


Рисунок 3.47. Сообщение о перезагрузке ОС

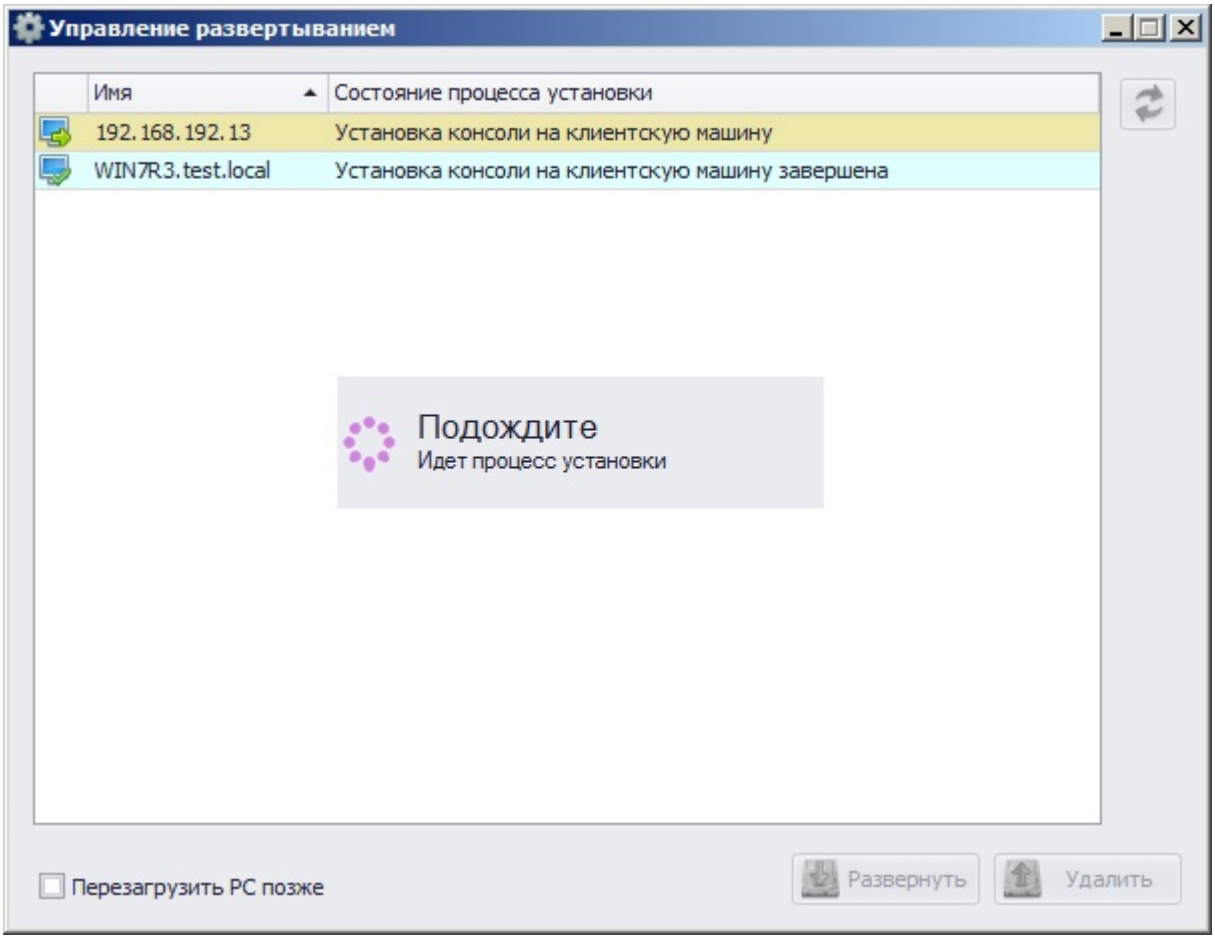


Рисунок 3.48. Отображение хода установки клиентской части СЗИ

3.4.3. Удаление СЗИ «Блокхост-сеть 2.0» с использованием агента системы развертывания

Если клиентскую часть СЗИ «Блокхост-сеть 2.0» необходимо удалить с защищаемой рабочей станции, на которой работает агент системы развертывания, это можно сделать через серверную консоль администрирования СЗИ следующим образом:

1. В окне **«Список машин»** консоли администрирования СЗИ выбрать пункт ***Все машины***;
2. В ***Основной панели настроек клиентов*** выбрать рабочую станцию (при помощи кнопок **<Ctrl>** или **<Shift>** можно выделить несколько рабочих станций), щелкнуть по имени рабочей станции правой кнопкой мыши и в контекстном меню выбрать пункт ***Удалить клиент*** (рис. 3.49).

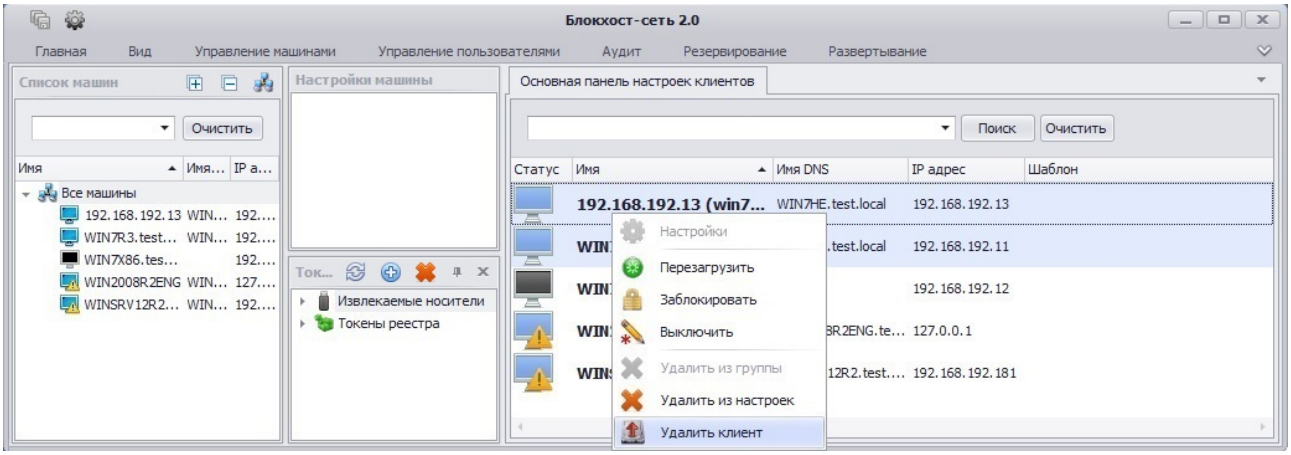


Рисунок 3.49. Контекстное меню контролируемой рабочей станции

3. В открывшемся окне **«Управление развертыванием»**, будут отображены рабочие станции с которых будет удаляться СЗИ. Для начала процесса удаления СЗИ с рабочих станций нажать кнопку ***Удалить***. В ходе процесса удаления клиентской части СЗИ с рабочей станции она будет автоматически перезагружена. Ход удаления СЗИ «Блокхост-сеть 2.0» для каждой рабочей станции из списка отображается в поле *Состояние процесса установки* в окне **«Управление развертыванием»** (рис. 3.50).

Следует учесть, что если параметр ***Перезагрузить PC позже*** в окне **«Управление развертыванием»** (см. рис. 3.50) не установлен, то по окончании процесса удаления СЗИ на рабочей станции появится окно с предупреждением о предстоящей перезагрузке компьютера (см. рис. 3.47). За это время пользователь рабочей станции должен сохранить все несохраненные данные, чтобы избежать их потери.

Установка параметра ***Перезагрузить PC позже*** позволит отменить принудительную перезагрузку рабочих станций после окончания процесса удаления клиентской части СЗИ «Блокхост-сеть 2.0». Окончательное удаление служебных файлов СЗИ с этих рабочих станций произойдет после их перезагрузки, которая в этом случае может быть инициирована пользователем этой рабочей станции.

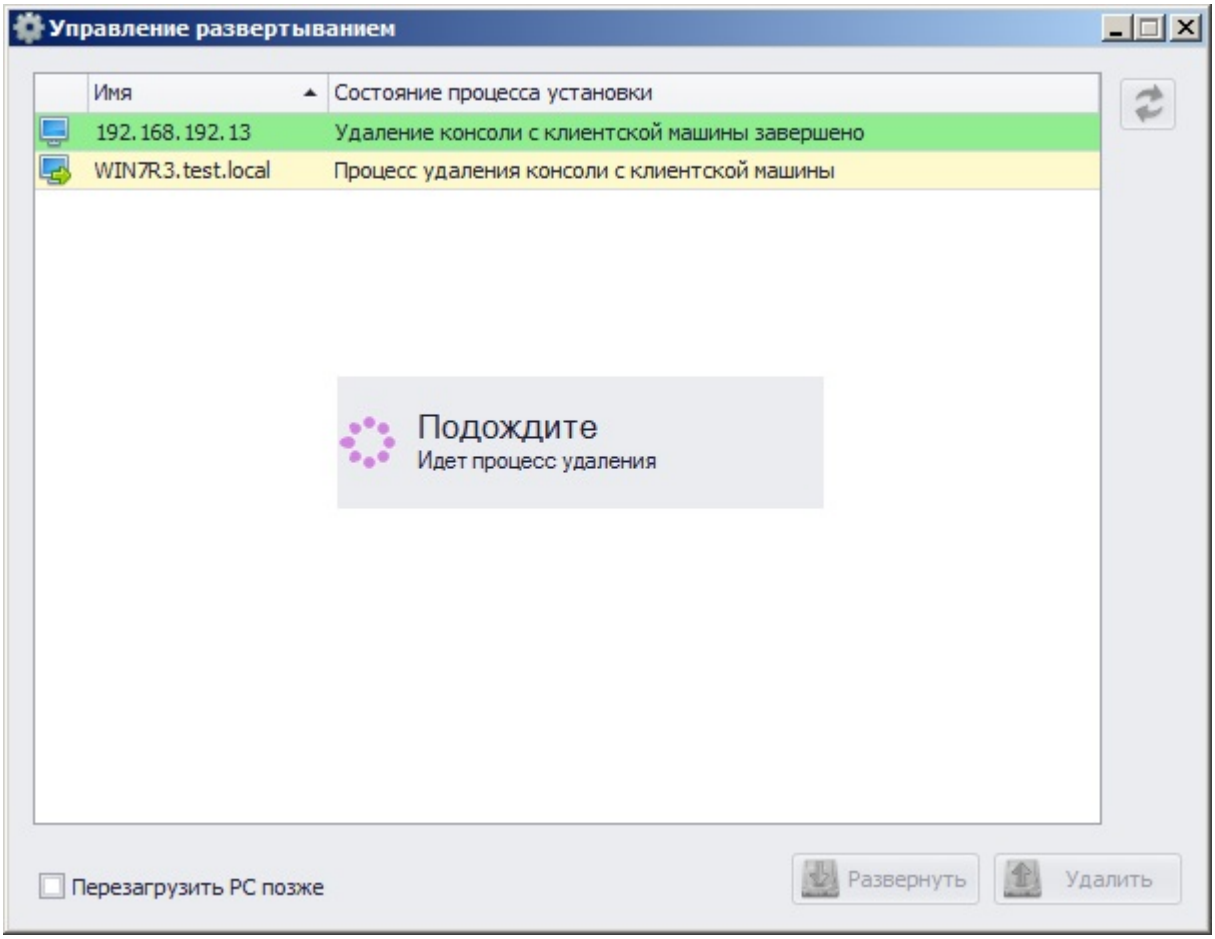


Рисунок 3.50. Отображение состояния процесса удаления клиентской части СЗИ

3.4.4. Автоматическое подключение рабочих станций, с настроенным клиентом СЗИ «Блокхост-сеть 2.0» к серверу

В серверной консоли управления СЗИ «Блокхост-сеть 2.0» существует возможность добавления в список, контролируемых текущим сервером СЗИ, рабочих станций с установленной и настроенной на подключение к текущему серверу клиентской частью СЗИ. Такая необходимость может понадобиться, например, при установке клиентской части на рабочие станции в сети с помощью групповых политик.

Для добавления в список, контролируемых текущим сервером СЗИ, рабочих станций с установленной и настроенной на подключение к текущему серверу клиентской частью СЗИ необходимо:

1. В окне **«Список машин»** выделить группу, в которую будут добавлены рабочие станции (например, группу по умолчанию ***Все машины***);
2. В главном меню выбрать пункт ***Развертывание →Ручное развертывание***;
3. В открывшейся вкладке **Ручное развертывание** (см. рис. 3.25) сформировать список рабочих станций для добавления их на сервер СЗИ (подробнее о формировании списка рабочих станций см. подраздел 3.3.3 настоящего руководства);
4. После того, как все необходимые рабочие станции с установленным и настроенным клиентом СЗИ «Блокхост-сеть 2.0» были добавлены во вкладку **Ручное развертывание**, необходимо подключить к серверу электронный идентификатор, выбрать его из выпадающего списка поля ***Носитель*** и ввести

PIN-код доступа к нему в соответствующее поле. Затем нажать кнопку ***Добавить рабочие станции***. В результате все рабочие станции из вкладки **Ручное развертывание** будут добавлены в выделенную группу в окне **«Список машин»** консоли управления СЗИ.

После перезагрузки сервера СЗИ рабочие станции с установленной и настроенной на подключение к текущему серверу клиентской частью СЗИ, добавленные на сервер через вкладку **Ручное развертывание**, станут доступны для управления из серверной консоли администрирования СЗИ. При этом переносить настройки, записанные на электронный идентификатор, нет необходимости.

Рабочие станции с установленной и настроенной на подключение к текущему серверу клиентской частью СЗИ, добавленные на сервер СЗИ через вкладку **Ручное развертывание**, будут доступны для управления из консоли администрирования СЗИ только в том случае, если совпадают параметры сервера СЗИ (***Сетевой интерфейс сервера***, ***Идентификатор машины по умолчанию*** и ***Пароль подключения клиента***) и параметры использованные при установке клиента СЗИ на эти рабочие станции (***SERVER_ADDRESS***, ***MACHINE_ID*** и ***MACHINE_KEY***). Подробнее о настройках сервера СЗИ см. пункт 3.3.2 «Настройка серверной части СЗИ «Блокхост-сеть 2.0» настоящего руководства. Подробнее о способах установки клиентской части СЗИ с настройкой параметров подключения к серверу СЗИ см. подпункты 1.4.2 «Руководства по инсталляции «СЗИ Блокхост-сеть 2.0». (Сетевой вариант)».

3.5. Удаленное администрирование рабочих станций

Список всех контролируемых на сервере СЗИ рабочих станций отображается в окне **«Список машин»** и в **Основной панели настроек клиентов** серверной консоли администрирования СЗИ «Блокхост-сеть 2.0»:

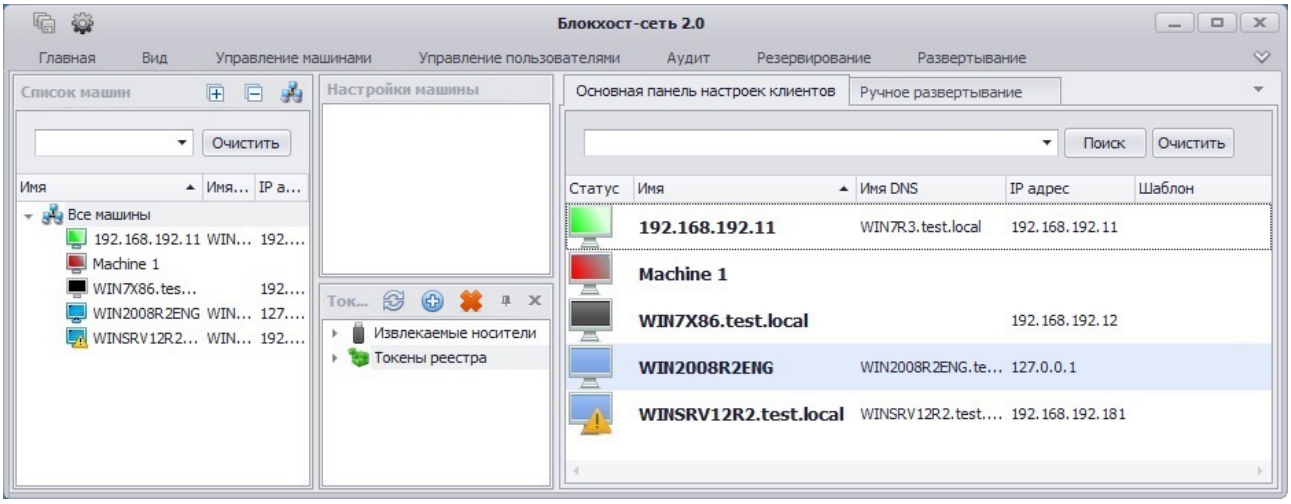


Рисунок 3.51. Список контролируемых станций

На рисунке 3.51 отображаются следующие пиктограммы контролируемых рабочих станций:

– рабочая станция включена, осуществлен вход пользователя в ОС, настройки СЗИ загружены в серверную консоль управления;

– рабочая станция включена, осуществлен вход пользователя в ОС, настройки СЗИ не загружались в серверную консоль управления;

– рабочая станция включена, службы СЗИ на ней запущены, настройки СЗИ загруженные в серверную консоль управления были отредактированы, но еще не сохранены;

– рабочая станция включена, службы СЗИ на ней запущены, но никто из пользователей не прошел аутентификацию;

– рабочая станция включена, службы СЗИ на ней запущены и активирован ***Мягкий режим*** (подробнее о ***Мягком режиме*** работы СЗИ см. п. 6.2.4 настоящего руководства);

– контролируемая рабочая станция, на которой не запущены службы СЗИ;

– рабочая станция была добавлена на сервер СЗИ, но настройки СЗИ этой рабочей станции еще ни разу не загружались на сервер;

В контекстном меню контролируемой рабочей станции в серверной консоли имеется пункт ***Обновить*** (рис. 3.52). Выбрав этот пункт контекстного меню можно обновить отображение всех настроек СЗИ конкретной станции.

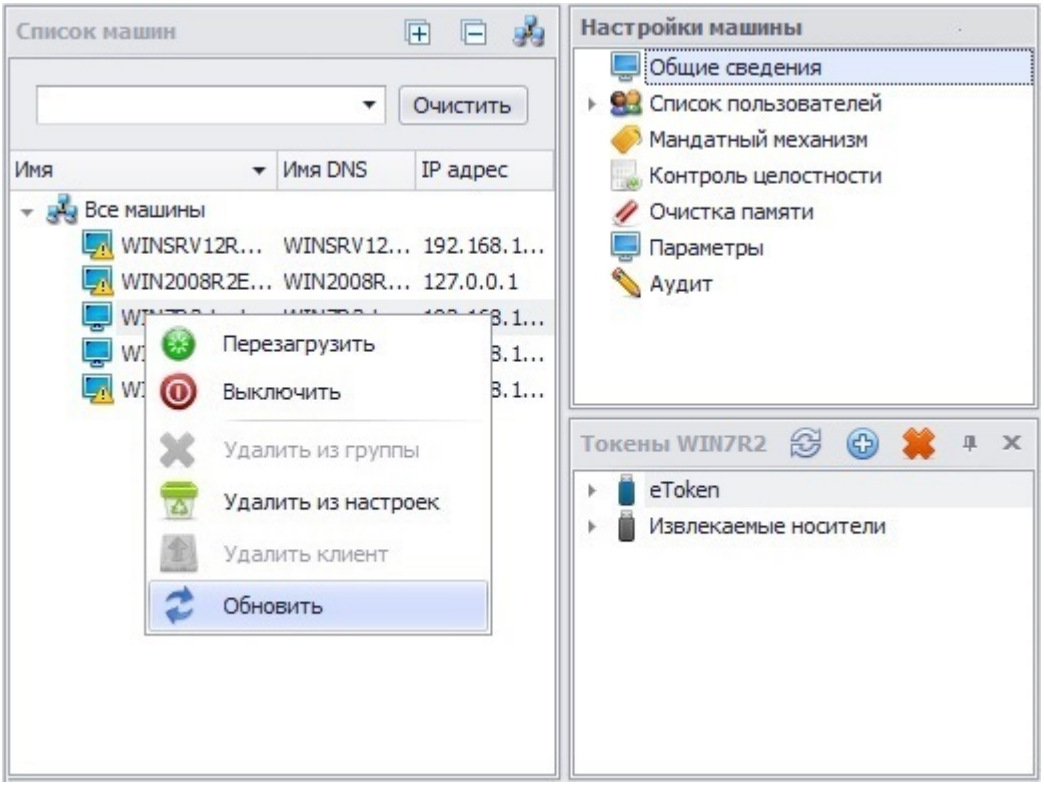


Рисунок 3.52. Обновление настроек рабочей станции

Операция обновления отображения настроек СЗИ рабочей станции может понадобиться для постановки на контроль файла или разграничения доступа к внешнему носителю информации, которые были созданы или подключены, соответственно, уже после загрузки в серверной консоли настроек механизмов СЗИ текущей рабочей станции.

Если в настройки механизмов СЗИ рабочей станции перед операцией обновления их отображения вносились изменения, то появится сообщение, предупреждающее о потере всех внесенных изменений в настройки механизмов СЗИ (рис. 3.53). В случае необходимости сохранения внесенных изменений следует нажать кнопку ***Нет*** (***No***) в диалоговом окне. Затем сохранить все произведенные изменения с помощью кнопки ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ, или воспользоваться пунктом меню ***Главная→ Сохранить***. После сохранения внесенных изменений в настройки

механизмов СЗИ повторить операцию обновления их отображения для текущей рабочей станции.

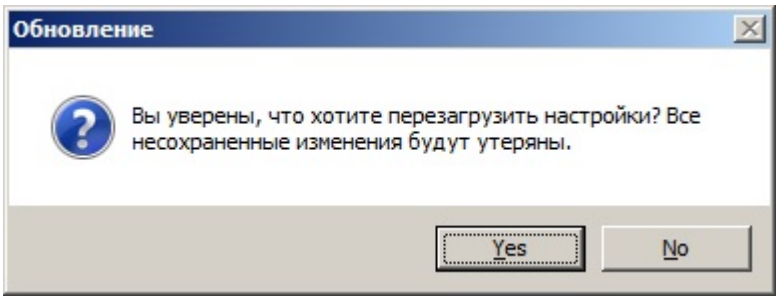


Рисунок 3.53. Окно-предупреждение о потере внесенных изменений

4. Защищенный вход в систему

4.1. Вход в систему

Реализованный в СЗИ «Блокхост-сеть 2.0» механизм двухфакторной аутентификации позволяет усилить защищенность входа рабочей станции за счет использования, помимо аутентификационных данных пользователя, персональных идентификаторов.

В СЗИ «Блокхост-сеть 2.0» основными возможностями механизма защиты входа являются:

- усиление стандартных механизмов операционной системы, связанных с идентификацией и аутентификацией пользователей;
- режим усиленной аутентификации пользователей на основе персональных идентификаторов;
- регистрация событий, связанных с входом пользователей в систему.

Основными функциями администратора безопасности по защите входа в систему с использование СЗИ «Блокхост-сеть 2.0» являются:

- организация и поддержка работы пользователей с персональными идентификаторами;
- управление режимом входа пользователей в систему и режимом усиленной аутентификации;
- настройка параметров временной блокировки экрана.

Организация и поддержка работы пользователей включает в себя выдачу пользователям идентификаторов, настройку режимов их использования, обеспечение доступа пользователей к компьютерам.

В СЗИ «Блокхост-сеть 2.0» для администратора безопасности реализована возможность работы по RDP (подключения к удаленному рабочему столу).

Важные особенности работы по RDP:

1) Подключение к удаленному рабочему столу должно использоваться только для администрирования СЗИ.

2) Подключение к удаленному рабочему столу должно быть разрешено только тем пользователям, которые могут администрировать СЗИ (запускать консоль администрирования) и только с этой целью. Такими пользователями могут быть администратор безопасности, либо пользователи, которым в СЗИ делегированы полномочия администрирования.

3) СЗИ не следует использовать для защиты от НСД терминальных серверов.

Перед подключением к удаленному рабочему столу предварительно необходимо:

- убедиться в наличии учетной записи администратора безопасности в списке пользователей удаленной рабочей станции;
- средствами ОС Windows рабочей станции установить разрешение на удаленное подключение к ней учетной записи администратора безопасности СЗИ;

- выполнить перезагрузку удаленной рабочей станции (если она работает под управлением ОС Windows XP).

Для подключения к удаленному рабочему столу необходимо выбрать пункт главного меню ***Пуск →Все программы →Стандартные →Подключение к удаленному рабочему столу*** и в появившемся окне ввести параметры подключения к удаленной рабочей станции.

После подключения к удаленной рабочей станции появится окно аутентификации СЗИ «Блокхост-сеть 2.0», описанное в пунктах 4.1.1, 4.1.2 и 4.1.3 настоящего руководства.

Важно помнить про особенности подключения персональных идентификаторов, используемых для аутентификации пользователя в СЗИ, при работе по RDP:

- *eToken, SafeNet eToken, ruToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, ESMART Token, Avest Token* подключаются к рабочей станции, **с которой** происходит подключение по RDP (т.е. – к локальной рабочей станции);
- *USB-носитель, дискета, персональный идентификатор в реестре* подключаются к рабочей станции, **к которой** происходит подключение по RDP (т.е.непосредственно к удаленной рабочей станции).

Особенности аутентификации с предъявлением USB-накопителя:

Если на ПК установлено СКЗИ «КриптоПРО CSP», при загрузке ОС и/или разблокировании ПК может возникнуть следующее неудобство: «шумит» дисковод. Это связано с тем, что СКЗИ обращается ко всем съемным носителям для поиска сертификата на них. Для устранения данной проблемы в настройках СКЗИ «КриптоПРО CSP» следует выбрать вкладку **Оборудование** и нажать кнопку ***Настроить считыватели***. В открывшемся окне **«Управление считывателями»** следует в списке установленных считывателей выбрать пункт ***Все съемные диски*** и нажать кнопку ***Удалить***. После выполнения этого шага обращение СКЗИ к дисководу происходить не будет. Однако, в настройки СКЗИ необходимо отдельно добавить USB-накопитель, который пользователь использует для аутентификации в ОС. Для этого USB-накопитель следует подключить к USB-порту и во вкладке **Оборудование** СКЗИ «КриптоПРО CSP» нажать кнопку ***Настроить считыватели***. Далее в открывшемся окне **«Управление считывателями»** нажать кнопку ***Добавить*** и, следуя указаниям мастера установки считывателя, указать сопоставленный пользователю USB-носитель. Он отобразится в списке ***Доступные считыватели*** как *Дисковод_<буква_диска>*. Однако, следует учесть, что данная настройка будет действовать только для того порта, к которому USB-накопитель был подключен при добавлении считывателя.

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).

Особенности входа в ОС при сбоях в работе персонального межсетевого экрана СЗИ.

При сбоях в работе персонального межсетевого экрана СЗИ «Блокхост-сеть 2.0» возможен вход пользователя в ОС только при выполнении следующих условий:

1. Осуществляется вход пользователя с мандатной меткой равной **1;**
2. Персональный межсетевой экран СЗИ для этого пользователя отключен.

В остальных случаях при входе пользователя в ОС возникнет ошибка (рис. 4.1).

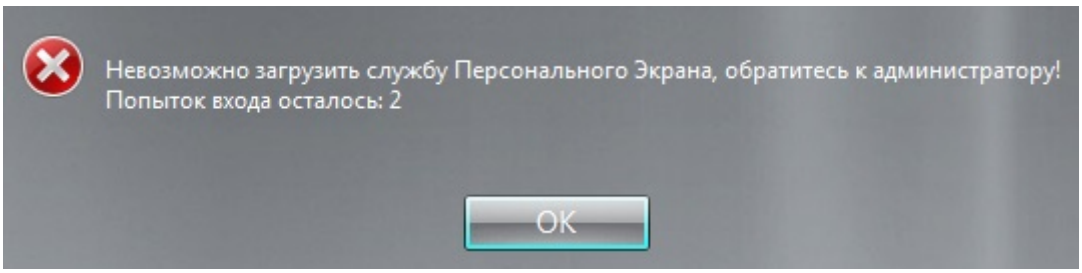


Рисунок 4.1. Ошибка загрузки службы персонального МЭ СЗИ

Для продолжения работы пользователю необходимо либо осуществить вход в ОС с мандатной меткой равной **1**, если для него не включен персональный межсетевой экран СЗИ. Или, если персональный МЭ СЗИ в настройках пользователя включен, то пользователю необходимо обратиться к администратору безопасности, который, осуществив вход от имени учетной записи встроенного администратора, восстановит работоспособность межсетевого экрана СЗИ (подробнее о восстановлении работы персонального МЭ СЗИ см. п. 1.6 настоящего руководства).

4.1.1. Аутентификация в ОС Windows Server 2003

Окно аутентификации в ОС Windows Server 2003 появляется при загрузке системы и при разблокировке рабочей станции и предназначено для ввода данных, необходимых для входа пользователя в систему, защищенную СЗИ «Блокхост-сеть 2.0» (рис. 4.2).

Рисунок 4.2. Окно аутентификации в ОС Windows Server 2003

Окно аутентификации состоит из следующих полей:

- ***Имя пользователя*** – вводится имя (логин) пользователя;

- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***Источник пароля*** – список доступных ключевых носителей (eToken\ SafeNet eToken\ruToken\JaCarta PRO\JaCarta ГОСТ\JaCarta PKI\Avest Token\ ESMART Token\USB-накопитель\ дискета\ персональный идентификатор в реестре);
- ***PIN-код*** – вводится PIN-код выбранного ключевого носителя;
- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально). Имя домена или локального компьютера вводится в зависимости от того, где зарегистрирован входящий в систему пользователь – в домене или на локальном компьютере;
- ***Уровень доступа*** – значение метки доступа, назначенной пользователю для обработки конфиденциальной информации соответствующего уровня (целочисленное значение в диапазоне от 1 до 255).

Если введенное имя пользователя присутствует в СЗИ «Блокхост-сеть 2.0», пароль и персональный идентификатор соответствуют пользователю, а PIN-код позволяет получить доступ к ключевой информации, то после нажатия кнопки ***ОК*** продолжится загрузка ОС. В процессе загрузки на экран будут выводиться сообщения о выполняемых действиях.

В случае незнания PIN-кода или утери персонального идентификатора вход в систему будет невозможен.

В случае трехкратного неправильного ввода идентификационных данных осуществляется перезагрузка ОС.

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

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).

4.1.1.1. Особенности работы с цифровыми сертификатами пользователей

Для настройки такого типа аутентификации необходимо, чтобы в домене уже была настроена возможность входа пользователей в домен по сертификатам типа ГОСТ. Следует отметить, что СЗИ также поддерживает вход по сертификатам типа RSA.

Для организации входа по сертификатам в домене предварительно должен быть развернут Удостоверяющий центр (УЦ) с возможностью выдачи пользователю сертификатов необходимого типа. Шаблон сертификата, с помощью которого возможно организовать выдачу необходимых для входа пользователя сертификатов, называется *smartcard logon.* Для того, чтобы сертификаты имели тип криптографии ГОСТ, шаблон необходимо настроить соответствующим образом. Также для поддержки криптографии типа ГОСТ на контролируемые рабочие станции и ПК с развернутым центром сертификации необходимо установить СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2, в зависимости от используемого в организации криптопровайдера.

Для корректного взаимодействия СКЗИ «КриптоПро CSP с СЗИ «Блокхост-сеть 2.0» необходимо ввести лицензию СКЗИ.

Также необходимо ввести лицензию на «КриптоПро Winlogon».

После выполнения перечисленных условий можно приступить к настройке входа по сертификатам в СЗИ «Блокхост-сеть 2.0».

Необходимо убедиться, что на пользовательский ключевой носитель записан действующий сертификат нужного типа!

Для того, чтобы пользователь смог осуществлять аутентификацию в СЗИ необходимо выполнить следующее (в локальной или серверной консоли администрирования СЗИ):

- добавить в СЗИ учетную запись пользователя, указав при добавлении ключевой носитель, содержащий сертификат пользователя;
- если данный пользователь уже существует в СЗИ, добавить ему ключевой носитель, содержащий цифровой сертификат, используя пункт главного меню ***Управление пользователями →Управление носителями***.

После выполненных действий пользователь сможет войти в СЗИ с использованием носителя, содержащего цифровой сертификат пользователя.

В этом случае для идентификации пользователю необходимо предъявить электронный идентификатор (eToken\SafeNet eToken\JaCarta PRO\JaCarta ГОСТ\JaCarta PKI\Avest Token\eSmart Token\ruToken) с цифровым сертификатом, выбрать его из списка в поле ***Источник пароля***, ввести PIN-код носителя и значение мандатной метки пользователя. Остальные данные будут считаны с носителя автоматически в процессе аутентификации.

Процедура настройки центра сертификации в ОС Windows 2008R2 и получение цифрового сертификата пользователя описаны в Приложении 1 к настоящему руководству.

4.1.2. Аутентификация в ОС Windows Server 2008R2

При аутентификации в ОС Windows Server 2008R2 при загрузке системы предусмотрены следующие виды входа в систему (рис. 4.3):

- 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 4.3. Аутентификация в ОС Windows Server 2008R2

4.1.2.1. 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 следующие поля (рис. 4.4):

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** – вводится имя пользователя;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код доступа к электронному идентификатору ruToken;
- ***Мандатная метка*** – вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки, **равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

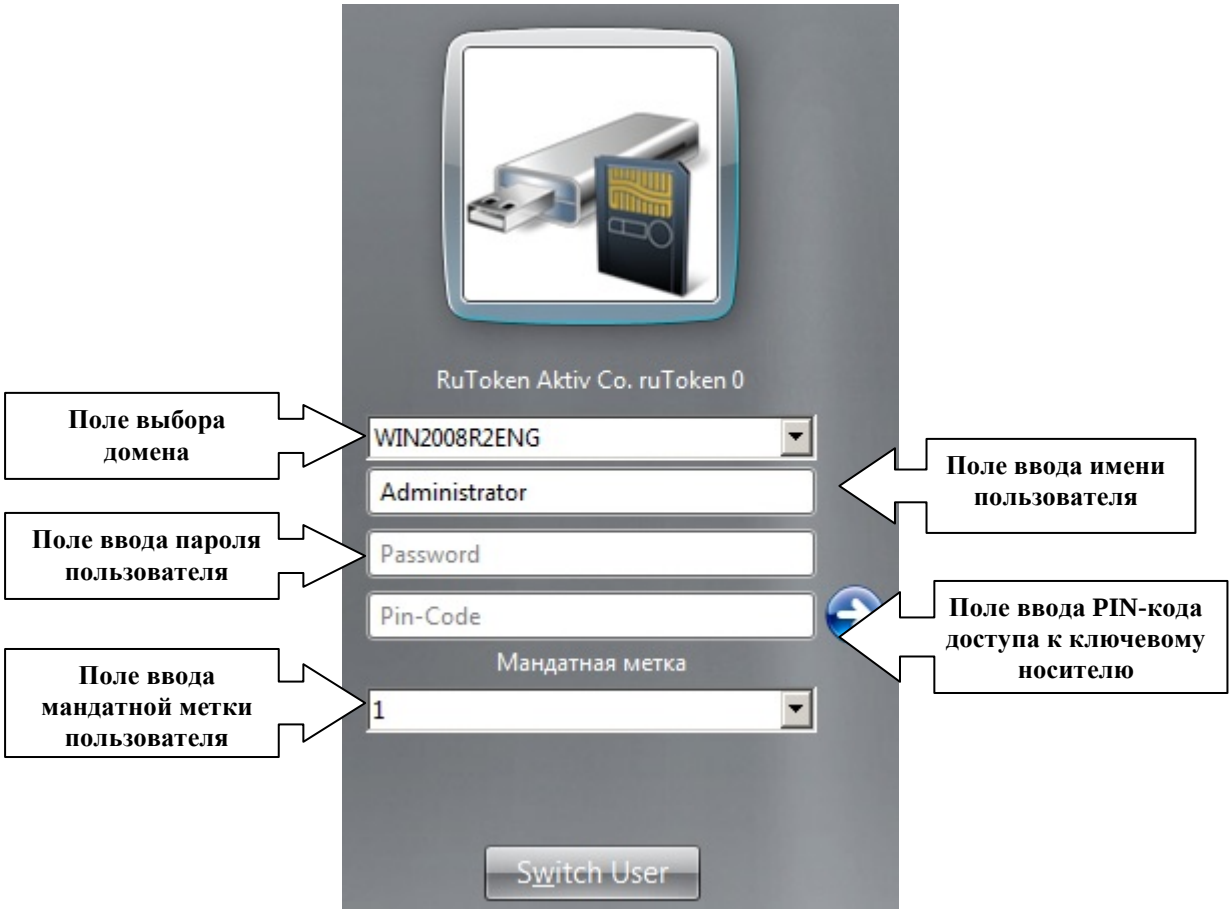


Рисунок 4.4. Аутентификация в ОС Windows Server 2008R2 с предъявлением ruToken

4.1.2.2. 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. 4.3) и заполнить поля (рис. 4.5):

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** – вводится имя пользователя;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки**, равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4.5. Аутентификация в ОС Windows Server 2008R2 с предъявлением eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI

4.1.2.3. Аутентификация с предъявлением электронного идентификатора Avest Token

Для аутентификации с предъявлением электронного идентификатора Avest Token необходимо подключить электронный идентификатор AvBign, затем нажать кнопку ***Avest AVEST-SYSTEMS <Имя носителя>*** (рис. 4.3) и заполнить поля (рис. 4.6):

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** – вводится имя пользователя;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки**, равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4.6. Аутентификация в ОС Windows Server 2008R2 с предъявлением Avest Token

4.1.2.4. 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. 4.3) и заполнить поля (рис. 4.7):

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** – вводится имя пользователя;
- ***Пароль*** – вводится пароль, соответствующий введенному имени пользователя;
- ***PIN-код*** – вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** – вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки**, равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4.7. Аутентификация в ОС Windows Server 2008R2 с предъявлением ESmart Token

4.1.2.5. 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. 4.3) и заполнить поля (рис. 4.8):

- ***Домен*** **–** имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** **–** вводится имя пользователя;
- ***Пароль*** **–** вводится пароль, соответствующий введенному имени пользователя**;**
- ***PIN-код*** **–** вводится PIN-код электронного идентификатора;
- ***Мандатная метка*** **–** вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки, **равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4.8. Аутентификация в ОС Windows Server 2008R2 с предъявлением отчуждаемого носителя

4.1.2.6. 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 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. 4.3). В появившемся окне нужно выбрать подключенный носитель в списке, ввести PIN-код доступа к нему и значение мандатной метки пользователя (рис. 4.9) (независимо от значения мандатной метки пользователя в СЗИ, **первый вход в ОС** он должен выполнить, указав значение метки, **равное 1**, это необходимо для корректного создания профиля пользователя операционной системой). Остальные данные пользователя будут автоматически считаны с носителя.

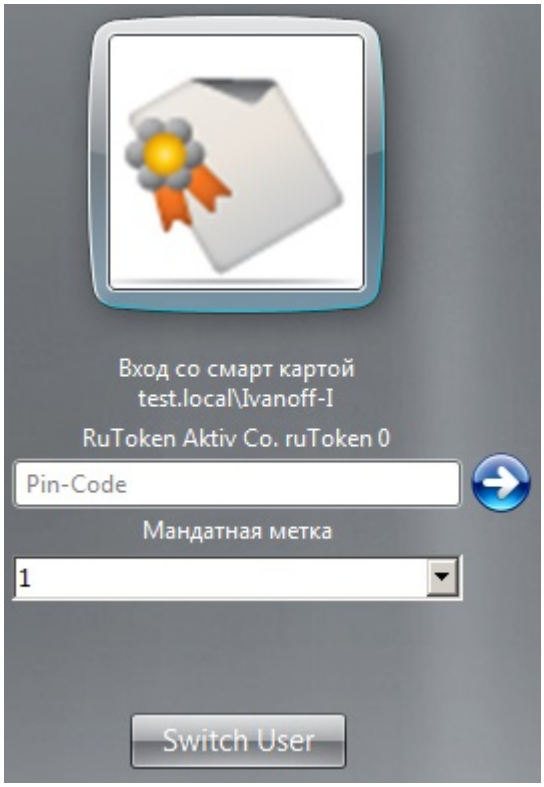


Рисунок 4.9. Вход ОС Windows Server 2008R2 по сертификату

Процедура настройки центра сертификации в ОС Windows 2008R2 и получение цифрового сертификата пользователя описаны в Приложении 1 к настоящему руководству.

4.1.2.7. 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. 4.3) и заполнить поля (рис. 4.10):

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация пользователя стандартными средствами ОС Windows (на контроллере домена или локально);
- ***Имя пользователя*** – вводится имя пользователя;
- ***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*** – вводится значение мандатной метки пользователя. Независимо от значения мандатной метки пользователя, **первый вход в ОС** он должен выполнить, указав значение метки**, равное 1**. Это необходимо для корректного создания профиля пользователя операционной системой.

Рисунок 4.10. Аутентификация в ОС Windows Server 2008R2 с предъявлением персонального идентификатора, хранящегося в реестре Windows

4.1.2.8. Вход Администратора

В СЗИ «Блокхост-сеть 2.0» существует возможность входа в ОС встроенного в ОС администратора по паролю без предъявления ключевого носителя. Для этого необходимо нажать кнопку ***Вход пользователя*** (см. рис. 4.3) и заполнить поля, показанные на рисунке 4.11:

- ***Домен*** – имя домена или локального компьютера, на котором будет осуществлена аутентификация администратора стандартными средствами ОС Windows (на контроллере домена (учетная запись встроенного администратора контроллера домена) или локально);
- ***Имя пользователя*** – вводится имя встроенного администратора;
- ***Пароль*** – вводится пароль встроенного администратора.

Рисунок 4.11. Вход администратора в ОС Windows Server 2008R2

4.1.3. Аутентификация в ОС Windows Server 2012/2012R2

При аутентификации в ОС Windows Server 2012/2012R2 при загрузке системы предусмотрены следующие виды входа в систему (рис. 4.12 и 4.13):

- 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.

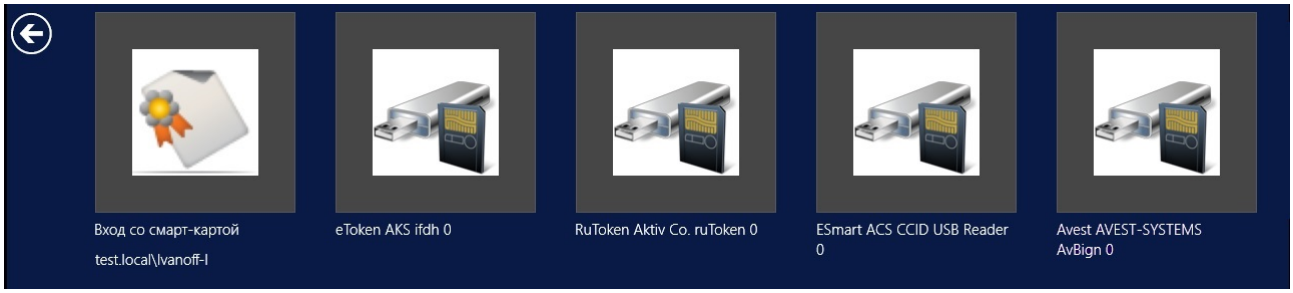


Рисунок 4.12. Аутентификация в ОС Windows Server 2012/2012R2

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

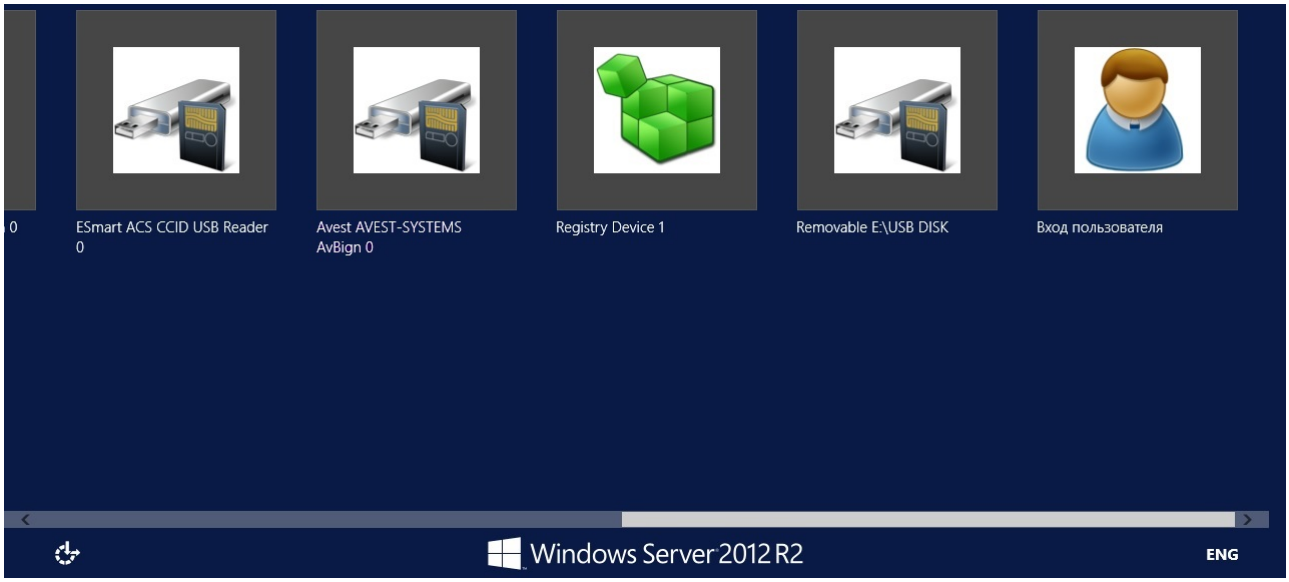


Рисунок 4.13. Аутентификация в ОС Windows Server 2012/2012R2

4.1.3.1 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. 4.14). Подробное описание назначения полей приведено в п. 4.1.2.1 настоящего руководства.

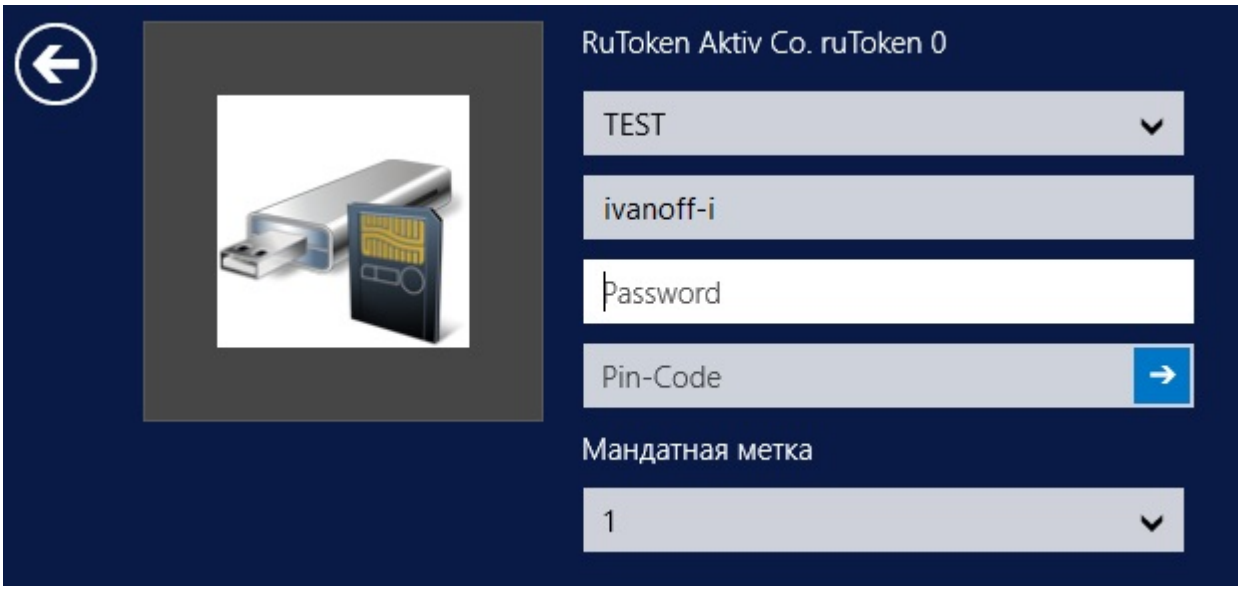


Рисунок 4.14. Аутентификация в ОС Windows Server 2012/2012R2 с предъявлением ruToken

4.1.3.2 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. 4.12) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 4.15). Подробное описание назначения полей приведено в п. 4.1.2.2 настоящего Руководства.

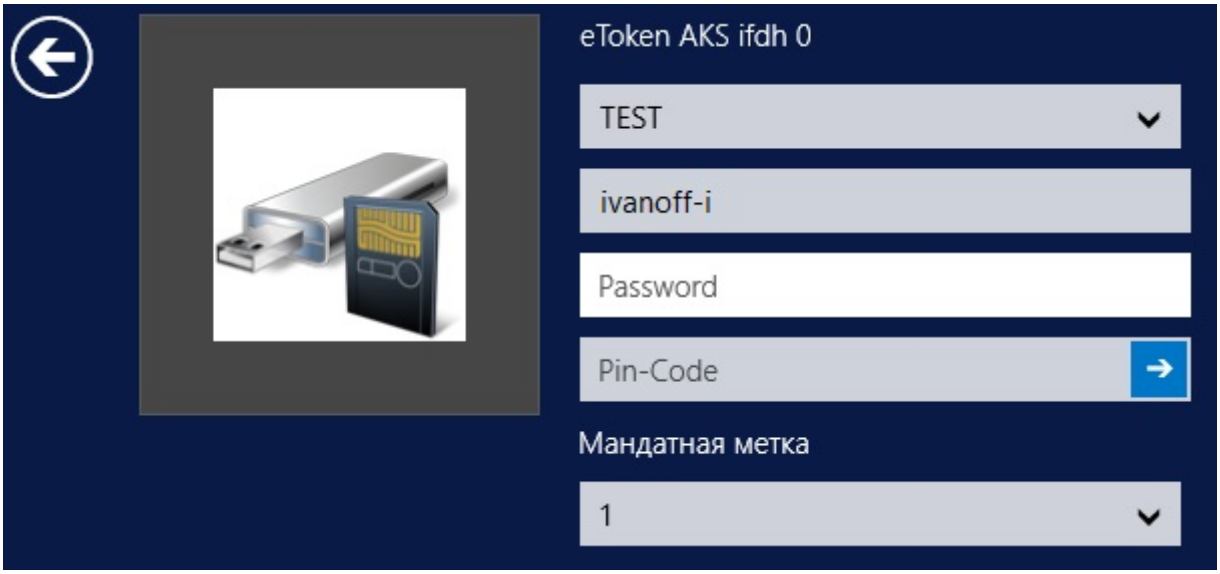


Рисунок 4.15. Аутентификация в ОС Windows Server 2012/2012R2
с предъявлением eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI

4.1.3.3 Аутентификация с предъявлением электронного идентификатора Avest Token

Для аутентификации с предъявлением электронного идентификатора Avest Token необходимо подключить электронный идентификатор AvBign, затем нажать кнопку ***Avest AVEST-SYSTEMS <Имя носителя>*** (рис. 4.12) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 4.16). Подробное описание назначения полей приведено в п. 4.1.2.3 настоящего Руководства.

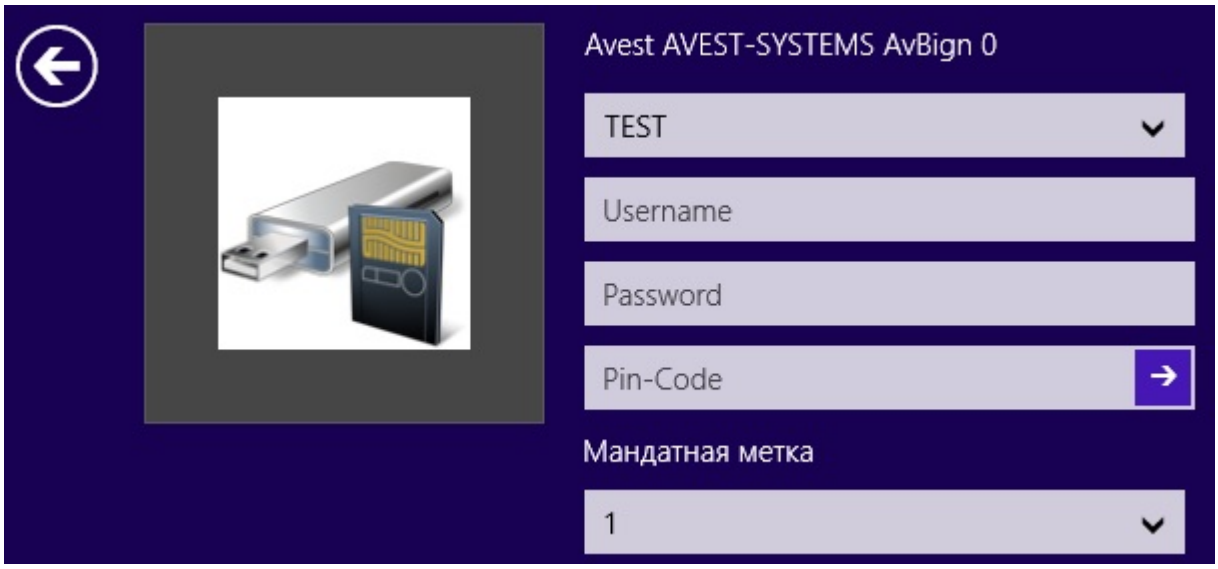


Рисунок 4.16. Аутентификация в ОС Windows Server 2012/2012R2 с предъявлением Avest Token

4.1.3.4 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. 4.12) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 4.17). Подробное описание назначения полей приведено в п. 4.1.2.4 настоящего Руководства.

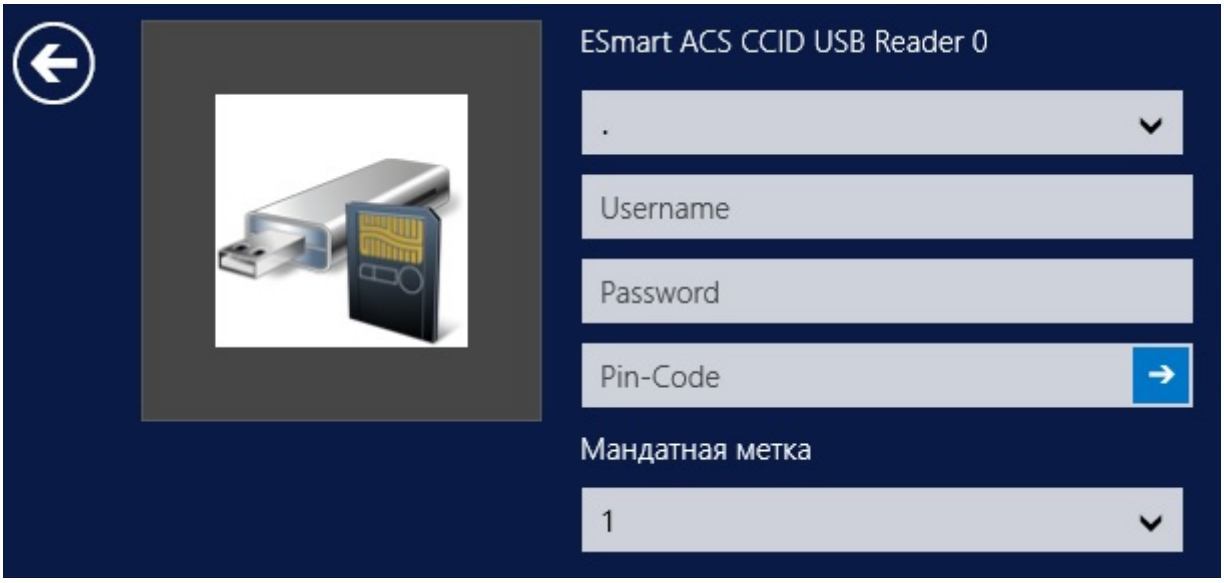


Рисунок 4.17. Аутентификация в ОС Windows Server 2012/2012R2 с предъявлением ESmart Token

4.1.3.5 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. 4.13) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 4.18). Подробное описание назначения полей приведено в п. 4.1.2.5 настоящего Руководства.

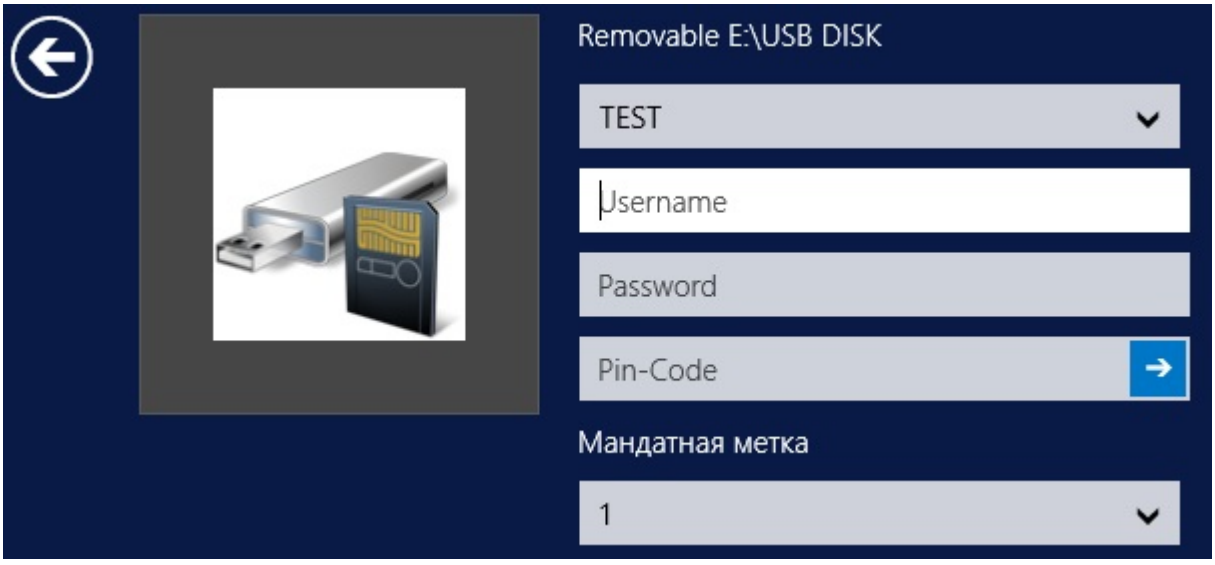


Рисунок 4.18. Аутентификация в ОС Windows Server 2012/2012R2
с предъявлением отчуждаемого носителя

4.1.3.6 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. 4.12). В открывшемся диалоговом окне идентификации пользователя нужно в соответствующие поля ввести PIN-код доступа к подключенному носителю и значение мандатной метки пользователя:

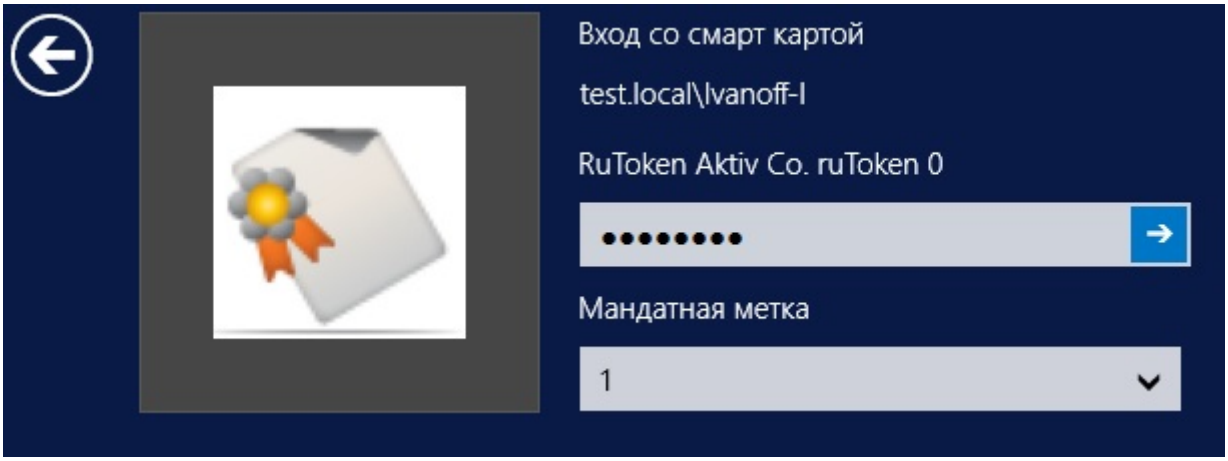


Рисунок 4.19. Вход в ОС Windows Server 2012/2012R2 по сертификату

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

4.1.3.7 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. 4.13) и заполнить все поля в диалоговом окне аутентификации пользователя (рис. 4.20). Подробное описание назначения полей приведено в п. 4.1.2.7 настоящего Руководства.

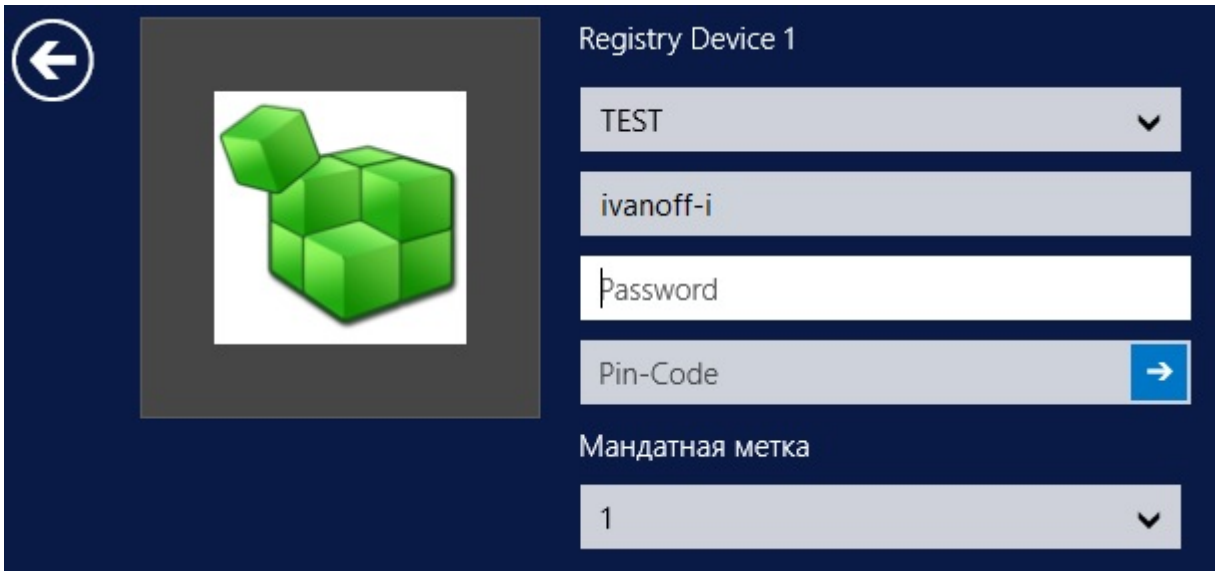


Рисунок 4.20. Аутентификация в ОС Windows 8/8.1/2012/2012R2 с предъявлением персонального идентификатора, хранящегося в реестре Windows

4.1.3.8 Вход Администратора

В СЗИ «Блокхост-сеть 2.0» существует возможность входа в ОС встроенного в ОС администратора по паролю без предъявления ключевого носителя. Для этого необходимо нажать кнопку ***Вход пользователя*** (см. рис. 4.13) и заполнить поля, показанные на рисунке 4.21. Подробное описание назначения полей диалогового окна аутентификации встроенного администратора приведено в п. 4.1.2.8 настоящего Руководства.

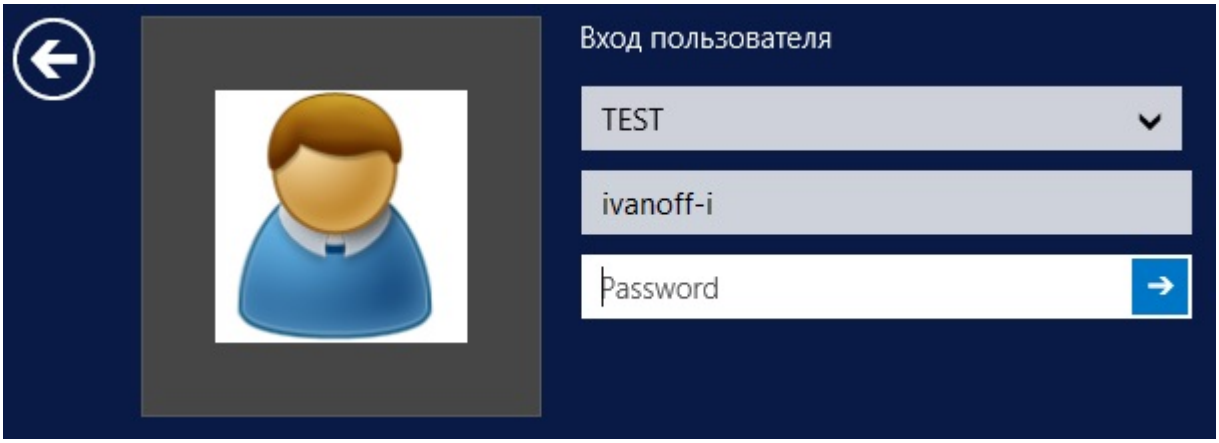


Рисунок 4.21. Вход Администратора в ОС Windows Server 2012/2012R2

4.2. Виды входа в ОС

Чтобы войти в систему с установленным СЗИ «Блокхост-сеть 2.0», необходимо ввести имя пользователя и пароль, а также «предъявить» персональный идентификатор (см. п. 1.4) 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.

Дополнительно в СЗИ «Блокхост-сеть 2.0» реализована функция ***Автовход***, которая позволяет осуществлять вход пользователю в систему без ввода данных в окно аутентификации СЗИ «Блокхост-сеть 2.0». После включения данной опции происходит автоматическая загрузка ОС под учетной записью указанного пользователя. Подробнее работа функции ***Автовход*** рассмотрена в п.4.2.3 настоящего руководства.

4.2.1. Стандартная аутентификация

После появления приглашения на вход в систему (рис. 4.2, 4.3, 4.12) 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 7/8/8.1/2008R2/2012/2012R2 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.

4.2.2. Вход 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 4.3, а порядок сохранения пароля на персональный идентификатор пользователя – в разделе 4.4 настоящего руководства.

После появления приглашения на вход в систему (окно приглашения входа в систему описано в пунктах 4.1.1, 4.1.2 и 4.1.3 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 (при входе в ОС Windows 7/8/8.1/2008/2008R2/2012/2012R2);
- заполнить поля ***Домен***, ***Имя пользователя***, ***PIN-код*** и ***Уровень доступа*** (***Мандатная метка***);
- поле ввода пароля оставить пустым;
- нажать кнопку ***ОК***.

Реакция СЗИ на такие действия зависит от информации о пароле, содержащейся в персональном идентификаторе. Возможны следующие варианты:

- персональный идентификатор содержит актуальный пароль;
- 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 в персональный идентификатор);
- в 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, на экране появится сообщение о неверном пароле. Для входа в ОС необходимо перейти к окну выбора идентификатора и выбрать необходимый тип идентификатора. В открывшемся окне (см. пример на рис. 4.22) 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.

При входе в ОС Windows XP/2003, с сохраненным на персональном идентификаторе паролем, *доменному пользователю* необходимо ввести *полное имя домена* (в примере на рисунке 4.22 – *test1.local*).

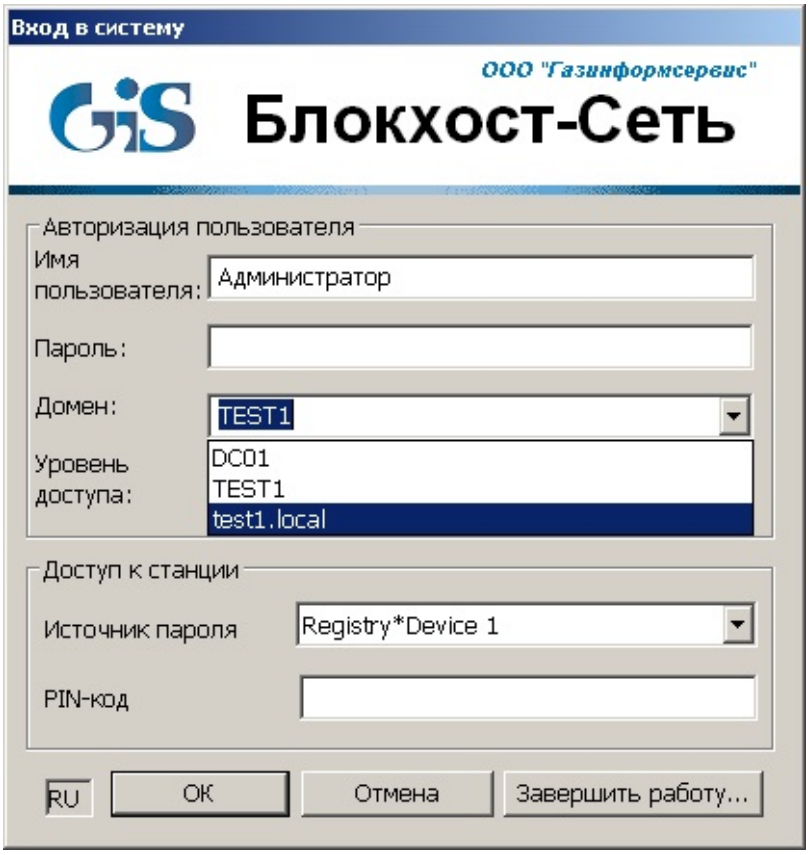
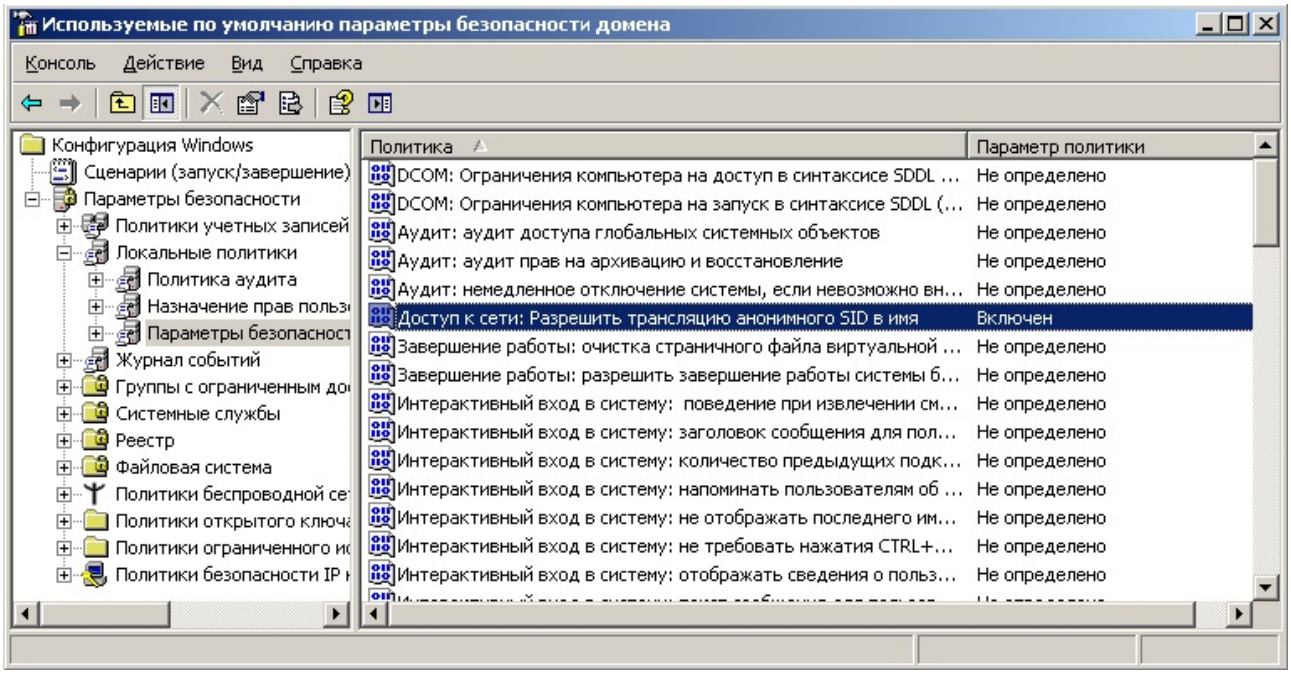
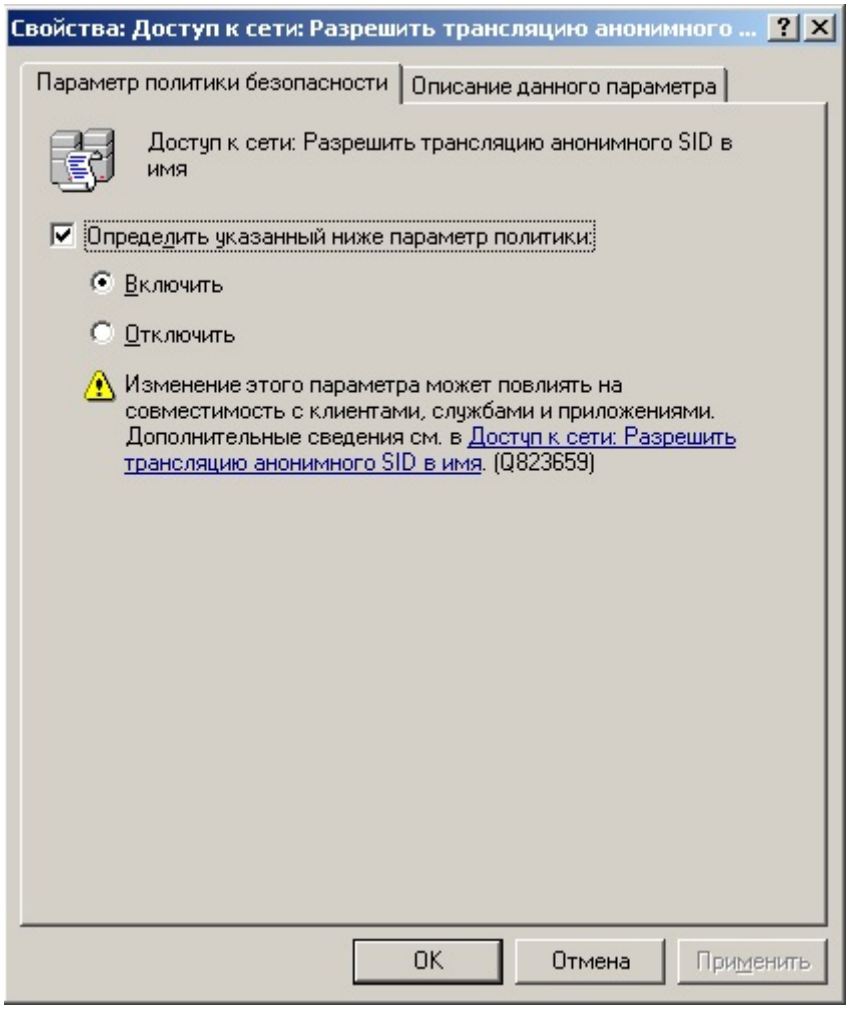


Рисунок 4.22. Выбор полного имени домена при входе в систему по персональному идентификатору

Для корректной работы механизма входа на контролируемую рабочую станцию по персональному идентификатору, с сохраненным на нём паролем, на контроллере домена должен быть включен параметр политики безопасности домена ***Доступ к сети: Разрешить трансляцию анонимного SID в имя*** (***Пуск →Администрирование →Политика безопасности домена***, в окне редактирования параметров безопасности домена (рис. 4.23, а) выбрать пункт ***Параметры безопасности →Локальные политики →Параметры безопасности*** в списке параметров безопасности два раза щелкнуть левой кнопкой мыши по параметру ***Доступ к сети: Разрешить трансляцию анонимного SID в имя*** и в открывшемся окне свойств (рис. 4.23, б) отметить параметры ***Определить указанный ниже параметр политики*** и ***Включить***).



а)



б)

Рисунок 4.23. Включение параметра «Разрешить трансляцию анонимного SID в имя»

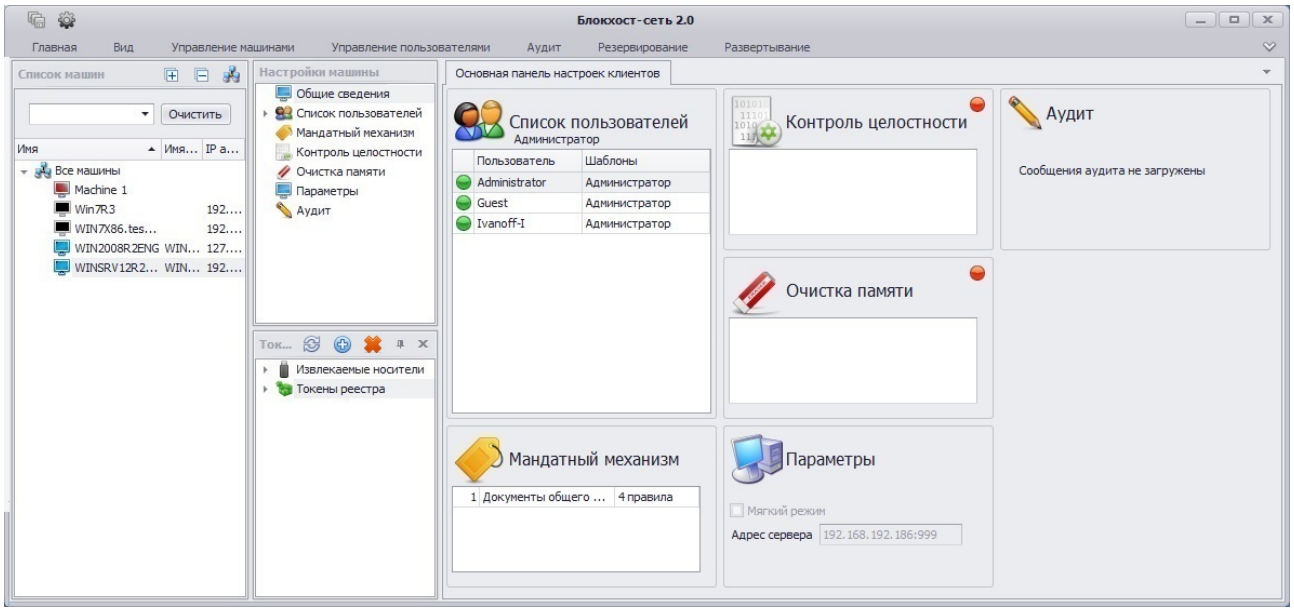
В случае аутентификации пользователя с использованием цифровых сертификатов, записанных на eToken/SafeNet eToken/JaCarta PRO/JaCarta ГОСТ/JaCarta PKI/Avest Token/ruToken, необходимо ввести PIN-код доступа к носителю и указать значение мандатной метки пользователя. Остальные данные будут считаны с носителя автоматически.

4.2.3. Автовход в ОС

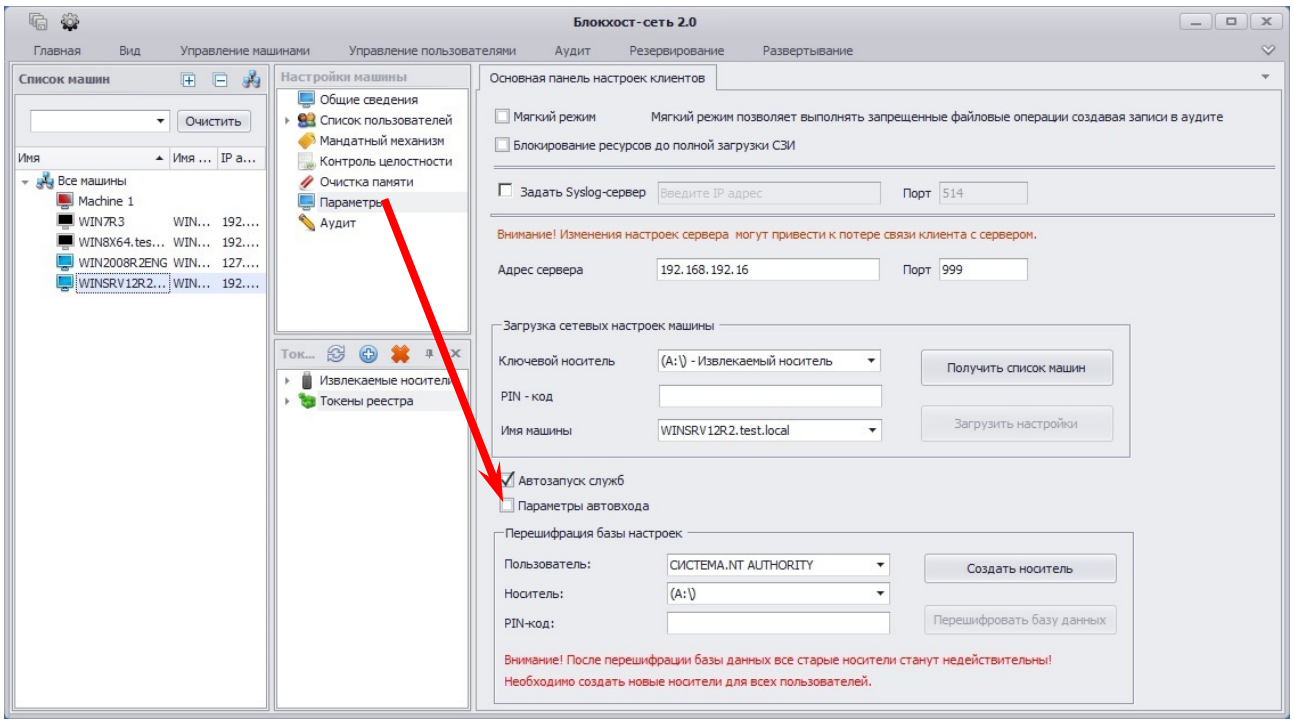
В СЗИ «Блокхост-сеть 2.0» доступна функция ***Автовход***. Она позволяет организовать вход пользователя в систему без отображения окна аутентификации СЗИ «Блокхост-сеть 2.0». При активации этой функции включение/перезагрузка компьютера (с подключенным персональным идентификатором пользователя) приводит к автоматической загрузке ОС под учетной записью указанного пользователя.

Для настройки функции ***Автовход*** администратору безопасности необходимо:

1. Сохранить пароль пользователя, от имени которого будет осуществляться автоматический вход в ОС, на его персональный идентификатор (подробнее о способах сохранения пароля пользователя на персональный идентификатор см. раздел 4.4 и пункт 5.3.2 настоящего руководства);
2. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка параметров функции ***Автовход***;
3. В **Основной панели настроек клиентов** щелкнуть по названию ***Параметры*** или в окне **«Настройки машины»** выбрать пункт ***Параметры*** (рис. 4.24, а). В обоих случаях в **Основной панели настроек клиентов** отобразятся настраиваемые параметры контролируемой рабочей станции (рис. 4.24, б);



а)



б)

Рисунок 4.24. Отображение настраиваемых параметров рабочей станции

4. В **Основной панели настроек клиентов** отметить параметр ***Параметры автовхода***;
5. В появившейся области ввода параметров автовхода (рис. 4.25):
   - выбрать из выпадающего списка поля ***Пользователь*** имя пользователя;
   - выбрать из выпадающего списка поля ***Ключевой носитель*** персональный идентификатор пользователя;
   - в поле ***PIN-код*** ввести PIN-код доступа к выбранному ключевому носителю.

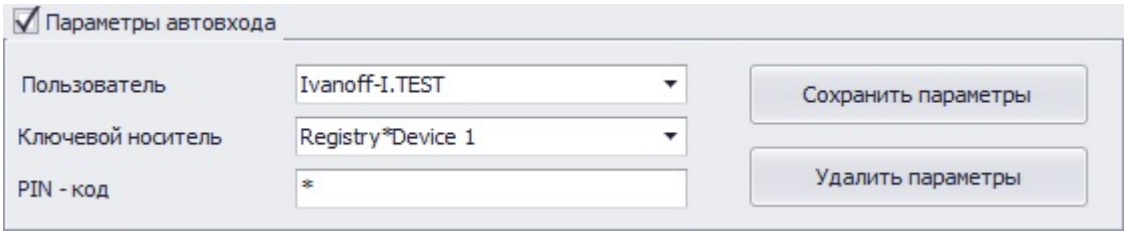


Рисунок 4.25. Область ввода параметров автовхода

По умолчанию в области настройки функции ***Автовход*** отсутствует поле ввода мандатной метки входа и пользователю устанавливается мандатная метка равная **1**. При необходимости настройки автовхода пользователя с мандатной меткой отличной от **1**, необходимо нажать сочетание клавиш **<Ctrl>+<M>** - появится поле ввода мандатной метки, в котором можно установить необходимое значение мандатной метки входа.

6. Для сохранения произведенных настроек нажать кнопку ***Сохранить параметры***, расположенную в области ввода параметров автовхода (см. рис. 4.25). Появится сообщение об успешном сохранении настроек (рис. 4.26). При этом соответствующие изменения будут внесены в реестр редактируемой рабочей станции и после перезагрузки ОС (завершения текущего сеанса) будет

автоматически выполняться вход в операционную систему от имени учетной записи указанного пользователя без появления диалогового окна ввода идентификационных данных СЗИ «Блокхост-сеть 2.0».

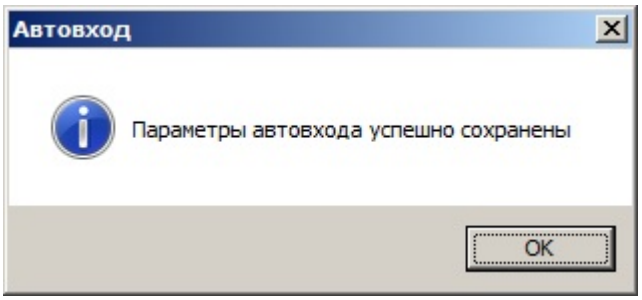


Рисунок 4.26. Информационное сообщение о сохранении параметров.

При выполнении автовхода к рабочей станции должен быть подключен персональный идентификатор пользователя, от имени которого осуществляется вход в систему.

Для отмены возможности автоматической загрузки ОС на контролируемой рабочей станции от имени учетной записи пользователя необходимо в **Основной панели настроек клиентов** в области ввода параметров автовхода нажать кнопку ***Удалить параметры*** (см. рис. 4.25). При этом в реестр редактируемой рабочей станции будут внесены соответствующие изменения, и появится сообщение об удалении параметров автовхода:

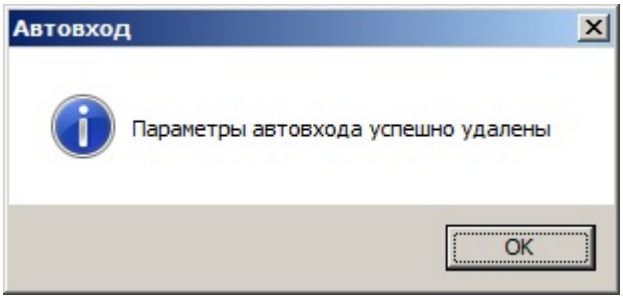


Рисунок 4.27. Информационное сообщение о сохранении параметров.

4.3. Операция смены пароля

Выполнить операцию смены пароля пользователя можно следующими способами:

- самим пользователем – через диалоговое окно СЗИ «Блокхост-сеть 2.0»;
- администратором безопасности – из консоли администрирования СЗИ «Блокхост-сеть 2.0».

4.3.1. Смена пароля через диалоговое окно «Блокхост-сеть 2.0»

4.3.1.1. *Смена пароля в ОС Windows Server 2003*

Для смены пароля текущего пользователя через диалоговое окно **«Смена пароля»** СЗИ «Блокхост-сеть 2.0» необходимо:

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**. На экране появится диалоговое окно СЗИ «Блокхост-сеть 2.0» (рис. 4.28);

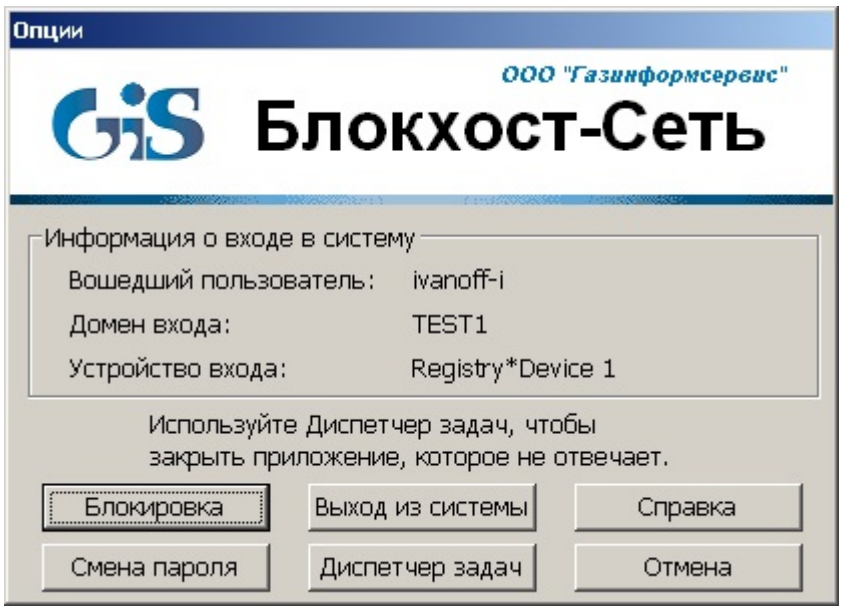


Рисунок 4.28. Диалоговое окно СЗИ «Блокхост-сеть 2.0»

2) нажать кнопку ***Смена пароля***. На экране появится диалоговое окно смены пароля:

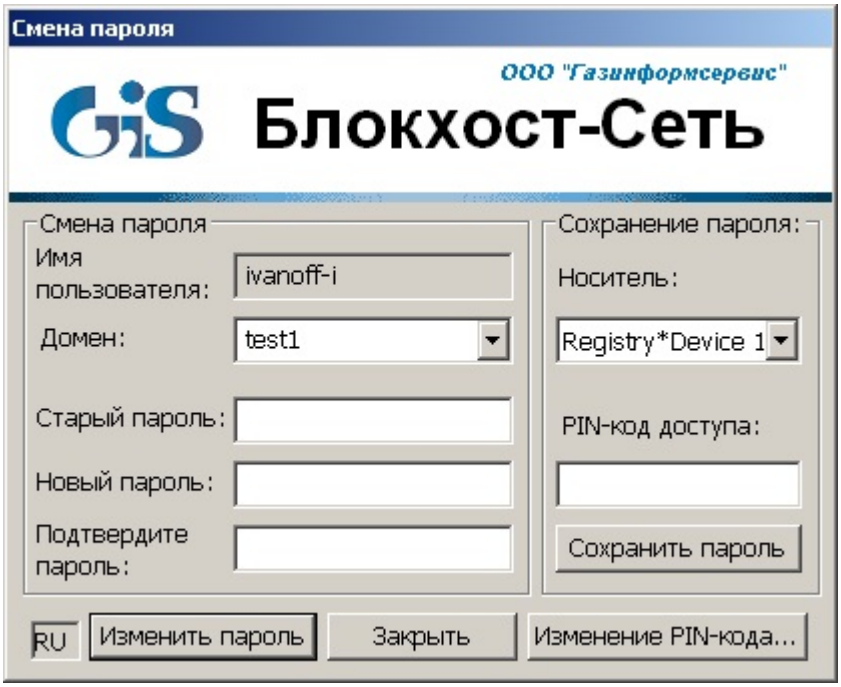


Рисунок 4.29. Диалоговое окно смены пароля в ОС Windows Server 2003

3) в окне **«Смена пароля»** ввести:
   - в поле ввода ***Старый пароль*** ввести текущий пароль пользователя;
   - в поле ввода ***Новый пароль*** ввести новый пароль пользователя;
   - повторить ввод нового пароля в поле ввода ***Подтвердите пароль***;
4) нажать кнопку ***Изменить пароль*** для запуска процедуры смены пароля.
5) нажать кнопку ***ОК*** в окне с сообщением об успешной смене пароля пользователя.

После изменения пароля и подтверждения успешной смены пароля на экране монитора останется диалоговое окно **«Смена пароля»**. Для выхода из данного окна следует нажать кнопку ***Закрыть***, далее в окне **«Опции»** – кнопку ***Отмена***. Также необходимо помнить о возможности сохранения пароля на носитель, которое осуществляется выбором соответствующего пункта в окне **«Смена пароля».** Если пароль уже был сохранен на носителе, то после его изменения требуется повторно сохранить пароль.

4.3.1.2. *Смена пароля в ОС Windows Server 2008R2*

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

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
2) нажать кнопку-ссылку ***Сменить пароль*** (***Change a password***);
3) в открывшемся диалоге нажать кнопку ***Смена пароля*** с иконкой персонального идентификатора пользователя:

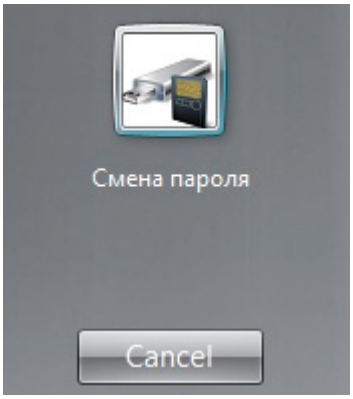


Рисунок 4.30. Выбор носителя для смены пароля в ОС Windows Server 2008R2

4) в открывшемся диалоге смены пароля заполнить поля ***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***:

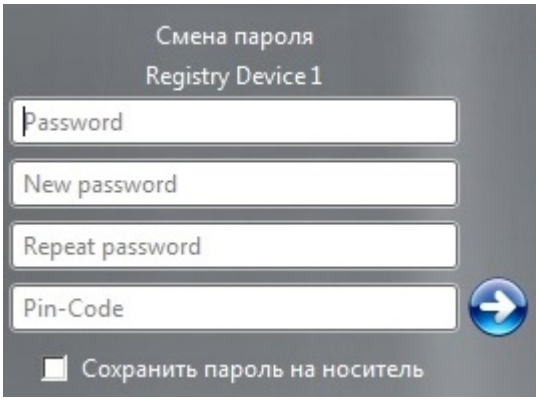


Рисунок 4.31. Диалоговое окно смены пароля в ОС Windows Server 2008R2

5) ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;
6) при необходимости сохранения нового пароля пользователя на ключевом носителе отметить параметр ***Сохранить пароль на носитель***;
7) 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.

4.3.1.3. *Смена пароля в ОС Windows Server 2012/2012R2*

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

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
2) нажать кнопку ***Сменить пароль*** (***Change a password***);
3) в открывшемся диалоге нажать кнопку ***Смена пароля*** с иконкой персонального идентификатора пользователя:

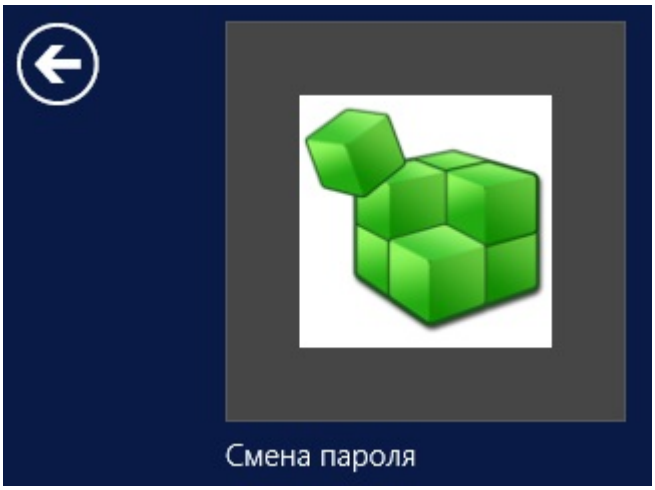


Рисунок 4.32. Выбор носителя для смены пароля в ОС Windows Server 2012/2012R2

4) в открывшемся диалоге смены пароля (рис. 4.33) заполнить поля ***Текущий пароль***, ***Новый пароль***, ***Подтверждение пароля***.

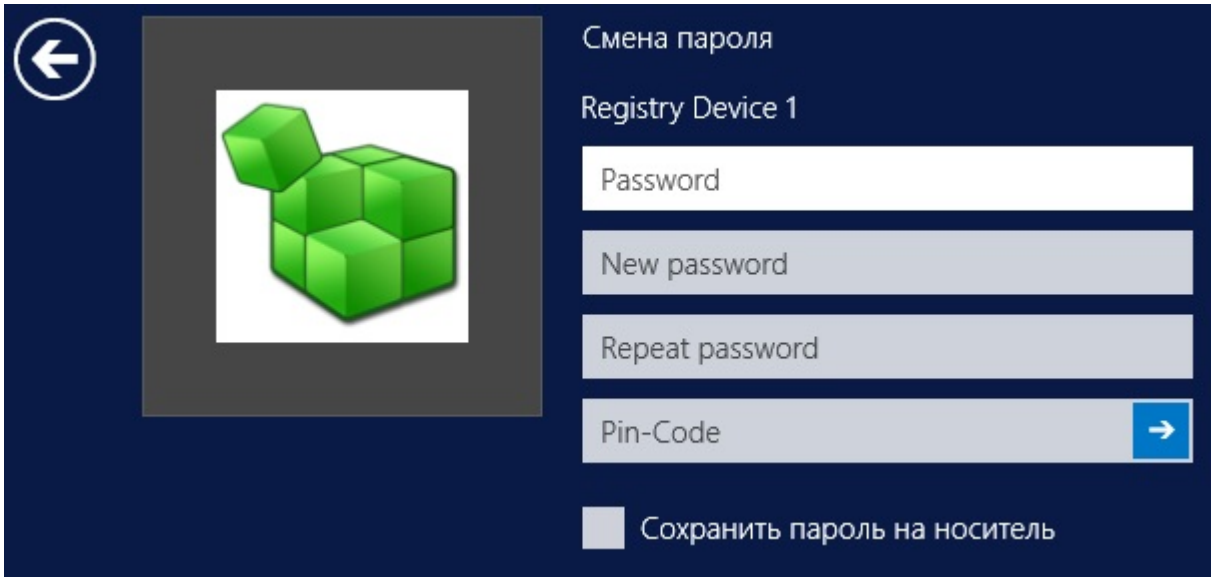


Рисунок 4.33. Диалоговое окно смены пароля в ОС Windows Server 2012/2012R2

5) ввести PIN-код доступа к ключевому носителю в поле ввода ***PIN-код***;
6) при необходимости сохранения нового пароля пользователя на ключевом носителе отметить параметр ***Сохранить пароль на носитель***;
7) 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.

4.3.2. Смена пароля через консоль администрирования СЗИ Блокхост-сеть 2.0»

В СЗИ «Блокхост-сеть 2.0» существует возможность смены пароля пользователя, зарегистрированного в СЗИ на контролируемой рабочей станции, из серверной консоли администрирования. Подробно процесс смены пароля пользователя, зарегистрированного в СЗИ на контролируемой рабочей станции, контролируемой рабочей станции рассмотрен в п. 5.3.1 «Изменение общих параметров пользователя» настоящего руководства.

После операции смены пароля из серверной консоли администрирования СЗИ администратор безопасности должен сообщить пользователю новый пароль.

Если пароль пользователя был изменен вне СЗИ «Блокхост-сеть 2.0» (например, средствами администрирования на контроллере домена), то при первом после смены пароля входе пользователя в ОС автоматически запустится мастер синхронизации паролей, и после ввода прежнего пароля он будет заменен в СЗИ на новый пароль, заданный в ОС Windows.

4.4. Запись пароля пользователя на персональный идентификатор

Необходимость сохранения пароля на персональном идентификаторе может обуславливаться требованиями к сложности пароля, принятыми в организации с целью невозможности его подбора (например, пароль, состоящий из двадцати случайных символов, пользователю сложно будет запомнить, а затем каждый раз вводить при аутентификации). При сохранении пароля на идентификаторе пользователю не нужно будет вводить его каждый раз при входе в ОС – его значение будет автоматически считываться из персонального идентификатора.

Процедура входа в систему с предъявлением персонального идентификатора с сохраненным паролем описана в пункте 4.2.2 настоящего руководства.

4.4.1. Сохранение пароля пользователя в ОС Windows XP/2003

Для записи текущего пароля пользователя на персональный идентификатор в ОС Windows XP/2003 необходимо:

- нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
- в открывшемся окне (см. рис. 4.28) нажать кнопку ***Смена пароля***;
- в окне **«Смена пароля»** (см. рис. 4.29) в поле ***Старый пароль*** ввести действующий пароль пользователя, поля ***Новый пароль*** и ***Подтвердите пароль*** оставить пустыми;
- из выпадающего списка поля ***Носитель*** выбрать персональный идентификатор пользователя и ввести PIN-код доступа к нему в соответствующее поле;
- нажать кнопку ***Сохранить пароль***;
- если PIN-код доступа к носителю и пароль пользователя были введены правильно, то пароль текущего пользователя будет записан на указанный персональный идентификатор.

4.4.2. Сохранение пароля пользователя в ОС Windows Vista/7/2008/2008R2/8/8.1/2012/2012R2

Для записи текущего пароля пользователя на носитель, с которым был осуществлен вход пользователя в ОС Windows Vista/7/2008/2008R2/8/8.1/2012/2012R2, необходимо:

- нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
- в отобразившемся меню нажать кнопку-ссылку ***Сменить пароль*** (***Change a password***);
- в открывшемся диалоге нажать кнопку с иконкой персонального идентификатора (см. примеры на рис. 4.30, 4.32)
- в открывшемся диалоге смены пароля (см. примеры на рис. 4.28, 4.30) 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.

Один персональный идентификатор может хранить пароли различных пользователей. Для этого необходимо выполнить процедуру сохранения пароля на персональный идентификатор для каждого пользователя.
Если в дальнейшем пароль пользователя будет изменен, то для возможности его автоматического считывания механизмом аутентификации СЗИ необходимо заново провести операцию сохранения пароля пользователя на персональный идентификатор.

4.5. Операция изменения 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 2.0» не следует использовать символы русского алфавита.

4.5.1. Изменение PIN-кода через диалоговое окно «Блокхост-сеть 2.0»

4.5.1.1. Изменение PIN-кода в ОС Windows XP/2003

Для изменения PIN-кода через диалоговое окно **«Смена пароля»** СЗИ «Блокхост-сеть 2.0» необходимо:

1) нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**, и в открывшемся диалоговом окне (см. рис. 4.28) выбрать пункт ***Изменить пароль***;
2) в открывшемся окне **«Смена пароля»** нажать кнопку ***Изменение PIN-кода*** (см. рис. 4.29);
3) в окне **«Смена PIN-кода»** заполнить поля ***Старый PIN-код***, ***Новый***, ***Подтверждение*** и нажать кнопку ***Изменить*** (рис. 4.34);

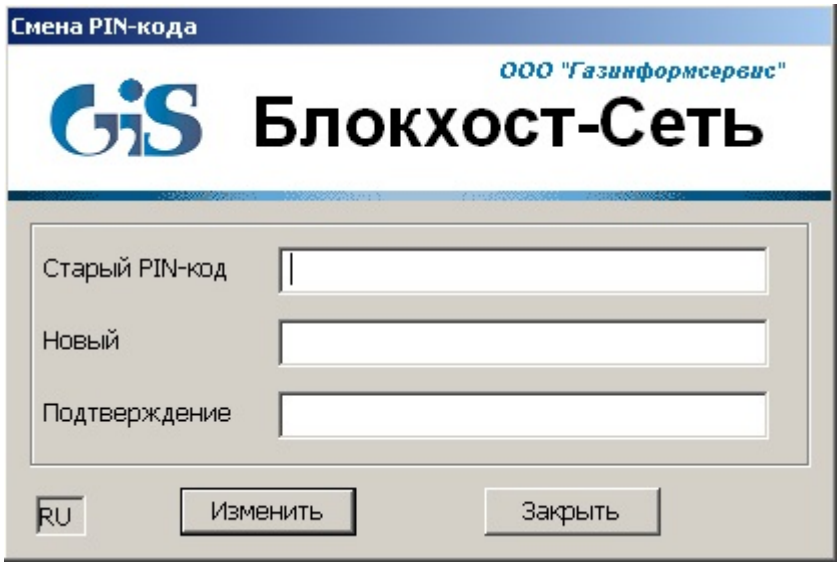


Рисунок 4.34. Диалоговое окно «Смена PIN-кода»

4) в случае успешного изменения PIN-кода на экране появится соответствующее сообщение.

4.5.1.2. Изменение PIN-кода в ОС Windows 2008R2/Vista/7/8/8.1/2012/2012R2

Возможность изменения пользователем PIN-кода доступа к ключевым носителям в ОС Windows 2008R2/Vista/7/8/8.1/2012/2012R2 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 консоли администрирования СЗИ (подробнее о процессе смены PIN-кода доступа к персональному идентификатору из консоли администрирования СЗИ см. пункт 6.2.5 «Идентификаторы входа» настоящего руководства).

4.5.2. Изменение PIN-кода через консоль администрирования

PIN-код персонального идентификатора пользователя может быть также изменен администратором безопасности во вкладке **Настройки токена** серверной консоли администрирования СЗИ. Подробное описание работы во вкладке **Настройки токена** приведено в пункте 6.2.5. «Механизм идентификаторов входа» настоящего документа.

В случае изменения PIN-кода электронного идентификатора (через консоль администрирования СЗИ или с использованием диалогового окна СЗИ «Блокхост-сеть 2.0» (для ОС Windows XP/2003)) может появиться окно о невозможности смены PIN-кода или о неудовлетворении PIN-кода требованиям установленной политики безопасности. Данная ситуация возникает из-за особенностей политики задания PIN-кода на носителе, которые приведены в документации на носитель (при наличии таковых особенностей).

4.6. Блокировка компьютера, смена пользователя, завершение работы

Если появляется необходимость временного перерыва в работе пользователя за компьютером, то для защиты от несанкционированного использования компьютера можно воспользоваться функцией его временной блокировки.

4.6.1. Блокировка и разблокировка компьютера в ОС Windows XP/2003

Для временной блокировки компьютера вручную:

1. Нажмите комбинацию клавиш **<Ctrl>+<Alt>+<Del>.**
2. Нажмите кнопку ***Блокировка*** в появившемся на экране диалоге (см. рис. 4.28).
3. Клавиатура и экран монитора будут заблокированы, на экране появится сообщение:

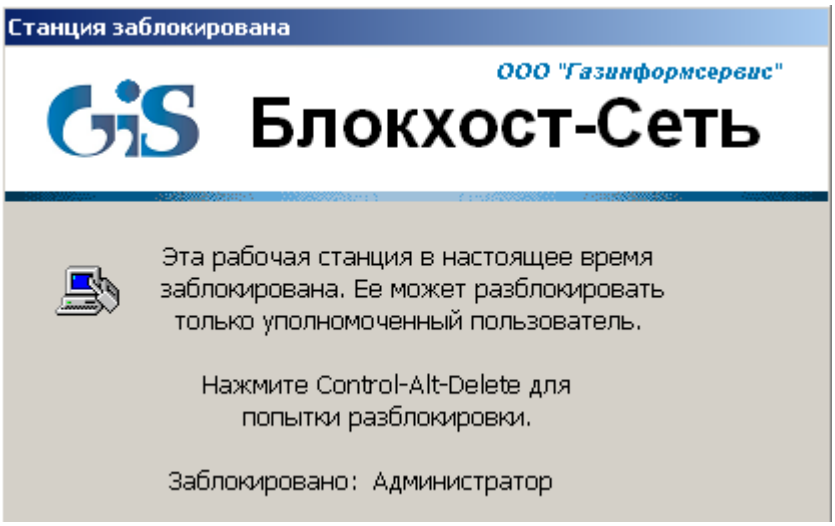


Рисунок 4.35. Сообщение на заблокированной станции

Разблокировать компьютер может только работающий на нем пользователь или администратор рабочей станции. Разблокирование компьютера администратором сопровождается завершением текущего сеанса работы пользователя и потерей всех несохраненных данных пользователя.

Для разблокирования компьютера необходимо нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**. На экране появится диалоговое окно **«Вход в систему»** (рис. 4.2). Дальнейшие действия по входу в систему совпадают с действиями, описанными в пунктах 4.2.1, 4.2.2 настоящего документа.

4.6.2. Блокировка и разблокировка компьютера в ОС Windows 2008R2/Vista/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>**. На экране появится диалоговое окно выбора персонального идентификатора, с использованием которого был произведен вход в систему:

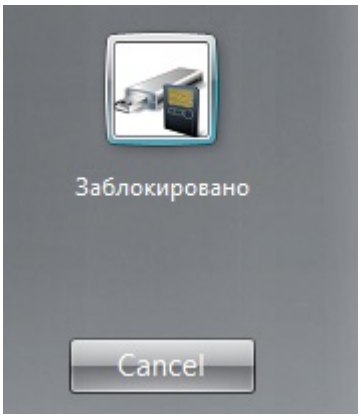


Рисунок 4.36. Выбор носителя для разблокировки в ОС Windows Server 2008R2

Для продолжения разблокировки компьютера необходимо нажать на иконку персонального идентификатора. В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 4.37). 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.

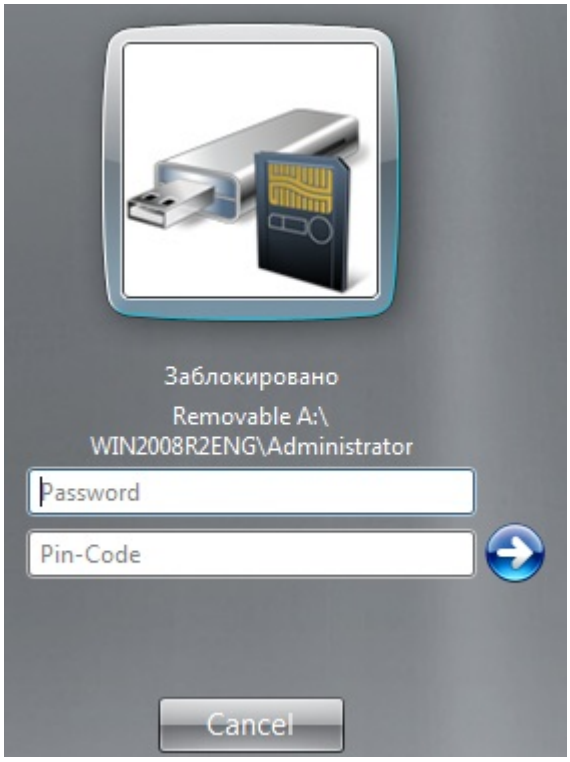


Рисунок 4.37. Ввод данных пользователя для разблокировки ОС Windows Server 2008R2

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоговых окнах разблокировки системы (см. рис. 4.36, 4.37) будет произведен возврат состояния компьютера в режим блокировки.

4.6.3. Блокировка и разблокировка компьютера в ОС Windows 8/8.1/2012/2012R2

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.

Для разблокирования компьютера пользователю необходимо нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**. На экране появится диалоговое окно выбора персонального идентификатора, с использованием которого был произведен вход в систему:

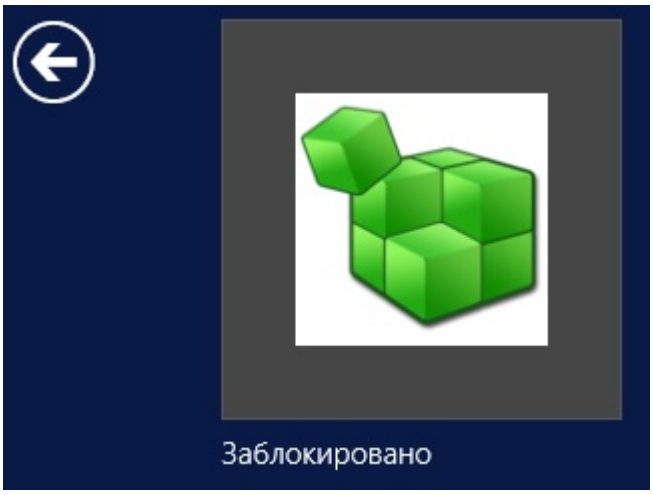


Рисунок 4.38. Выбор носителя для разблокировки в ОС Windows Server 2012/2012R2

Для продолжения разблокировки компьютера необходимо нажать на иконку персонального идентификатора. В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 4.39). 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.

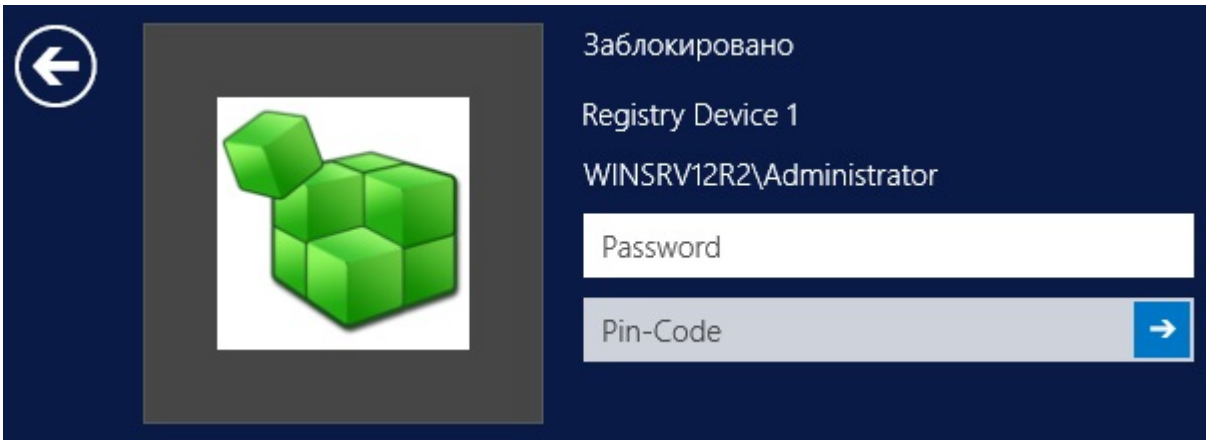


Рисунок 4.39. Ввод данных пользователя для разблокировки ОС Windows Server 2012/2012R2

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоговых окнах разблокировки системы (см. рис. 4.38, 4.39) будет произведен возврат состояния компьютера в режим блокировки.

4.6.4. 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 изъятия 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 4.6.1 – 4.6.3 настоящего руководства.

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

4.6.5. Операции смены пользователя и завершения работы

Операции смены пользователя и завершения работы выполняются стандартными средствами операционной системы Windows. Порядок входа пользователей в систему описан в пунктах 4.1.1, 4.1.2, 4.1.3 настоящего руководства.

4.7. Информация по текущей версии программы

Для получения в Windows XP/2003 справки о текущей версии СЗИ «Блокхост-сеть 2.0» необходимо:

1) открыть апплет **Панели управления** ***Установка и удаление программ*** (***Пуск →Панель управления →Установка удаление программ***);
2) в открывшемся окне в списке установленных программ выделить пункт ***Блокхост-сеть 2.0***;
3) нажать ссылку ***Чтобы получить сведения о поддержке, щелкните здесь***;
4) в результате появится окно с информацией о текущей версии продукта. Пример показан на рисунке 4.40.

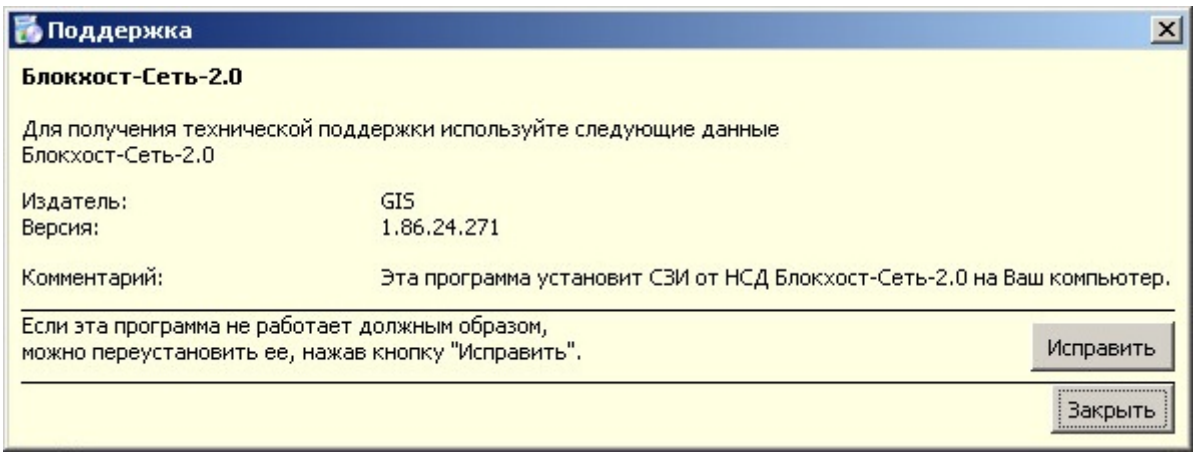


Рисунок 4.40. Информация о версии продукта в Windows Server 2003

Для получения в Windows Vista/2008R2/7/8/8.1/2012/2012R2 справки о текущей версии СЗИ «Блокхост-сеть 2.0» необходимо:

1) открыть апплет **Панели управления *Программы и компоненты***;
2) в открывшемся окне в списке установленных программ выделить пункт ***Блокхост-сеть 2.0***;
3) в результате в нижней части окна отобразится информация о текущей версии продукта. Пример показан на рисунке 4.41.

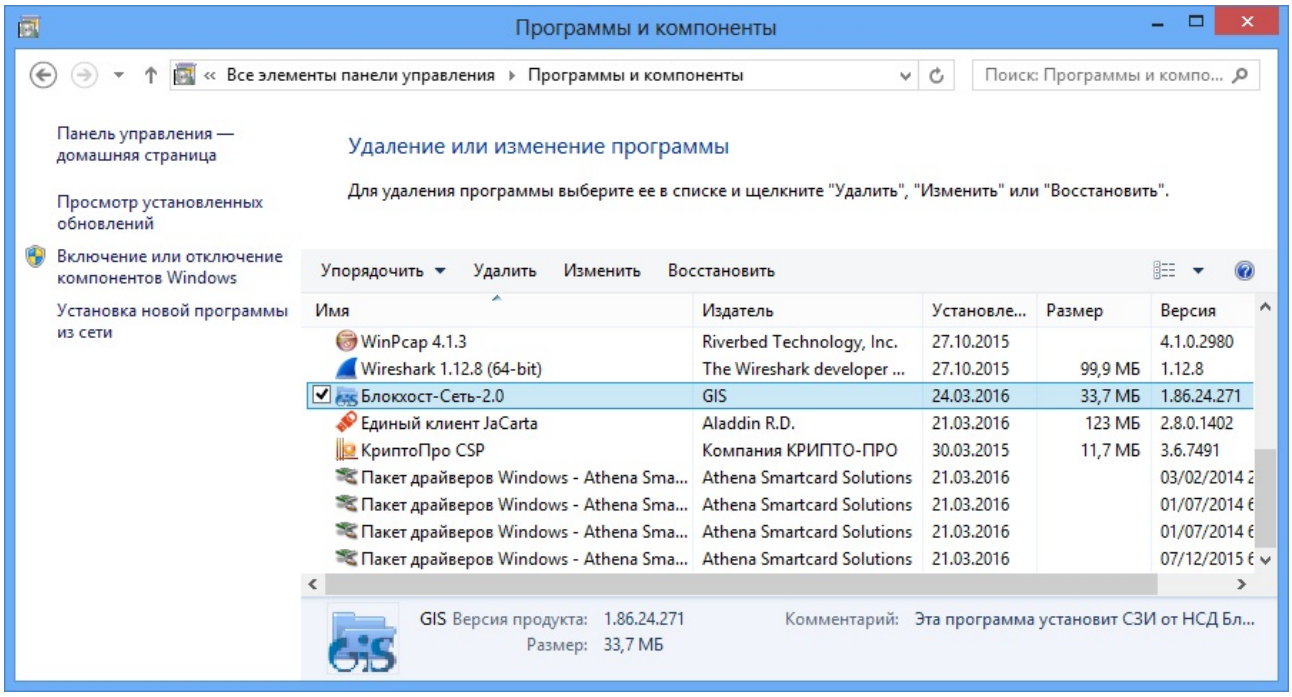


Рисунок 4.41. Информация о версии продукта в Windows Server 2012/2012R2

5. Пользователи в СЗИ «Блокхост-сеть 2.0»

Для формирования политик безопасности администратору безопасности необходимо определить список субъектов доступа (пользователей), к которым будут применяться настройки механизмов разграничения доступа и защиты информации.

5.1. Параметры учетной записи пользователя

Каждая учетная запись пользователя обладает набором параметров, которые администратор безопасности может менять в консоли администрирования СЗИ «Блокхост-сеть 2.0» в интересах соблюдения политик безопасности. Изменяться могут следующие параметры:

- пароль пользователя;
- имя пользователя;
- значение мандатной метки, поставленной в соответствие данной учетной записи;
- разрешение пользователю локального или сетевого входа на контролируемую рабочую станцию;
- персональный идентификатор и PIN-код доступа к нему.

Также администратор безопасности может локально или удаленно заблокировать:

- учетную запись пользователя в СЗИ;
- персональный идентификатор пользователя.

5.2. Добавление пользователей в СЗИ «Блокхост-сеть 2.0»

5.2.1 Общий порядок добавления пользователей в СЗИ «Блокхост-сеть 2.0».

Для добавления пользователя в СЗИ «Блокхост-сеть 2.0» на контролируемую рабочую станцию администратору безопасности необходимо осуществить следующие действия:

1. В серверной консоли администрирования в окне **«Список машин»** выбрать рабочую станцию, на которую необходимо добавить пользователя, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции.
2. В окне **«Настройки машины»** выбрать пункт ***Список пользователей*** (рис. 5.1).
3. В меню ***Управление пользователями*** выбрать пункт ***Добавление пользователей***. Откроется окно **«Добавление пользователей»** (рис. 5.2).

   Окно **«Добавление пользователей»** состоит из:

   - поля выбора источника учетной записи;
   - поля выбора учетной записи пользователей;
   - поля добавляемых пользователей;
   - поля свойств добавляемых пользователей.

   Из окна добавления пользователей можно добавить в СЗИ существующего локального пользователя удаленной рабочей станции, создать нового локального пользователя на контролируемой рабочей станции или добавить учетную запись пользователя домена.

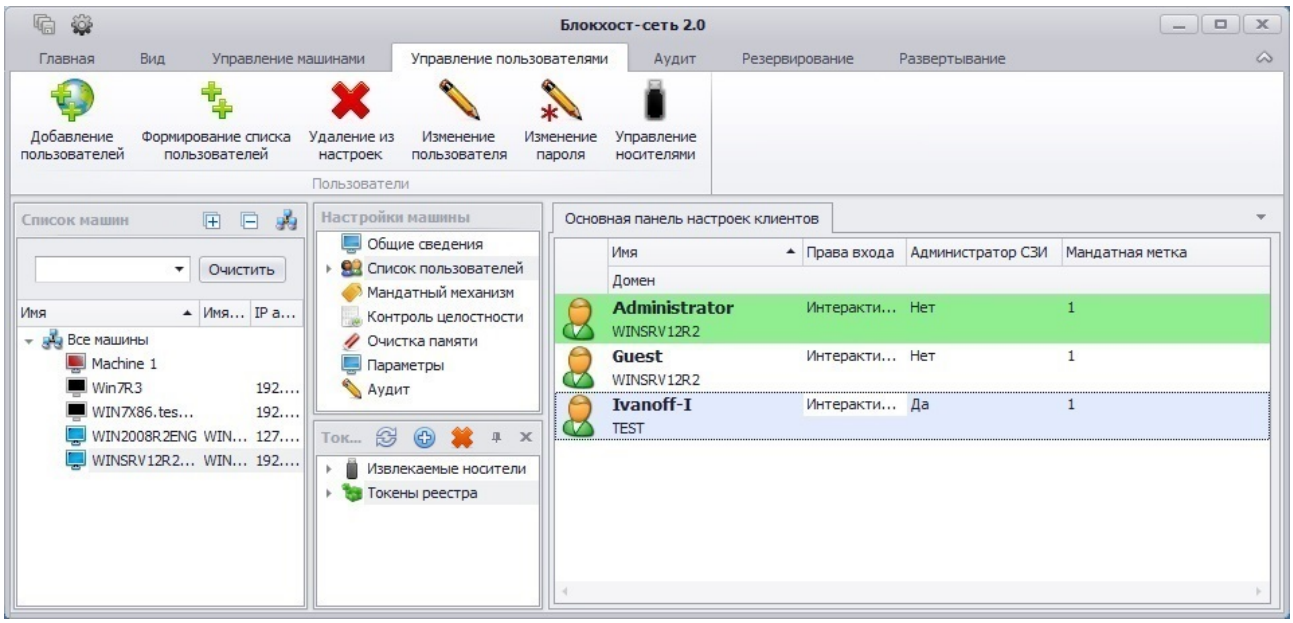


Рисунок 5.1. Консоль администрирования СЗИ «Блокхост-сеть 2.0»

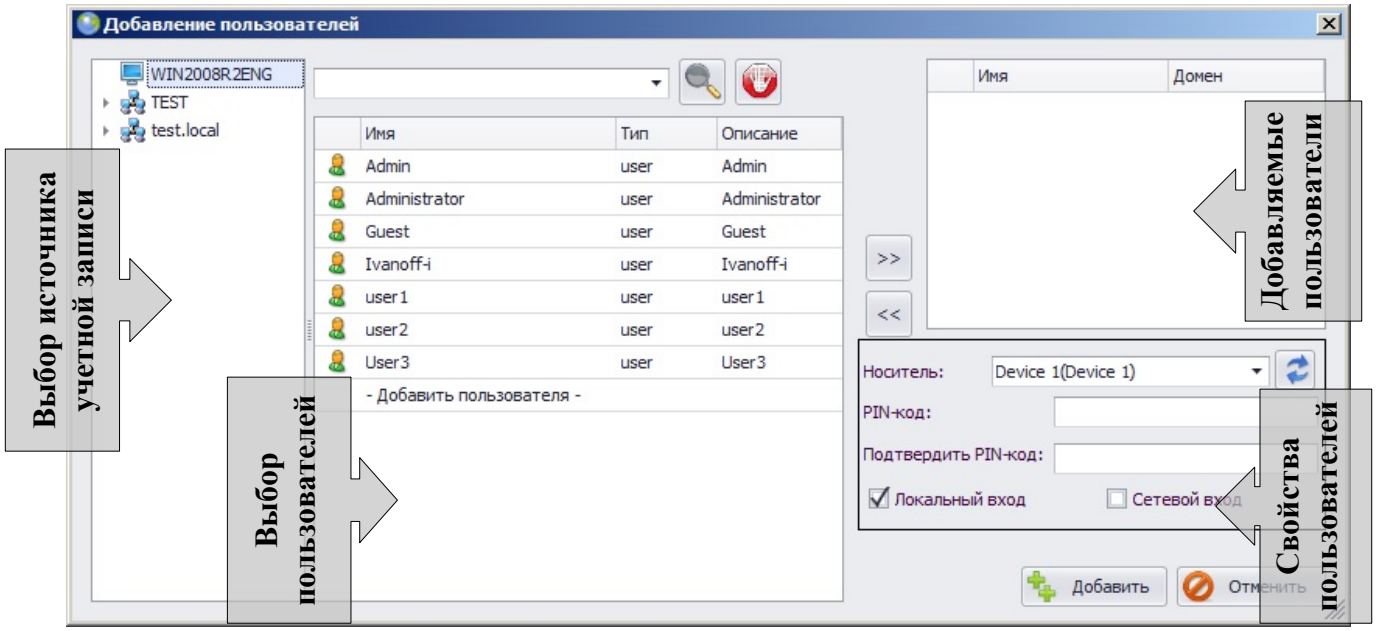


Рисунок 5.2. Окно добавления пользователей

4. В окне **«Добавление пользователей»** необходимо:
   - выбрать источник учетной записи: рабочая станция или домен;
   - выделить необходимую учетную запись пользователя (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить сразу несколько учетных записей);
   - с помощью кнопки >> перенести выбранную учетную запись пользователя в поле добавляемых пользователей;
   - указать тип входа. **Локальный вход** – позволяет пользователю выполнять интерактивный вход в систему. **Сетевой вход –** предоставляет пользователю доступ к открытым (имеющим общий доступ) ресурсам контролируемой рабочей станции с удаленной рабочей станции сети. Особенности добавления сетевых пользователей описаны в пункте 5.2.4 настоящего руководства.

- выбрать из выпадающего списка поля ***Носитель*** электронный идентификатор пользователя (предварительно подключив его к серверу безопасности или к редактируемой рабочей станции), ввести и подтвердить PIN-код доступа к нему в соответствующие поля;

1. В окне **«Добавление пользователей»** отображаются персональные идентификаторы, как подключенные к серверу СЗИ (имеют постфикс Сервер), так и подключенные к редактируемой рабочей станции. Кроме этого существует возможность назначить пользователю идентификатор в реестре Windows, для этого необходимо выбрать пункт ***-Добавить токен в реестр-*** раскрывающегося списка поля ***Носитель***. Персональный идентификатор в реестре Windows создается в реестре редактируемой рабочей станции.

2. В случае если персональный идентификатор был подключен к редактируемой рабочей станции в момент формирования списка пользователей СЗИ, то для его отображения в списке доступных идентификаторов необходимо нажать кнопку ***Обновить***  , расположенную справа от поля ***Носитель***.

- нажать кнопку ***Добавить***.

При применении электронных идентификаторов SafeNet eToken 7200 и SafeNet eToken 7300 существует ряд важных особенностей, их описание приведено в пункте 5.2.1.1 настоящего документа.

Добавляемый в СЗИ «Блокхост-сеть 2.0» *доменный* пользователь должен уже существовать в домене.

5. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

По умолчанию удаленный доступ к открытым ресурсам рабочей станции закрыт, независимо от настроек доступа в ОС Windows.

При добавлении пользователя в СЗИ и при смене его пароля администратором через консоль администрирования СЗИ запрещено использовать символ звездочки «*» в пароле. При изменении пароля пользователем использование символа звездочки «*» не запрещается.

Стоит отметить, что если создаваемому пользователю в дальнейшем будет присвоено значение мандатной метки больше **1, первый вход в ОС** он должен будет выполнить **с мандатной меткой, равной 1.** Это необходимо для корректного создания профиля пользователя операционной системой.

В СЗИ «Блокхост-сеть 2.0» реализована возможность двухфакторной аутентификации пользователей в домене Microsoft Active Directory с использованием цифровых сертификатов пользователей. В этом случае при добавлении пользователя должен быть предъявлен носитель (eToken/SafeNet eToken/JaCarta/eSmart Token/Avest Token/ruToken) с цифровым сертификатом пользователя. Процедура настройки центра сертификации в ОС Windows 2008R2 и получение цифрового сертификата пользователя описаны в Приложении 1 к настоящему руководству.

5.2.1.1 Особенности применения электронных идентификаторов SafeNet eToken 7200 и SafeNet eToken 7300

SafeNet eToken 7200 и SafeNet eToken 7300 – комбинированные USB-ключи, сочетающие возможности средства аутентификации (eToken) и переносного защищенного накопителя данных (флешки).

С помощью специальной утилиты eToken NG-FLASH Partition Application дополнительная Flash-память устройства SafeNet eToken 7200 размечена на две области – доступную только для чтения ROM-область и перезаписываемую область. В ROM-область предустановлено необходимое пользователю ПО и определен конфигурационный файл для его автозапуска. При подсоединении электронного ключа к компьютеру дополнительная Flash-память токена будет распознана как два логических диска, с одного из которых, представляющего ROM-область, будет произведен автоматический запуск приложений.

Flash-память устройства SafeNet eToken 7300 также размечена на две области – доступную только для чтения, ROM-область и перезаписываемую область. В ROM-область предустановлено необходимое ПО и определен конфигурационный файл для его автозапуска. При подсоединении электронного ключа SafeNet eToken 7300 к компьютеру, дополнительная Flash-память токена будет распознана, как два логических диска, с одного из которых, представляющего ROM-область, будет произведен автоматический запуск приложений.

Администрирование eToken-части осуществляется средствами SafeNet Authentication Client, администрирование флеш-части осуществляется предустановленным в ROM-области ПО.

Ограничения по применению SafeNet eToken 7200:

- для использования eToken-части необходимо наличие интерфейса USB 3.0;
- не следует выполнять блокировку флеш-части при помощи предустановленного ПО, т.к. в этом случае при использовании флеш-части для установки СЗИ и для входа пользователя в систему она автоматически блокируется после перезагрузки ОС. Для ее разблокировки необходимо войти в систему, запустить предустановленное на носителе ПО и ввести заданный ранее PIN-код. Далее следует выполнить LogOff\LogOn, после чего FLASH-часть будет разблокирована.

Ограничения по применению SafeNet eToken 7300:

- может не отображаться на виртуальных АРМ, построенных на структуре ESXi;
- не следует использовать флеш-часть данного носителя для установки СЗИ и для входа пользователя в систему, так как флеш-часть после перезагрузки ОС автоматически блокируется. Для ее разблокировки необходимо войти в систему, запустить предустановленный в ROM-области Launcher и ввести PIN-код (PIN-код FLASH-части соответствует PIN-коду, заданному для SafeNet eToken 7300). Далее следует выполнить LogOff\LogOn, после чего флэш-часть будет разблокирована. При использовании LogOff\LogOn флэш-часть работает штатно без блокировки.

5.2.2 Особенности добавления доменных пользователей

При добавлении в СЗИ «Блокхост-сеть 2.0» пользователя из домена необходимо:

1. В окне **«Добавление пользователя»** (см. рис. 5.2) выбрать домен в качестве источника учетной записи;
2. В появившемся окне доменной идентификации ввести учетные данные пользователя домена (в частности – администратора домена) и нажать кнопку ***Подключить***:

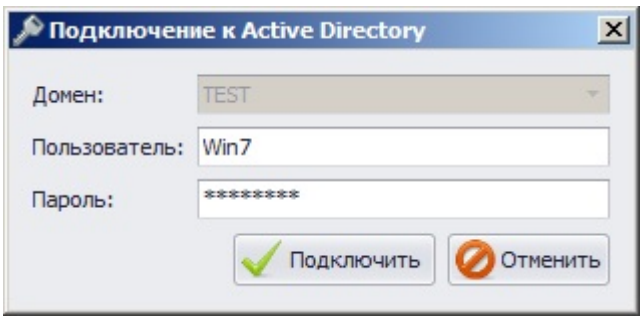


Рисунок 5.3. Окно доменной идентификации пользователя

При вводе корректных учетных данных пользователя домена произойдет подключение к Active Directory. При этом в полях выбора пользователей и выбора источника учетной записи окна **«Добавление пользователя»** отобразится структура Active Directory.

3. Выбрать объект AD, содержащий нужную учетную запись, и содержимое этого контейнера отобразится в поле выбора пользователей (в примере на рис. 5.4 показано содержимое контейнера ***Users***);

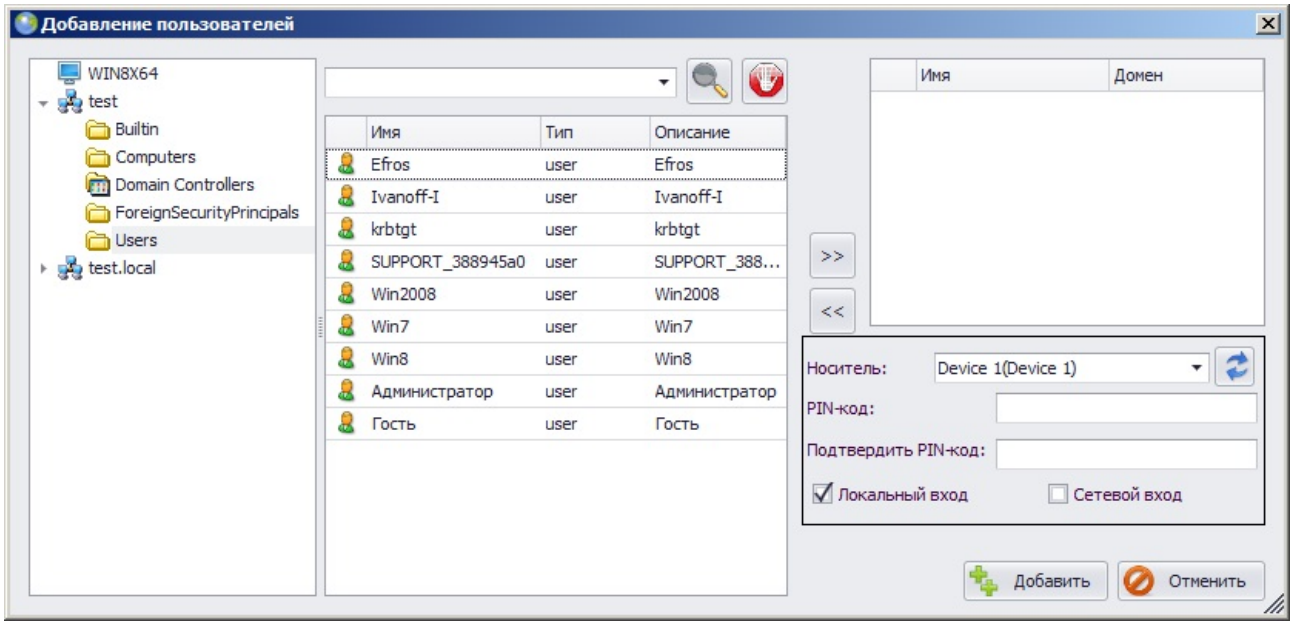


Рисунок 5.4. Добавление доменного пользователя»

4. Выделить учетную запись добавляемого пользователя и с помощью кнопки >> перенести выбранную учетную запись в поле добавляемых пользователей;
5. Указать тип входа: ***Локальный*** или ***Сетевой***;
   - в случае выбора параметра ***Локальный вход*** (или ***Локальный вход*** и ***Сетевой вход***) выбрать из выпадающего списка поля ***Носитель*** электронный идентификатор, ввести и подтвердить PIN-код доступа к нему в соответствующие поля;
   - в случае выбора только параметра ***Сетевой вход*** поля выбора электронного идентификатора и ввода/подтверждения PIN-кода доступа к нему будут недоступны для редактирования.

1. В окне **«Добавление пользователей»** отображаются персональные идентификаторы, как подключенные к серверу СЗИ (имеют постфикс Сервер), так и подключенные к редактируемой рабочей станции. Кроме этого существует возможность назначить пользователю идентификатор в реестре Windows, для этого необходимо выбрать пункт ***-Добавить токен в реестр-*** раскрывающегося списка поля ***Носитель***. Персональный идентификатор в реестре Windows создается в реестре редактируемой рабочей станции.

2. В случае если персональный идентификатор был подключен к редактируемой рабочей станции в момент формирования списка пользователей СЗИ, то для его отображения в списке доступных идентификаторов необходимо нажать кнопку ***Обновить***  , расположенную справа от поля ***Носитель***.

6. Нажать кнопку ***Добавить***. Окно **«Добавление пользователей»** закроется, а добавленный пользователь появится в списке пользователей. Добавленному пользователю автоматически назначается мандатная метка равная **1**, которую в дальнейшем можно изменить (подробнее см. п. 5.3 «Изменение параметров учетной записи пользователей» настоящего руководства);
7. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

5.2.3 Добавление нескольких пользователей

Для добавления нескольких учетных записей пользователей необходимо:

1. В окне **«Добавление пользователей»** (см. рис. 5.4) сформировать (с помощью кнопок  и ) список добавляемых пользователей (для выделения сразу нескольких учетных записей можно воспользоваться клавишами **<Ctrl>** или **<Shift>**);
2. Указать тип входа и параметры электронного идентификатора;
3. Нажать кнопку ***Добавить***.

   В результате все выбранные пользователи отобразятся в списке пользователей контролируемой рабочей станции во вкладке **Основная панель настроек клиентов**. Всем добавленным таким образом пользователям сопоставляется один электронный идентификатор и типы входа, указанные в окне добавления пользователей, и присваивается мандатная метка равная ***1***. Указанные параметры пользователя в дальнейшем можно изменить (подробнее см. п. 5.3 «Изменение параметров учетной записи пользователей» настоящего руководства);
4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Для возможности доступа сетевых пользователей к ресурсам контролируемой рабочей станции (клиента), а также для запуска служб СЗИ, запускаемых от имени учётной записи пользователя, на рабочей станции (клиенте), необходимо чтобы на нее был выполнен локальный (интерактивный) вход пользователя с предъявлением его персонального идентификатора. С этой целью может быть также использована одна из функций: ***Автовход*** (настройка автовхода приведена в пункте 4.2.3 «Автовход в ОС» настоящего руководства) или ***Автозапуск служб***.

5.2.3.1 Автоматическое формирование списка пользователей

В серверной консоли СЗИ «Блокхост-сеть 2.0» реализована возможность автоматического добавления в список пользователей в СЗИ пользователей рабочей станции на основе информации об их работе в ОС. Для формирования такого списка пользователей необходимо:

1. В окне **«Настройки машины»** серверной консоли администрирования выбрать пункт ***Параметры***;
2. В **Основной панели настроек клиентов** установить указатель напротив поля ***Мягкий режим***:

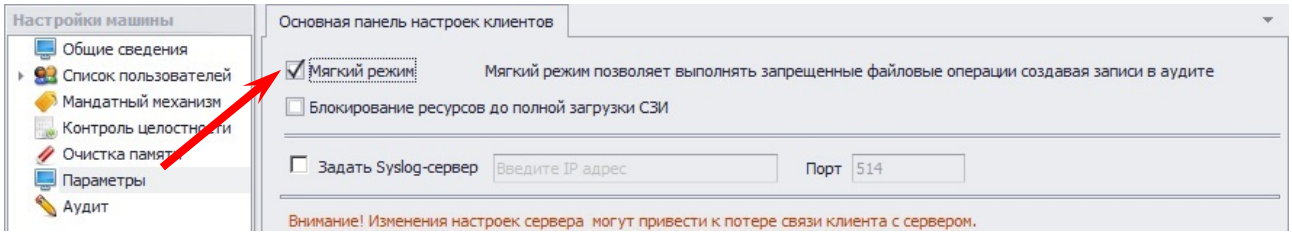


Рисунок 5.5. Включение «Мягкого режима»

3. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ;
4. Затем работающие на контролируемой рабочей станции пользователи осуществляют вход в ее ОС, с использованием любого доступного ключевого носителя.

При работе СЗИ в мягком режиме, при входе пользователя в ОС не осуществляется проверка принадлежности ключевого носителя пользователю, а также проверка PIN-кода доступа к ключевому носителю.

5. Далее АБ в серверной консоли администрирования СЗИ должен снова перейти к процессу добавления пользователей в СЗИ «Блокхост-сеть 2.0» контролируемой рабочей станции:
   - в окне **«Настройки машины»** для выбранной рабочей станции выделить параметр ***Список пользователей***;
   - выбрать пункт меню ***Управление пользователями →Формирование списка пользователей***.
6. В результате, после загрузки сообщений аудита, откроется окно **«Формирование списка пользователей»**, в котором необходимо указать промежуток времени, в течение которого происходила фиксация входа пользователей в ОС контролируемой станции, и нажать кнопку ***ОК***:

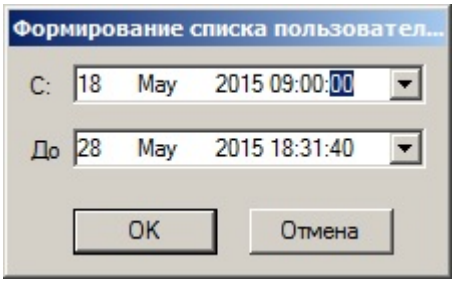


Рисунок 5.6. Окно «Формирование списка пользователей»

7. В **Основной панели настроек клиентов** появятся все пользователи, которые входили на рабочую станцию в указанный период времени. Всем добавленным пользователям СЗИ присваивается мандатная метка равная ***1*** и оба типа входа на рабочую станцию (***Локальный*** и ***Сетевой***):

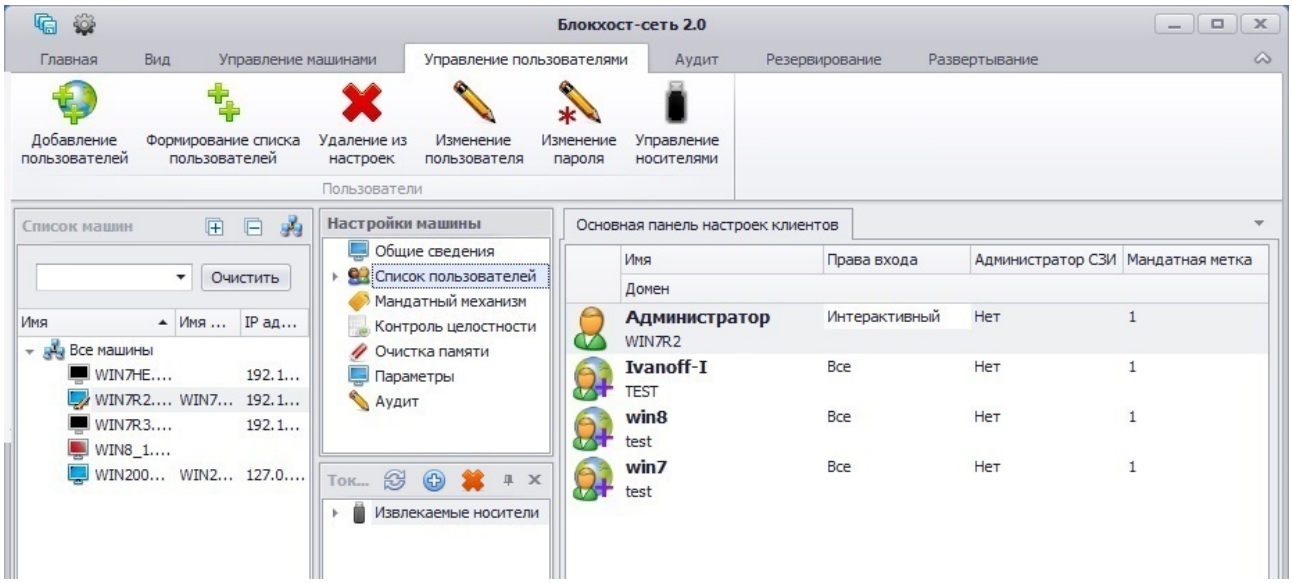


Рисунок 5.7. Список пользователей рабочей станции

8. Затем необходимо отредактировать добавленных пользователей (подробнее о редактировании учетных записей пользователей см. п. 5.3 «Редактирование параметров учетных записей пользователей» настоящего руководства):
   - установить требуемый тип входа;
   - присвоить персональный идентификатор;
   - присвоить мандатную метку.
9. Отключить опцию ***Мягкий режим*** на настраиваемой рабочей станции, выбрав в окне **«Настройки машины»** консоли администрирования пункт ***Параметры*** и сняв указатель с поля ***Мягкий режим*** в **Основной панели настроек клиентов** (см. рис. 5.5);
10. Сохранить настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Необходимо обратить внимание, что для неактивных в мягком режиме компонентов СЗИ при нарушении субъектами заданных правил разграничения доступа защищаемая информация может быть утрачена, а субъекты могут получить доступ к запрещенным ресурсам (подробнее о работе СЗИ в мягком режиме см. п. 6.2.4 «Механизм мягкого режима» настоящего Руководства).

5.2.4 Создание нового локального пользователя

В серверной консоли управления СЗИ «Блокхост-сеть 2.0» существует возможность создания учетной записи локального пользователя на контролируемой рабочей станции. Для создания нового локального пользователя и последующего его добавления в список пользователей в СЗИ редактируемой рабочей станции администратору безопасности необходимо в консоли администрирования:

1. В окне **«Добавление пользователей»** (см. рис. 5.2) выделить редактируемую рабочую станцию в качестве источника списка учетных записей;
2. В поле выбора пользователей дважды щелкнуть левой кнопкой мыши на пункте ***-Добавить пользователя-***;

> Возможность создания нового локального пользователя из консоли администрирования СЗИ появляется только после запуска служб СЗИ «Блокхост-сеть 2.0» на редактируемой рабочей станции.

3. В открывшемся окне **«Создание локального пользователя»** (рис. 5.8):
   - ввести имя пользователя;
   - выбрать группу, в которую он будет включен;
   - задать пароль пользователя и подтвердить его. Введенный пароль необходимо сообщить пользователю, чтобы он смог войти в систему;
   - установить параметр ***Требовать смену пароля при следующем входе в систему*** для принудительной смены введенного администратором пароля нового пользователя;
   - нажать кнопку ***Создать***.

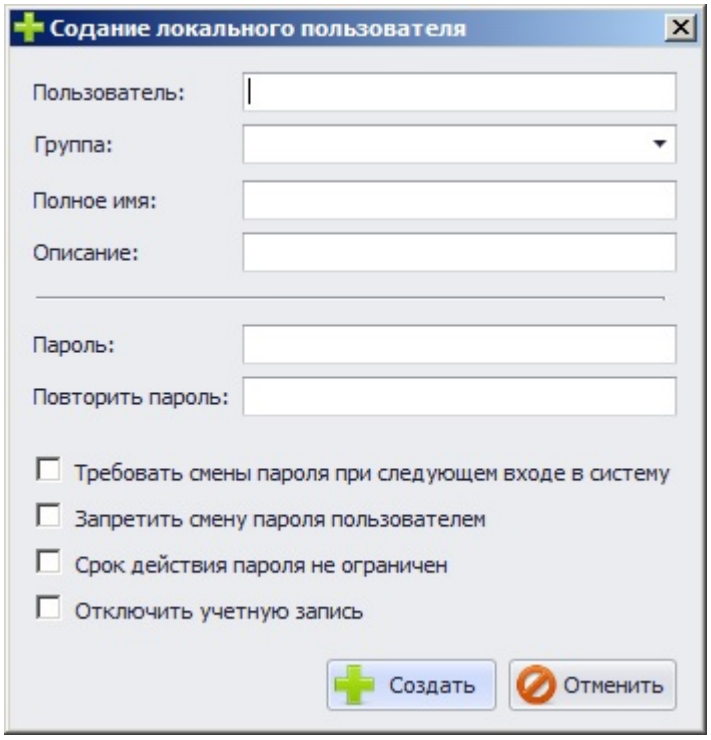


Рисунок 5.8. Окно «Создание локального пользователя»

Окно **«Создание локального пользователя»** консоли администрирования СЗИ повторяет окно **«Новый пользователь»** консоли **mmc** операционной системы Windows. Действия администратора по созданию нового пользователя в серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» повторяют аналогичные действия администратора ОС Windows.

4. В окне добавления пользователей с помощью кнопки >> перенести созданную учетную запись пользователя в поле добавляемых пользователей;
5. Выбрать из выпадающего списка электронный идентификатор пользователя, ввести и подтвердить его PIN-код в соответствующие поля, указать тип входа;
6. Нажать кнопку ***Добавить***. Созданная учетная запись локального пользователя появится в списке пользователей СЗИ рабочей станции. Добавленному в СЗИ пользователю автоматически назначается мандатная метка равная ***1***, которую в дальнейшем можно изменить (подробнее см. п. 5.3 «Изменение параметров учетной записи пользователей» настоящего руководства);

В случае ошибки добавления пользователя соответствующее сообщение отобразится в окне **«Лог»** консоли администрирования СЗИ.

7. Сохранить произведенные изменения выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***, расположенной в левом верхнем углу консоли администрирования СЗИ.

5.2.5 Поддержка работы неавторизованных в СЗИ пользователей

В СЗИ «Блокхост-сеть 2.0» реализована возможность работы неавторизованных в СЗИ пользователей или служб, запущенных от имени неавторизованных в СЗИ пользователей, с ресурсами контролируемой рабочей станции. Механизм работы неавторизованных в СЗИ пользователей заключается в следующем:

- При первоначальной установке СЗИ в список пользователей добавляется локальная учетная запись **Гость** (**Guest**).
- По умолчанию пользователю **Гость** (**Guest**) установлены полные права на доступ к локальным дискам контролируемой рабочей станции, а также возможность сетевого входа на рабочую станцию.
- Настройки механизмов СЗИ, установленные для пользователя **Гость** (**Guest**), присваиваются всем пользователям, которые явно не внесены в базу СЗИ, но осуществляют попытки доступа к информации (от своего имени или от имени служб) на уровне:
  - файловой системы,
  - сетевого входа,
  - запуска приложений от имени пользователя.

В дальнейшем для этой учетной записи возможны все операции по настройке механизмов СЗИ (см. подраздел 6.1 «Настройка индивидуальных механизмов разграничения доступа» настоящего руководства). Также в дальнейшем при необходимости можно удалить учетную запись **Гость** (**Guest**) из списка пользователей (см. подраздел 5.4 «Удаление пользователя из СЗИ «Блокхост-сеть 2.0» настоящего руководства).

5.3. Редактирование параметров учетных записей пользователей

5.3.1. Изменение общих параметров учетных записей пользователей

Учетные записи пользователей можно редактировать в консоли администрирования СЗИ «Блокхост-сеть 2.0». В серверной консоли администрирования СЗИ могут быть изменены следующие параметры учетной записи пользователя:

- имя пользователя;
- мандатная метка;
- тип входа на рабочую станцию;
- пароль.

Изменение мандатной метки и типа входа пользователя на рабочую станцию

Для изменения мандатной метки и типа входа пользователя на контролируемую рабочую станцию администратору безопасности следует:

1. В серверной консоли администрирования в окне «**Список машин**» выбрать рабочую станцию, свойства пользователя которой необходимо изменить, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции (см. рис. 5.1).
2. В окне **«Настройки машины»** выбрать пункт ***Список пользователей***.
3. В **Основной панели настроек клиентов** выбрать учетную запись пользователя и выбрать пункт меню ***Управление пользователями →Изменение пользователя***.
4. Откроется окно **«Изменение пользователя»**, в котором администратор безопасности может изменить имя пользователя, его мандатную метку, тип входа (***Локальный***, ***Сетевой***), а также заблокировать (разблокировать) этого пользователя:

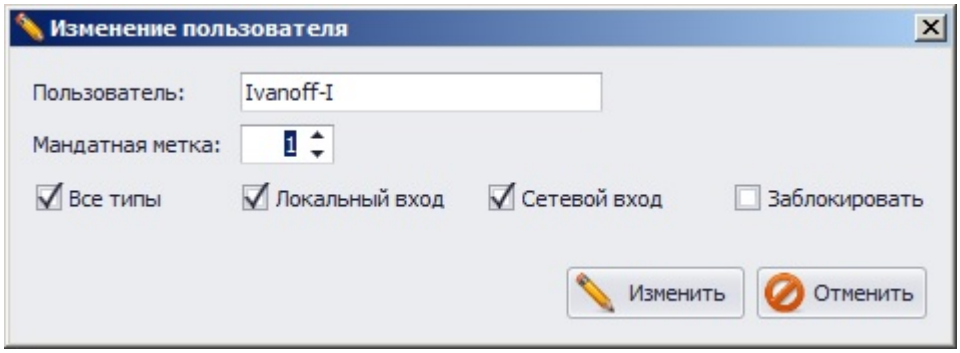


Рисунок 5.9. Окно редактирования параметров пользователя

После ввода новых параметров учетной записи пользователя необходимо нажать кнопку ***Изменить***. Нажатие кнопки ***Отменить*** позволит выйти из окна без изменения параметров учетной записи пользователя.

5. Сохранить произведенные изменения в настройках СЗИ выбрав пункт меню ***Главная→ Сохранить***, или воспользоваться кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Изменить тип входа пользователя на рабочую станцию можно также и с использованием контекстного меню. Для этого необходимо в списке пользователей в **Основной панели настроек клиентов** щелкнуть правой кнопкой мыши на существующем значении типа входа пользователя и в контекстном меню выбрать требуемое значение:

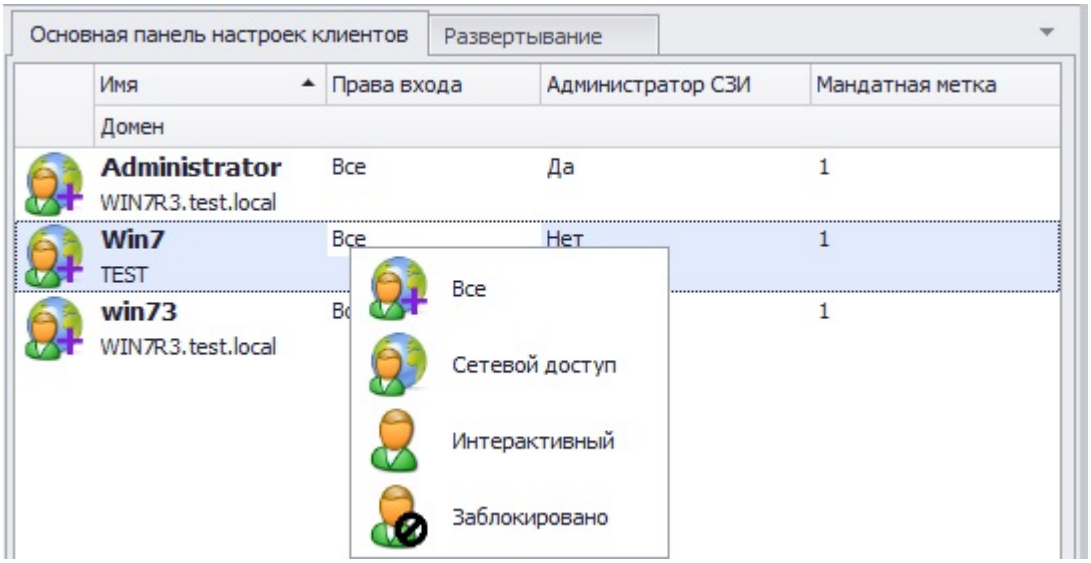


Рисунок 5.10. Контекстное меню выбора типа входа пользователя

Изменить значение мандатной метки также можно в списке пользователей **Основной панели настроек клиентов** (см. рис. 5.10), для этого необходимо установить курсор в поле ***Мандатная метка*** выбранного пользователя и ввести необходимое значение.

Изменение имени пользователя

Изменение имени пользователя из серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» влечет за собой изменение имени этого пользователя в СЗИ «Блокхост-сеть 2.0» и в ОС Windows или в домене, в зависимости от того локальный это пользователь или пользователь домена.

Для изменения имени локальной учетной записи пользователя администратору безопасности следует:

1. В окне **«Изменение пользователя»** (см. рис. 5.9) ввести в поле ***Пользователь*** необходимое имя и нажать кнопку ***Изменить***;
2. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Для изменения имени доменной учетной записи пользователя администратору безопасности следует:

1. В окне **«Изменение пользователя»** (см. рис. 5.9) ввести в поле ***Пользователь*** необходимое имя и нажать кнопку ***Изменить***;
2. В открывшемся окне доменной аутентификации (см. рис. 5.3) ввести логин и пароль учетной записи пользователя, входящего в группу администраторов домена. При успешной авторизации в домене, произойдет изменение имени учетной записи пользователя и в домене, и в СЗИ. В этом случае дополнительных диалоговых окон, подтверждающих факт смены имени пользователя домена, не будет.
3. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

В случае если в окно доменной аутентификации (см. рис. 5.3) введены данные учетной записи, не входящей в группу администраторов домена, имя пользователя на контроллере домена изменено не будет, и появится сообщение об ошибке смены имени:

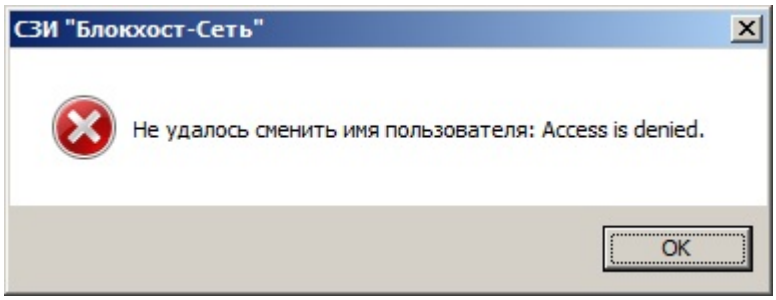


Рисунок 5.11. Контекстное меню выбора типа входа пользователя

После нажатия на кнопку ОК откроется диалоговое окно с предложением сменить имя только в СЗИ «Блокхост-сеть 2.0»:

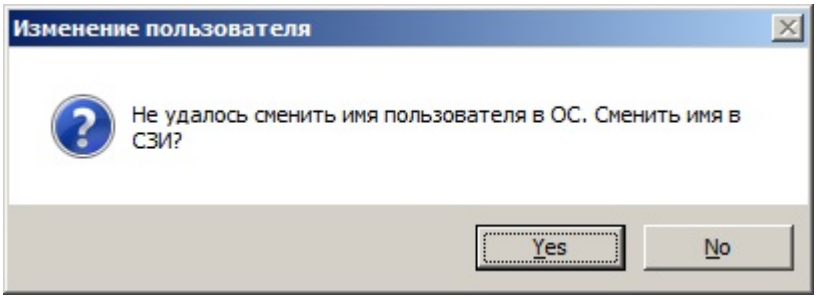


Рисунок 5.12. Контекстное меню выбора типа входа пользователя

Если нажать кнопку ***Да/Yes*** имя пользователя будет изменено только в СЗИ и останется без изменений на контроллере домена. При нажатии кнопки ***Нет/No*** – имя пользователя останется без изменений и в СЗИ и на контроллере домена.

Для того чтобы все-таки изменить имя доменной учетной записи пользователя из консоли администрирования СЗИ администратору безопасности следует заново запустить процесс изменения параметров пользователя и после внесения необходимых изменений (см. рис. 5.9) ввести в окно доменной аутентификации (см. рис. 5.3) корректные данные администратора домена.

Изменение пароля пользователя

Изменение пароля пользователя из консоли администрирования СЗИ «Блокхост-сеть 2.0» влечет за собой изменение пароля этого пользователя в ОС Windows или в домене, в зависимости от того локальный это пользователь или пользователь домена.

Для изменения пароля локального пользователя ОС Windows администратору безопасности следует:

1. В консоли администрирования в окне «**Список машин**» выбрать рабочую станцию, пароль пользователя которой необходимо изменить, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции.
2. В окне **«Настройки машины»** выбрать пункт ***Список пользователей*** (рис. 5.1).
3. В **Основной панели настроек клиентов** выбрать учетную запись пользователя и выбрать пункт меню ***Управление пользователями →Изменение пароля***.
4. Откроется окно **«Изменение пароля пользователя»** (рис. 5.13), в котором администратор безопасности должен ввести новый пароль пользователя и его подтверждение в соответствующие поля.

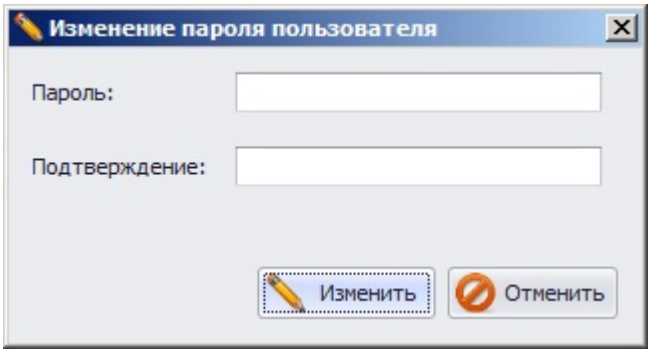


Рисунок 5.13. Окно изменения пароля пользователя

При смене пароля пользователя через консоль администрирования СЗИ запрещено использование символа звездочки «*» в пароле.

5. После ввода нового пароля пользователя необходимо нажать кнопку ***Изменить***. Нажатие кнопки ***Отменить*** позволяет выйти из окна изменения пароля без изменения параметров учетной записи пользователя.
6. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

Для изменения пароля пользователя домена администратору безопасности следует:

1. Повторить действия по смене пароля локального пользователя, приведенные выше в п.п. 1-5.
2. В открывшееся окно доменной аутентификации (см. рис. 5.3) ввести логин и пароль учетной записи пользователя, входящего в группу администраторов домена. При успешной авторизации в домене, произойдет изменение имени учетной записи пользователя и в домене, и в СЗИ. В этом случае дополнительных диалоговых окон, подтверждающих факт смены пароля пользователя домена, не будет.
3. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

В случае если в окно доменной аутентификации (см. рис. 5.3) введены данные учетной записи, не входящей в группу администраторов домена, пароль пользователя изменен не будет, и появится сообщение об ошибке смены пароля (рис. 5.14).

После закрытия окна с сообщением об ошибке изменения пароля пользователя (нажав на кнопку ***ОК*** или кнопку закрытия окна) появится диалоговое окно (рис. 5.15), с предложением изменить пароль этого пользователя в СЗИ «Блокхост-сеть 2.0». Нажатие на кнопку ***Yes*** приведет к смене пароля пользователя в СЗИ, нажатие на кнопку ***No –*** отменит все произведенные изменения.

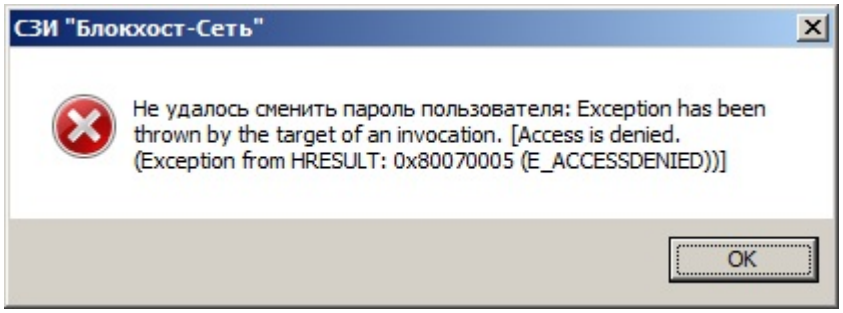


Рисунок 5.14. Сообщение об ошибке изменения пароля пользователя домена

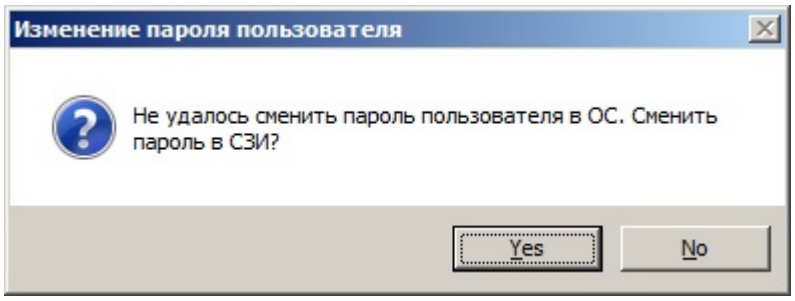


Рисунок 5.15. Окно подтверждения изменения пароля пользователя в СЗИ

Рекомендуется отказываться от сохранения пароля пользователя в СЗИ при ошибке изменения пароля в домене. В случае сохранения пароля только в СЗИ – пароли пользователя на контроллере домена и в СЗИ будут различаться, и при входе на рабочую станцию пользователю необходимо будет ввести два пароля: доменный (прежний) и СЗИ (новый). При этом пароль пользователя в СЗИ будет снова заменен на доменный.

5.3.2. Управление ключевыми носителями пользователя

В серверной консоли администрирования СЗИ существует возможность управления персональными идентификаторами пользователя:

- присвоение пользователю нового персонального идентификатора;
- блокировка (разблокировка) назначенного пользователю персонального идентификатора;
- удаление персонального идентификатора пользователя.

Добавление пользователю нового персонального идентификатора

Для добавления пользователю дополнительного персонального идентификатора в СЗИ «Блокхост-сеть 2.0» администратору безопасности необходимо:

1. Подключить присваиваемый пользователю дополнительный персональный идентификатор к серверу безопасности;
2. В серверной консоли администрирования в окне «**Список машин**» выбрать рабочую станцию, свойства пользователя которой необходимо изменить, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции;
3. В окне **«Настройки машины»** выбрать пункт ***Список пользователей*** (рис. 5.1);
4. В **Основной панели настроек клиентов** выделить учетную запись пользователя, которому будет присвоен дополнительный идентификатор, и выбрать пункт меню ***Управление пользователями →Управление носителями***;
5. Откроется окно **«Управление носителями»** (рис. 5.16), в котором администратор безопасности может присвоить пользователю новый персональный идентификатор, заблокировать или удалить уже используемый этим пользователем ключевой носитель;

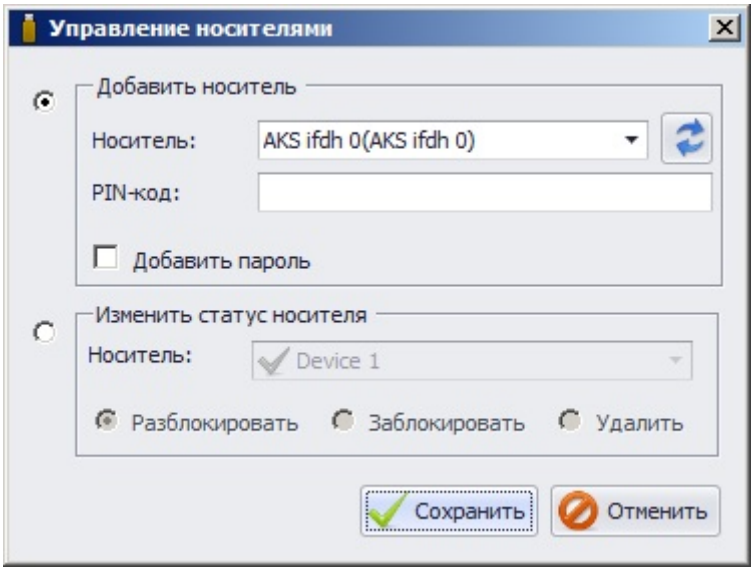


Рисунок 5.16. Окно управления ключевыми носителями пользователя

6. В окне **«Управление носителями»**:
   - отметить маркер в области *Добавить носитель*;
   - из выпадающего списка поля ***Носитель*** выбрать новый персональный идентификатор, присваиваемый пользователю, и ввести PIN-код доступа к нему в соответствующее поле;

В случае если персональный идентификатор был подключен к редактируемой рабочей станции в момент назначения пользователю нового носителя, то для его отображения в списке доступных идентификаторов необходимо нажать кнопку ***Обновить***  , расположенную справа от поля ***Носитель***.

   - при необходимости записи на добавляемый носитель пароля пользователя отметить параметр ***Добавить пароль***;
   - нажать кнопку ***Сохранить***:
     - ✓ если параметр ***Добавить пароль*** не отмечен, появится окно с сообщением об успешном добавлении идентификатора:

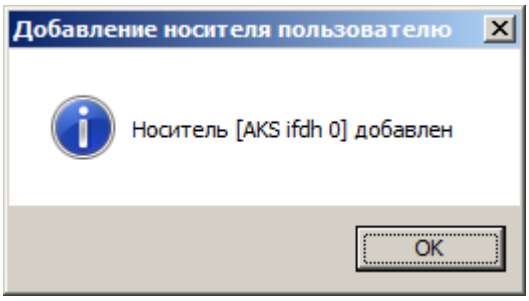


Рисунок 5.17. Сообщение об успешном добавлении носителя

     - ✓ если был отмечен параметр ***Добавить пароль*** – откроется окно ввода пароля пользователя, в котором необходимо указать пароль редактируемой учетной записи пользователя и нажать кнопку ***Ввести***:

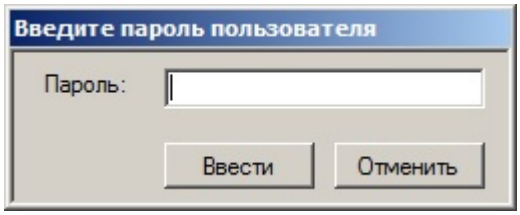


Рисунок 5.18. Окно ввода пароля редактируемого пользователя

- ✓ при сохранении на носителе пароля пользователя домена появится дополнительное окно доменной аутентификации (см. рис. 5.3), в котором необходимо ввести логин и пароль любого пользователя домена. Если в диалоговые окна введены корректные данные, то появится сообщение об успешном добавлении идентификатора (см. рис. 5.17).

  Если в окно ввода пароля пользователя или окно доменной аутентификации были введены некорректные данные (неверный пароль; в окне доменной аутентификации указаны неверные учетные данные пользователя домена), то появится окно с сообщением об ошибке, и в окне **«Лог»** консоли администрирования отобразится запись об ошибке проверки пароля. Для продолжения операции добавления носителя необходимо снова нажать кнопку ***Сохранить*** в окне **«Управление носителями»** и заново ввести необходимые данные в диалоговые окна сохранения пароля пользователя на носителе.

- нажатие кнопки ***Отменить*** позволит выйти из окна управления носителями без изменения параметров учетной записи пользователя;

7. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Изменение статуса персонального идентификатора пользователя

Администратор безопасности из серверной консоли администрирования СЗИ может заблокировать (разблокировать) персональный идентификатор, назначенный пользователю, или удалить ключевой носитель пользователя. Для изменения статуса персонального идентификатора пользователя необходимо:

1. В **Основной панели настроек клиентов** выбрать учетную запись пользователя, статус идентификатора которого будет изменяться, и выбрать пункт меню ***Управление пользователями →Управление носителями***;
2. В окне **«Управление носителями»** (рис. 5.16) отметить маркер области *Изменить статус носителя*;
3. В выпадающем списке поля ***Носитель*** выбрать персональный идентификатор пользователя;
4. В зависимости от требуемого с персональным идентификатором действия отметить соответствующий параметр:
   - ***Заблокировать*** – позволяет запретить использование пользователем выбранного персонального идентификатора для осуществления входа в ОС;
   - ***Разблокировать*** – позволяет разблокировать ранее заблокированный персональный идентификатор;
   - ***Удалить*** – позволяет отвязать выбранный персональный идентификатор от учетной записи пользователя;
5. Нажать кнопку ***Сохранить***. Нажатие кнопки ***Отменить*** позволит выйти из окна управления носителями без изменения параметров учетной записи пользователя;

6. Сохранить изменения параметров учетной записи пользователя выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

5.3.3. Создание резервного носителя администратора безопасности

Для того, чтобы в случае утери своего ключевого носителя администратор безопасности мог войти на локальную рабочую станцию (или на сервер безопасности) и запустить консоль администрирования, можно создать резервный ключевой носитель АБ.

Для этого необходимо:

1) добавить учетную запись администратора безопасности в список пользователей в СЗИ редактируемой рабочей станции, указав при этом ключевой носитель, который будет резервным (подробно процесс добавления пользователя в СЗИ на контролируемой рабочей станции описан в пункте 5.2.1 настоящего руководства);
2) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Если администратор безопасности уже добавлен в список пользователей с указанием другого носителя, то ему можно назначить резервный носитель, используя пункт меню ***Управление пользователями →Управление носителями*** (подробнее см. пункт 5.3.2 настоящего документа).

После назначения администратору безопасности дополнительного персонального идентификатора он, при необходимости, сможет войти на локальную рабочую станцию (или сервер безопасности) с использованием резервного носителя и запустить консоль администрирования СЗИ.

5.4. Удаление пользователя из СЗИ «Блокхост-сеть 2.0»

Для удаления пользователей из СЗИ «Блокхост-сеть 2.0» администратору безопасности следует:

1. В серверной консоли администрирования в окне «**Список машин**» выбрать рабочую станцию, пользователя которой необходимо удалить из СЗИ, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции;
2. В окне **«Настройки машины»** выбрать пункт ***Список пользователей*** (рис. 5.1);
3. В **Основной панели настроек клиентов** выделить учетную запись удаляемого пользователя и выбрать пункт меню ***Управление пользователями →Удаление из настроек*** для его удаления из СЗИ;

При удалении пользователя из списка пользователей в СЗИ «Блокхост-сеть 2.0» не происходит удаления его учетной записи из домена (или рабочей станции).

4. Подтвердить удаление пользователя в появившемся диалоговом окне:

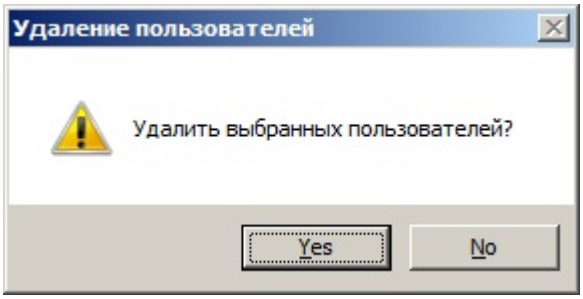


Рисунок 5.19. Диалоговое окно подтверждения удаления пользователя

5. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

6. Формирование политики безопасности

Формирование политики безопасности осуществляется администратором безопасности с помощью механизмов разграничения доступа и защиты информации, реализованных в СЗИ «Блокхост-сеть 2.0». Механизмы разграничения доступа и защиты информации, реализованные в СЗИ «Блокхост-сеть 2.0», делятся на:

- **Индивидуальные** механизмы разграничения доступа и защиты информации. Настройки таких механизмов являются строго индивидуальными для каждого зарегистрированного в СЗИ «Блокхост-сеть 2.0» пользователя.
- **Системные** механизмы защиты информации. Настройки таких механизмов производятся администратором безопасности для локального компьютера, на котором установлена СЗИ «Блокхост-сеть 2.0». Эти механизмы являются общими для всех зарегистрированных в СЗИ «Блокхост-сеть 2.0» пользователей.

Механизмы защиты информации реализованы в соответствии с требованиями РД Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» для третьего класса защищенности.

Для корректного использования дискреционного, мандатного механизма защиты и механизма запуска процессов СЗИ администратору безопасности следует:

- контролировать наличие и возможность создания пользователем жестких ссылок, поддерживаемых файловой системой NTFS. При отсутствии такой возможности необходимо использовать файловую систему FAT32;
- на ЭВМ пользователя обеспечить отсутствие специализированного программного обеспечения, предназначенного для создания дополнительных жестких или символьных ссылок, а также иных точек монтирования для повторной обработки.

6.1 Настройка индивидуальных механизмов разграничения доступа

Индивидуальные механизмы защиты информации настраиваются строго индивидуально для каждого зарегистрированного в СЗИ «Блокхост-сеть 2.0» пользователя. В состав индивидуальных механизмов входят следующие: дискреционный, разграничение доступа к отчуждаемым физическим носителям информации, разграничение доступа к запуску процессов, разграничение времени входа в систему, разграничение доступа к администрированию СЗИ, разграничение доступа к сетевым ресурсам и фильтрация сетевого трафика, контроль печати.

Произведенные настройки индивидуальных механизмов разграничения доступа вступают в силу после завершения текущего сеанса пользователя или перезагрузки ОС на контролируемой рабочей станции. Следует учесть, что перезагрузка ОС, инициированная с консоли администрирования СЗИ, начнется без каких-либо предупреждений для пользователя и несохраненные данные могут быть потеряны. Чтобы этого избежать, можно дождаться, когда пользователь сам завершит работу ПК (например, в конце рабочего дня) и при последующей загрузке ОС новые настройки вступят в силу.

6.1.1. Дискреционное разграничение доступа к объектам файловой системы

Реализация дискреционного механизма в СЗИ «Блокхост-сеть 2.0» заключается в контроле доступа поименованных субъектов (пользователей) к поименованным объектам (ресурсам файловой системы). Для каждой пары субъект-объект администратором безопасности в СЗИ задается перечисление типов доступа, являющихся санкционированными для данного субъекта к данному объекту (ресурсу файловой системы). Ниже описаны возможные виды доступа к ресурсам.

6.1.1.1 Контролируемые в дискреционном механизме виды доступа

Для обеспечения дискреционного разграничения доступа в СЗИ «Блокхост-сеть 2.0» возможны следующие виды доступа:

- **Чтение**. С помощью данного вида доступа санкционируется возможность чтения субъектом информации из объекта и возможность копирования объекта в любое незапрещенное данным, либо другим механизмом защиты информации место файловой системы.
- **Запись.** С помощью этого вида доступа администратор безопасности может санкционировать такие действия контролируемых субъектов, которые приводят к изменениям информации в объекте, удалению, переименованию и перемещению объекта.

Кроме того, для каждого объекта, сопоставленного субъекту, администратор безопасности может задать следующие опции:

- **Гарантированное удаление.** Включение данного механизма позволяет осуществлять гарантированное уничтожение информации с физического носителя при удалении выбранного объекта.

  Возможны следующие варианты:

  1) пользователь удаляет объекты, отмеченные для гарантированного удаления, минуя корзину (сочетание клавиш **<Shift>+<Del>**). В этом случае они сразу гарантированно уничтожаются;
  2) пользователь удаляет объекты (файл или папку на диске), отмеченные для гарантированного удаления, сначала в корзину. В этом случае гарантированное удаление объектов происходит после очистки корзины.

  Если параметр ***Гар.уд.*** отмечен для отдельной папки или файла на диске, то объект файловой системы ***Корзина*** соответствующего логического диска также должен быть добавлен в настройки дискреционного механизма редактируемого пользователя. Для объекта ***Корзина*** должны быть отмечены такие параметры как: ***Чтение***, ***Запись*** и ***Гар.уд***.

  Если параметр ***Гар.уд.*** отмечен для логического диска целиком, то и для объекта файловой системы ***Корзина*** данного логического диска механизм гарантированного удаления будет включен автоматически и дополнительно добавлять его (объект) в настройки дискреционного механизма редактируемого пользователя не нужно.

Если удаляемый файл был создан при помощи приложения, которое создает в процессе работы *временные файлы* (например, MS Word), то при необходимости гарантированного уничтожения информации, содержащейся в этом файле, механизм гарантированного удаления *нужно включать не для самого файла*, а для папки, в которой он находится.

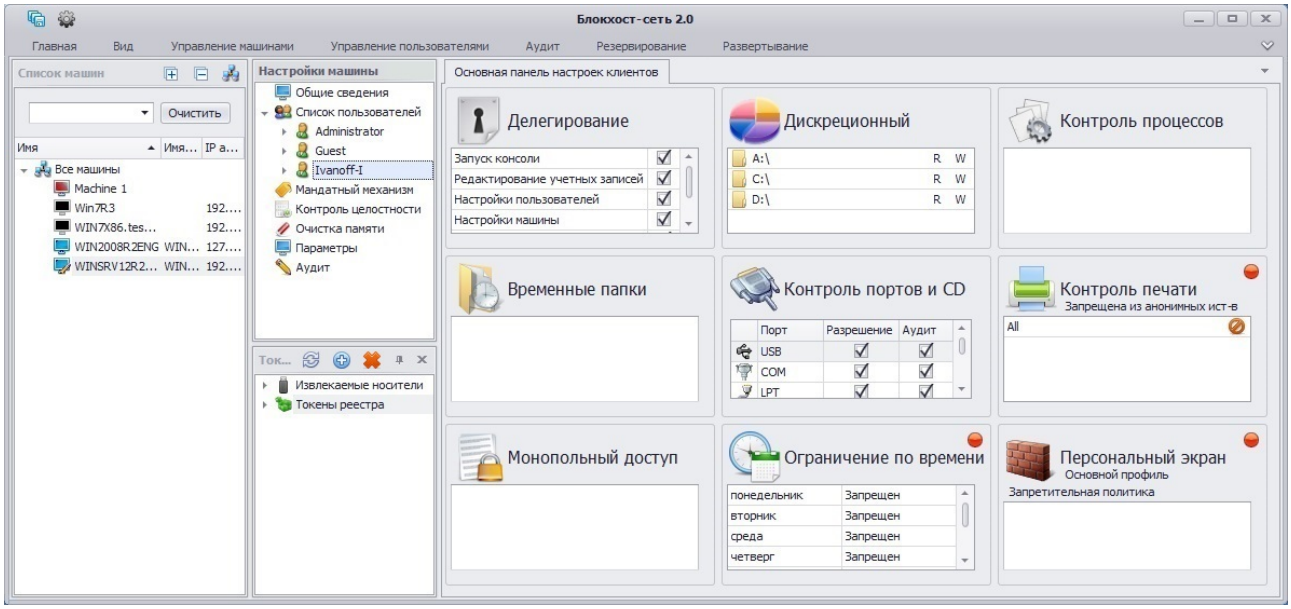
При установке программного обеспечения, использующего в процессе инсталляции временные файлы (например, Антивирус Касперского, MS Office, некоторые драйверы), может потребоваться предварительно отключить механизм гарантированного удаления (поле ***Гар.уд.*** в **Основной панели настроек клиентов** консоли администрирования СЗИ), поскольку механизм гарантированного удаления удаляет временный файл, как только завершился процесс, который обращался к такому файлу.

- **Аудит.** Включение данного механизма для объекта доступа позволяет администратору безопасности санкционировать регистрацию событий, осуществленных соответствующим субъектом и связанных с безопасностью информации, содержащейся в объекте.

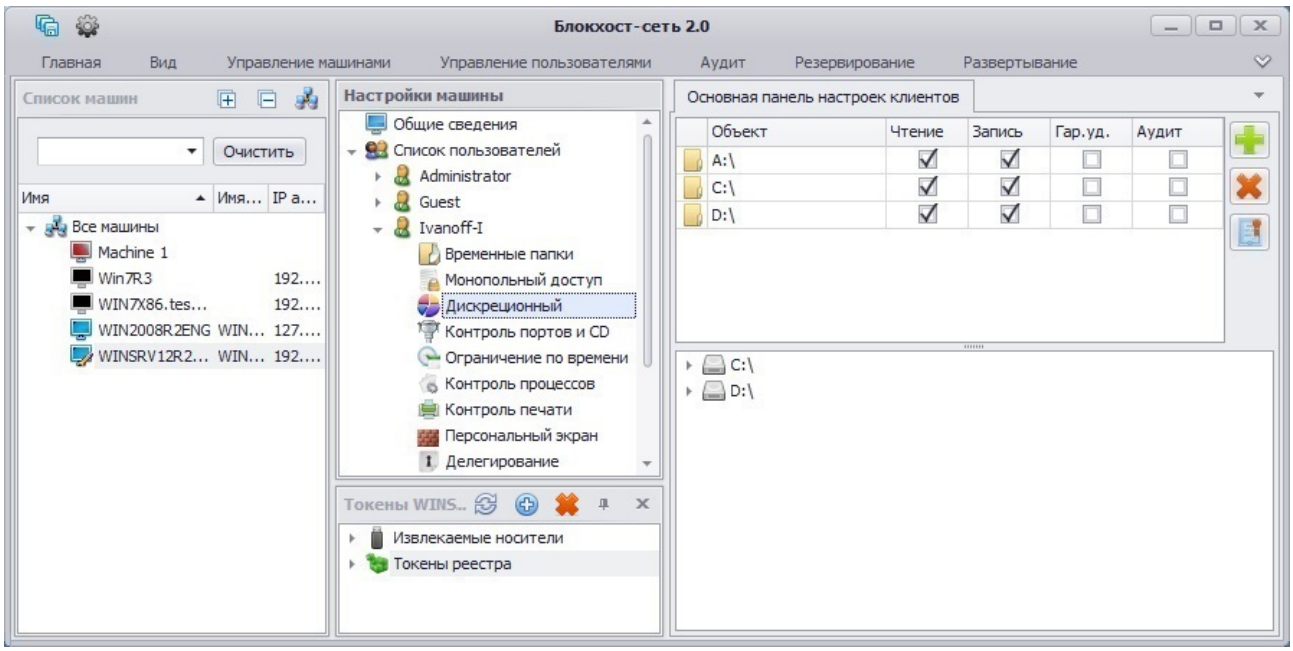
6.1.1.2. Реализация дискреционной модели разграничения доступа

Для того, чтобы реализовать с помощью СЗИ «Блокхост-сеть 2.0» дискреционную модель разграничения доступа, администратору безопасности необходимо выполнить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования выбрать рабочую станцию, для которой будет производиться настройка дискреционного механизма, раскрыв пункт ***Все машины***;
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Дискреционный*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Дискреционный*** (рис. 6.1, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.1, б);



а)



б)

Рисунок 6.1. Настройка дискреционного механизма разграничения доступа

3. В **Основной панели настроек клиентов** добавить ресурсы на контроль, захватив и перетащив мышью необходимые объекты файловой системы из дерева ресурсов в нижней части панели (для добавления ресурса можно также воспользоваться кнопкой ***Добавить***);

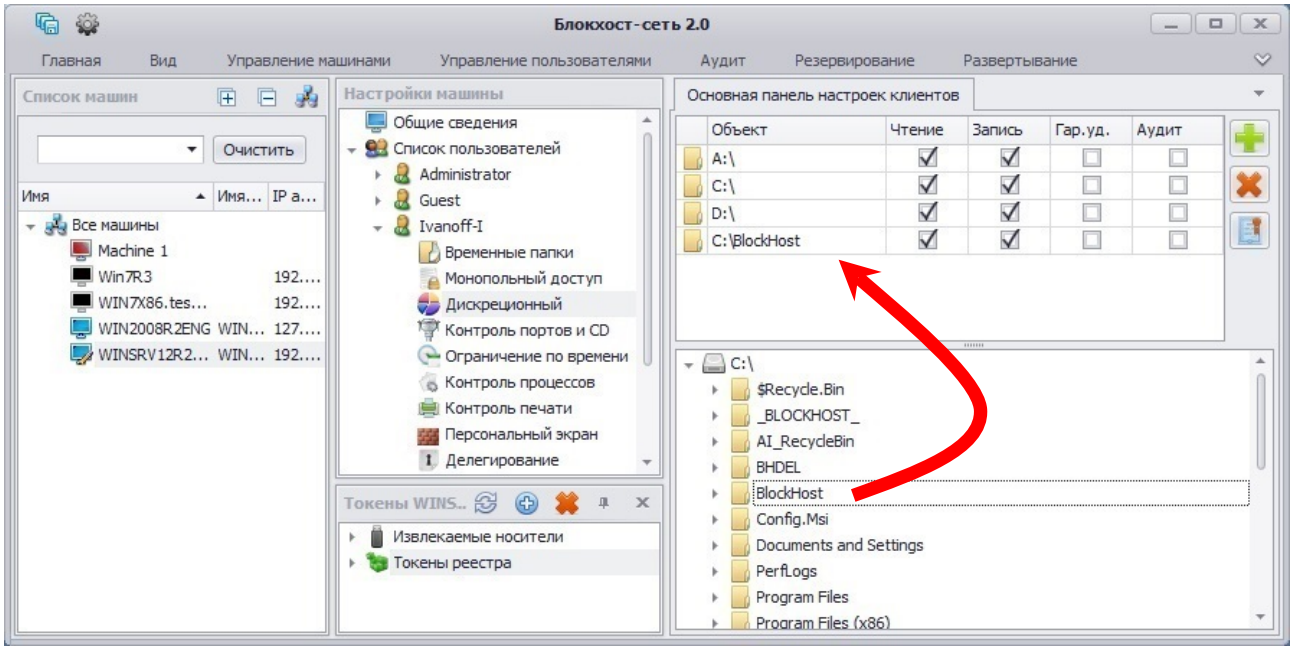


Рисунок 6.2. Добавление контролируемых объектов в настройки дискреционного механизма

4. Для удаления объектов из списка контролируемых достаточно выделить в области настроек требуемый ресурс и нажать клавишу **<Del>**. Также для удаления объекта можно воспользоваться кнопкой ***Удалить*** ;
5. Для разрешения доступа на чтение и/или запись администратор безопасности должен отметить соответствующие параметры (***Чтение***, ***Запись***) в группе полей, расположенных справа от выбранного объекта файловой системы;

6. Для включения механизма гарантированного уничтожения информации при удалении файлового объекта необходимо в области настроек отметить параметр ***Гар.уд.*** для соответствующего объекта файловой системы;
7. При необходимости администратор безопасности может разрешить фиксацию событий, связанных с безопасностью информации, содержащейся в данном объекте, в журнал СЗИ «Блокхост-сеть 2.0». Для этого в области настроек необходимо отметить параметр ***Аудит***, расположенный в группе полей справа от выбранного объекта файловой системы (рис. 6.3);

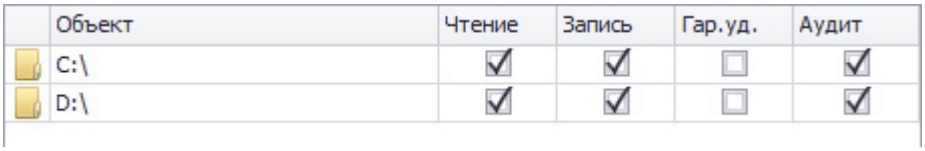


Рисунок 6.3. Включение настройки аудита в дискреционном механизме разграничения доступа

8. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Политика безопасности в СЗИ «Блокхост-сеть 2.0» построена по принципу – что явно не разрешено, то запрещено. В списке контролируемых объектов дискреционного механизма СЗИ, по умолчанию, указаны все логические диски рабочей станции, с правом полного доступа к ним зарегистрированных в СЗИ пользователей.

Разграничение доступа к контролируемым объектам выполняется сочетанием политик доступа к объектам файловой системы операционной системы и СЗИ. При этом необходимо учитывать следующее:

- дискреционный механизм СЗИ «Блокхост-сеть 2.0» дополняет, но не исключает действующей политики разграничения NTFS;
- права доступа СЗИ к объектам распространяются на вложенные в них папки и файлы, при отсутствии отличных прав доступа к ним;
- для исключения вложенного объекта из действующей политики доступа СЗИ, данный объект указывается с иными правами доступа к нему;
- при закрытии доступа к USB-носителям (флэш-дискам) средствами дискреционного механизма СЗИ необходимо устанавливать запрет доступа к ним и в настройках механизма СЗИ ***Контроль портов и CD*** (подробнее о настройке механизма ***Контроль портов и CD*** см. п. 6.1.2 настоящего руководства).

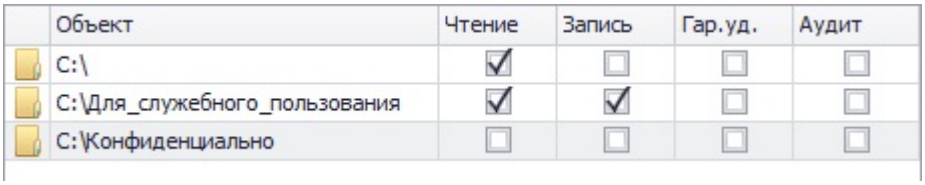


Рисунок 6.4. Пример дискреционной политики разграничения доступа

На рисунке 6.4 показан пример дискреционной политики разграничения доступа пользователя к объектам файловой системы. Из рисунка видно, что пользователь наделен правом чтения диска «C:\», не имея возможности изменять его содержимое. Для работы пользователю выделена папка «C:\Для_служебного_пользования\». Поскольку папка наследует только право чтения от диска «C:\», ее необходимо добавить в список с указанием прав полного доступа к ней, тем самым исключив наследуемое право чтения от диска «C:\». Аналогично выполнен полный запрет доступа к папке «C:\Конфиденциально».

6.1.1.3. Особенности работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа

В файловой системе NTFS существует технология привязки (Link), позволяющая одному и тому же файлу существовать в нескольких каталогах, иногда под разными именами (т.е. два разных имени файла указывают на одну и ту же внутреннюю структуру данных). Подобная привязка называется жесткой связью или жесткой ссылкой (hard link). Жесткие ссылки могут быть созданы только для файлов в переделах одного логического диска.

Другим вариантом привязки файлов является символьная ссылка. В файловой системе NTFS существует два вида символьных ссылок: «junction point» и «symlink». Junction point (точка соединения NTFS) позволяет отображать указанную папку или логический диск, как папку на другом логическом диске, либо в другой папке. Symlink представляет собой небольших размеров файл, содержащий путь к исходному файлу (папке). При запуске файла, являющегося символьной ссылкой, по содержащемуся в нему пути происходит обращение к исходному (оригинальному) файлу (папке).

Junction point могут быть созданы для каталогов на диске и/или логического диска целиком. Symlink могут быть созданы для файлов и каталогов, при этом они могут пересекать границы логических дисков, а также указывать на имена файлов, находящихся на удаленных компьютерах.

Создать junction point возможно средствами ОС Windows XP/2003/Vista/7/2008R2/8/8.1/2012/2012R2. Для создания symlink в ОС Windows XP/2003 дополнительно необходим специальный драйвер symlink.sys.

Для того чтобы установить дискреционное разграничение доступа для объекта, имеющего жесткие и/или символьные ссылки, администратору безопасности необходимо:

1. Проверить наличие жестких и символьных ссылок, относящихся к контролируемым объектам. Методика проверки наличия жестких и символьных ссылок и работы с ними приведены ниже.
2. В настройках дискреционного механизма консоли администрирования СЗИ вместе с контролируемыми объектами добавить на контроль жесткие ссылки, относящиеся к ним, с правами доступа исходных (оригинальных) объектов.
3. Для объектов, имеющих символьные ссылки, необходимо убедиться, что в настройках дискреционного механизма консоли администрирования СЗИ на контроль добавлены исходные (оригинальные) файлы, а не их символьные ссылки. Методика проверки наличия символьных ссылок и работы с ними приведены ниже. Установленные в СЗИ права доступа для оригинального файла будут действовать при попытках доступа к нему по символьной ссылке.

Особенности работы с жесткими ссылками

Для проверки наличия жестких ссылок (hardlink), относящихся к контролируемым объектам, администратору безопасности необходимо:

1) выполнить подготовительные операции – на жестком диске создать папку с именем **HardlinkList** со следующими файлами *HardlinkFull.bat, CutTheTrash.bat, FindLinks.exe.* Содержимое командных файлов *HardlinkFull.bat* и *CutTheTrash.bat* приведено на рисунках 6.5 и 6.6 соответственно. Данные командные файлы можно также скопировать из каталога *GIS\Documents\Linklist\HardlinkList* дистрибутивного диска.

Программа *FindLinks.exe* поставляется на дистрибутивном диске СЗИ (каталог *GIS\Documents\LinkList\HardlinkList*), а также доступна на официальном сайте компании Microsoft (http://technet.microsoft.com/ru-ru/sysinternals/hh290814);

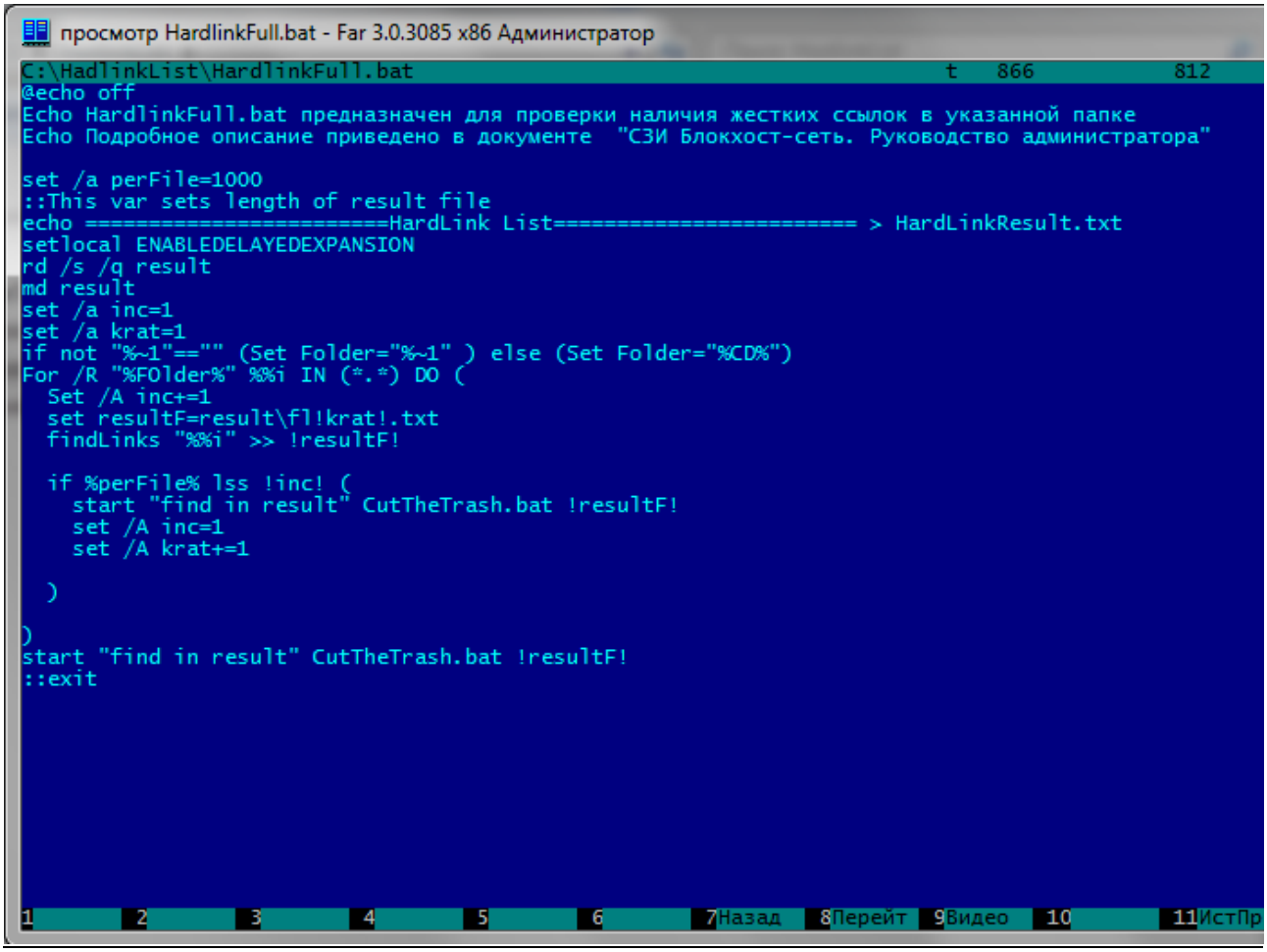


Рисунок 6.5. Содержимое файла HardlinkFull.bat

2) проверить наличие жестких ссылок (в отдельной папке или целиком на жестком диске). Для этого в командной строке (cmd.exe) необходимо выполнить команду *HardlinkFull.bat <Полный путь до проверяемой папки>*\. Вызываемый командный файл *HardlinkFull.bat* запускает программу *FindLinks.exe* для проверки наличия жестких ссылок по указанному пути.

Пример:

- *C:\HardlinkList\HardlinkFull.bat C:* (проверяется наличие жестких ссылок на диске *C:*\);
- *C:\HardlinkList\HardlinkFull.bat C:\user1* (проверяется наличие жестких ссылок в папке C:\user1\).

Если в наименовании пути к проверяемой папке содержатся пробелы или русские буквы, имена папок и файлов необходимо указывать в формате 8.3 (например, Docume~1);

В качестве промежуточного результата в папке запуска командного файла *HardlinkFull.bat* создается папка *result* с перечнем всех файлов по указанному адресу, независимо от наличия у них жестких ссылок.

Командный файл *CutTheTrash.bat* выбирает из общего перечня файлы, которые имеют жесткие ссылки.

В результате в папке …**HardlinkList** (в папке запуска командного файла *HardlinkFull.bat*) создается итоговый файл *HardlinkResult.txt*, содержащий перечень файлов и их жестких ссылок (рис. 6.7).

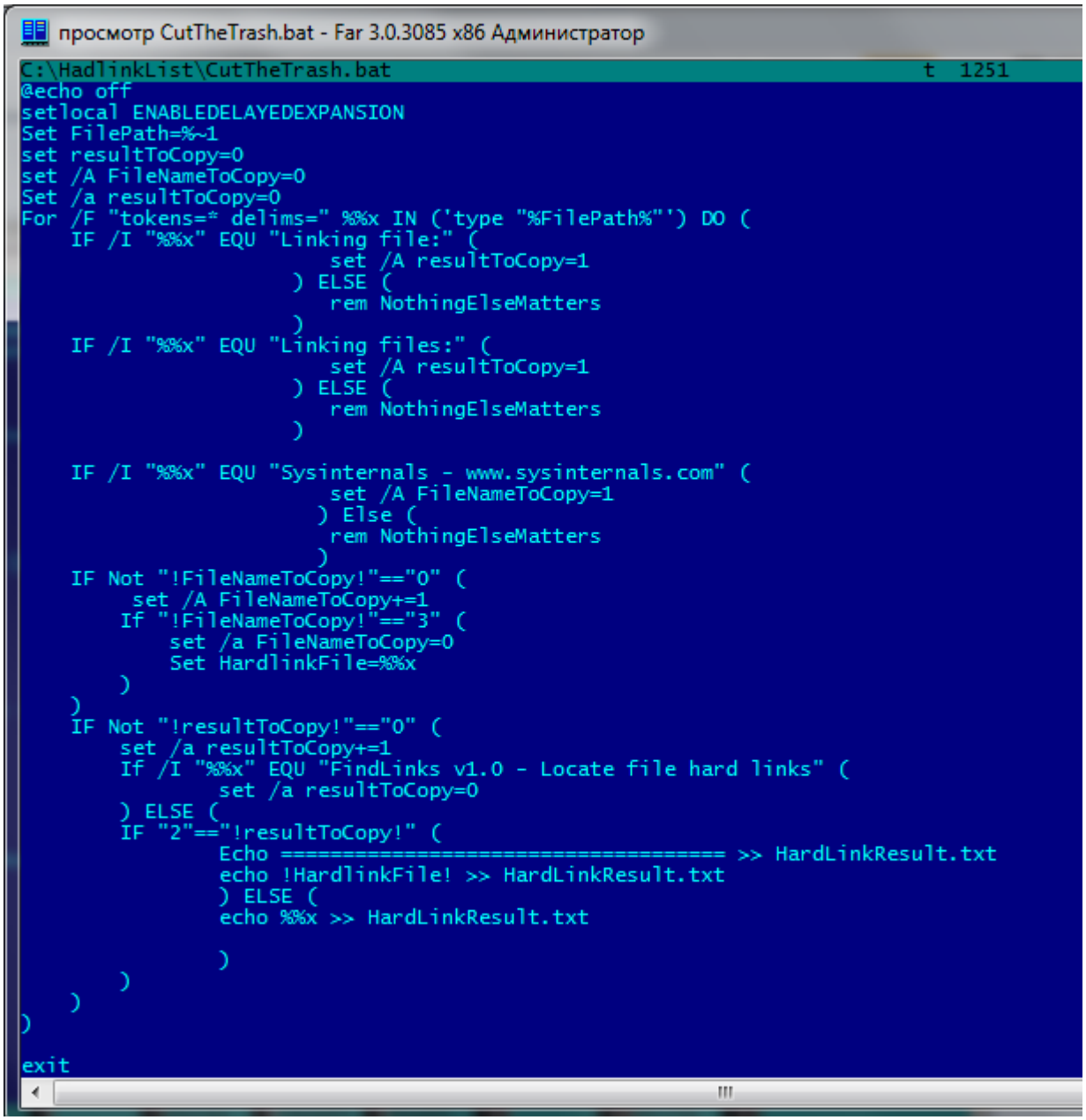


Рисунок 6.6. Содержимое файла CutTheTrash.bat при создании жестких ссылок

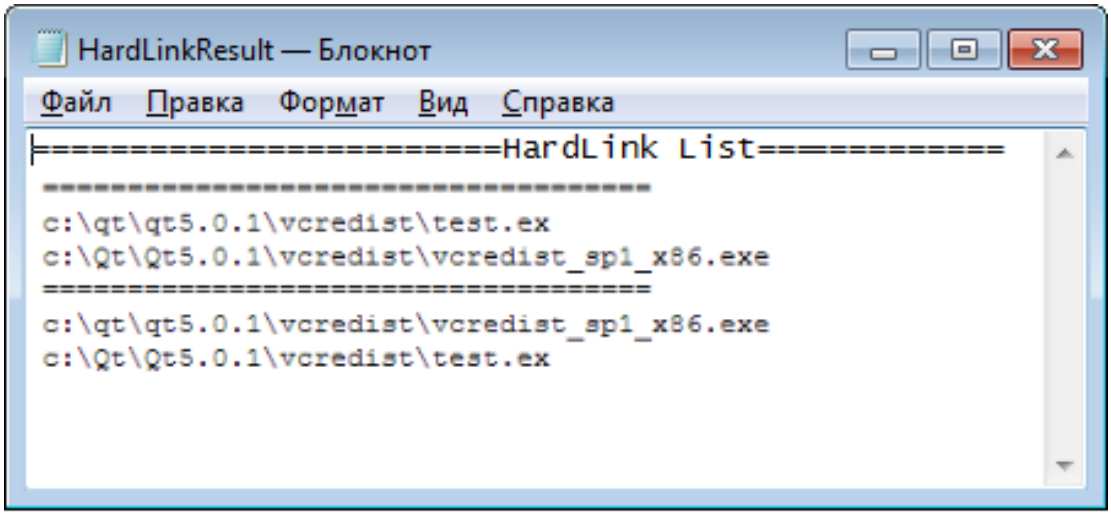


Рисунок 6.7. Пример содержимого файла HardlinkResult.txt

В консоли администрирования СЗИ настройки разграничения доступа к объектам должны быть продублированы и для их жестких ссылок.

При удалении файла с жесткого диска существующие жесткие ссылки, относящиеся к данному файлу, остаются. Доступ к файлу будет возможен, пока в системе существует хотя бы одна жесткая ссылка на него, даже если исходный файл был удален.

Пример.

Для выбранного администратором безопасности пользователя необходимо установить дискреционное разграничение доступа для папок e:\tests\BHS\test1-RW, e:\tests\BHS\test2-R, e:\tests\BHS\test3-W, e:\tests\BHS\test4- в соответствии с таблицей 6.1.1.

Таблица 6.1.1. – Пример дискреционного разграничение доступа для папок при работе с жесткими ссылками

	Права доступа
e:\tests\BHS\test1-RW	RW
e:\tests\BHS\test2-R	R
e:\tests\BHS\test3-W	W
e:\tests\BHS\test4-	-

В этих папках следует проверить наличие файлов, имеющих жесткие ссылки. Это можно сделать с помощью команды *C:\hardlinkList\HardlinkFull.bat e:\tests\BHS*.

В результате в папке *C:\hardlinkList* создается файл *HardlinkResult.txt*, содержащий список файлов и жестких ссылок (рис. 6.8). Из рисунка 6.8 видно, что были обнаружены попарно одинаковые объекты (например, при проверке файла e:\tests\BHS\test1-RW\read.txt был обнаружен файл с такой же структурой данных по адресу e:\tests\bhs\temp\hardlink\test1.txt). Таким образом, при настройке дискреционного механизма разграничения доступа на контроль необходимо устанавливать оба объекта с одними и теми же правами доступа согласно таблице 6.1.1 (рис. 6.9).

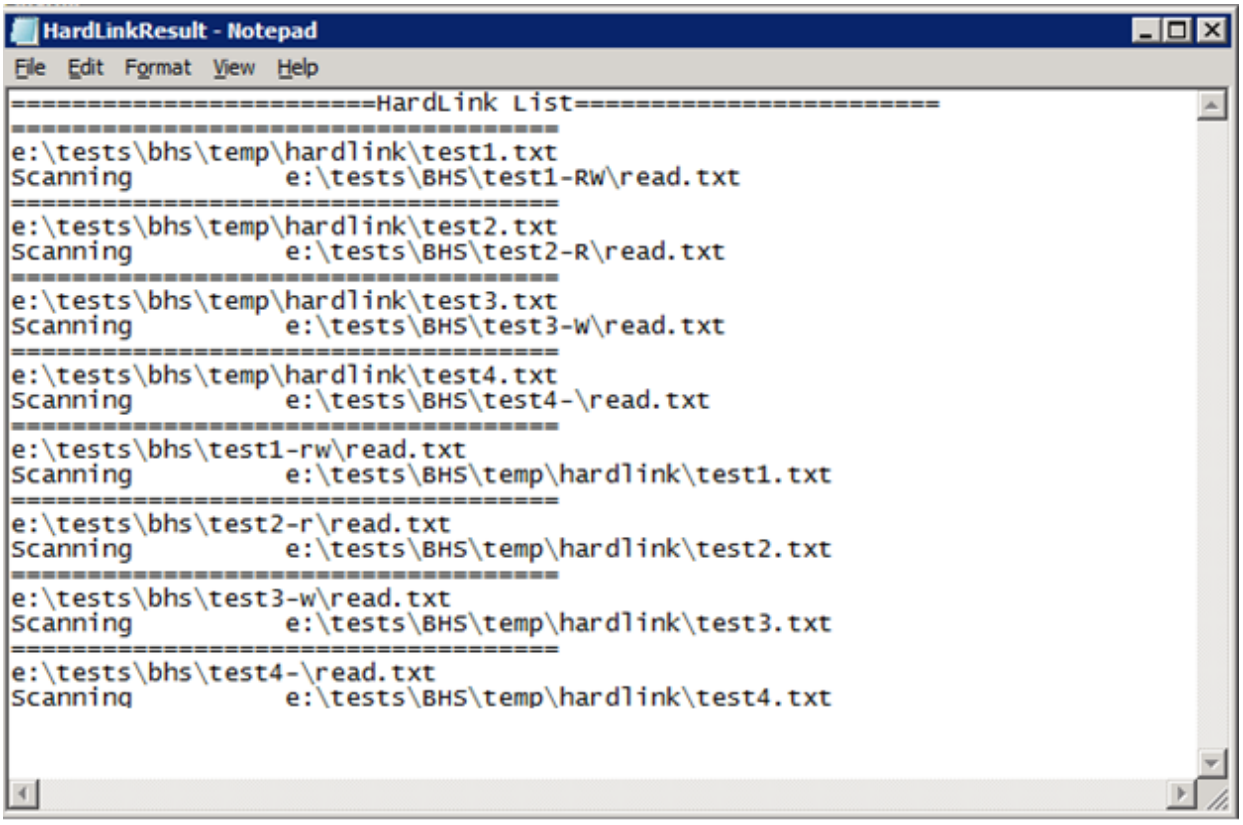


Рисунок 6.8. Пример проверки наличия жестких ссылок

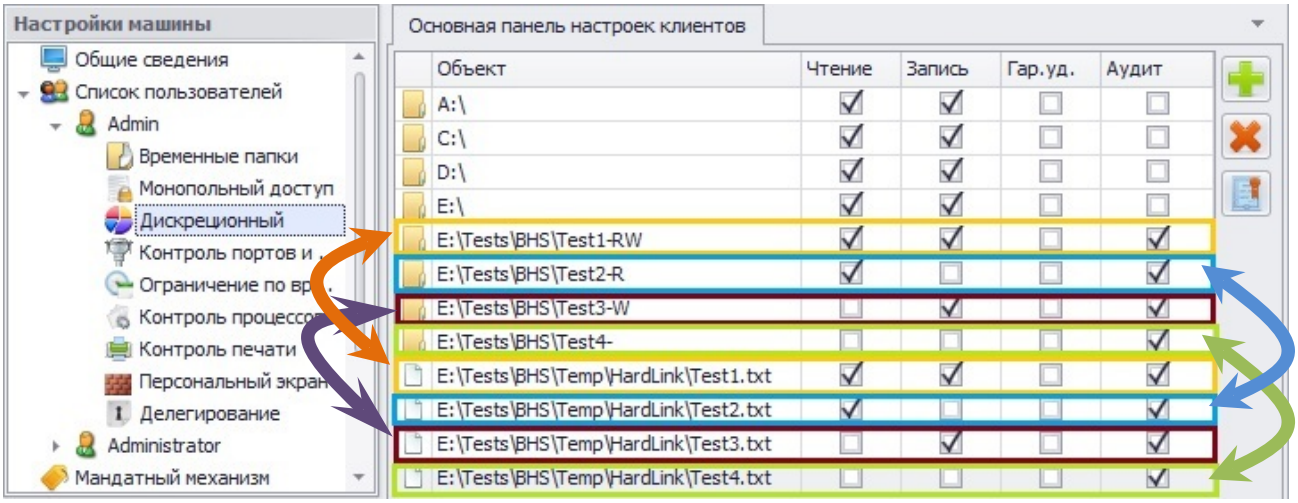


Рисунок 6.9. Установка разграничений доступа в СЗИ для файлов и их жестких ссылок

Особенности работы с символьными ссылками

Основная особенность разграничения доступа к файлам (папкам), имеющим символьные ссылки, состоит в следующем – в консоли администрирования СЗИ права доступа должны быть настроены администратором безопасности обязательно для оригинального файла (оригинальной папки). В этом случае при попытке доступа к этому файлу (папке) через symlink (junction point) будет также осуществляться с учетом настроек СЗИ.

Для проверки наличия символьных ссылок (symbolic links и/или junction points**)** необходимо:

1) выполнить подготовительные операции – на жестком диске создать папку с именем *JunctionList* со следующими файлами: *Junctionlist.vbs*, *CutTheTrash.bat*, *junction.exe*. Содержимое командных файлов *HardlinkFull.bat* и *CutTheTrash.bat* приведено на рисунках 6.10 и 6.11. Данные командные файлы также можно скопировать из каталога *GIS\Documents\LinkList\JunctionList* дистрибутивного диска СЗИ. Программа *junction.exe* поставляется на дистрибутивном диске СЗИ (каталог *GIS\Documents\LinkList\JunctionList*), а также доступна на официальном сайте компании Microsoft (http://technet.microsoft.com/en-us/bb896768).

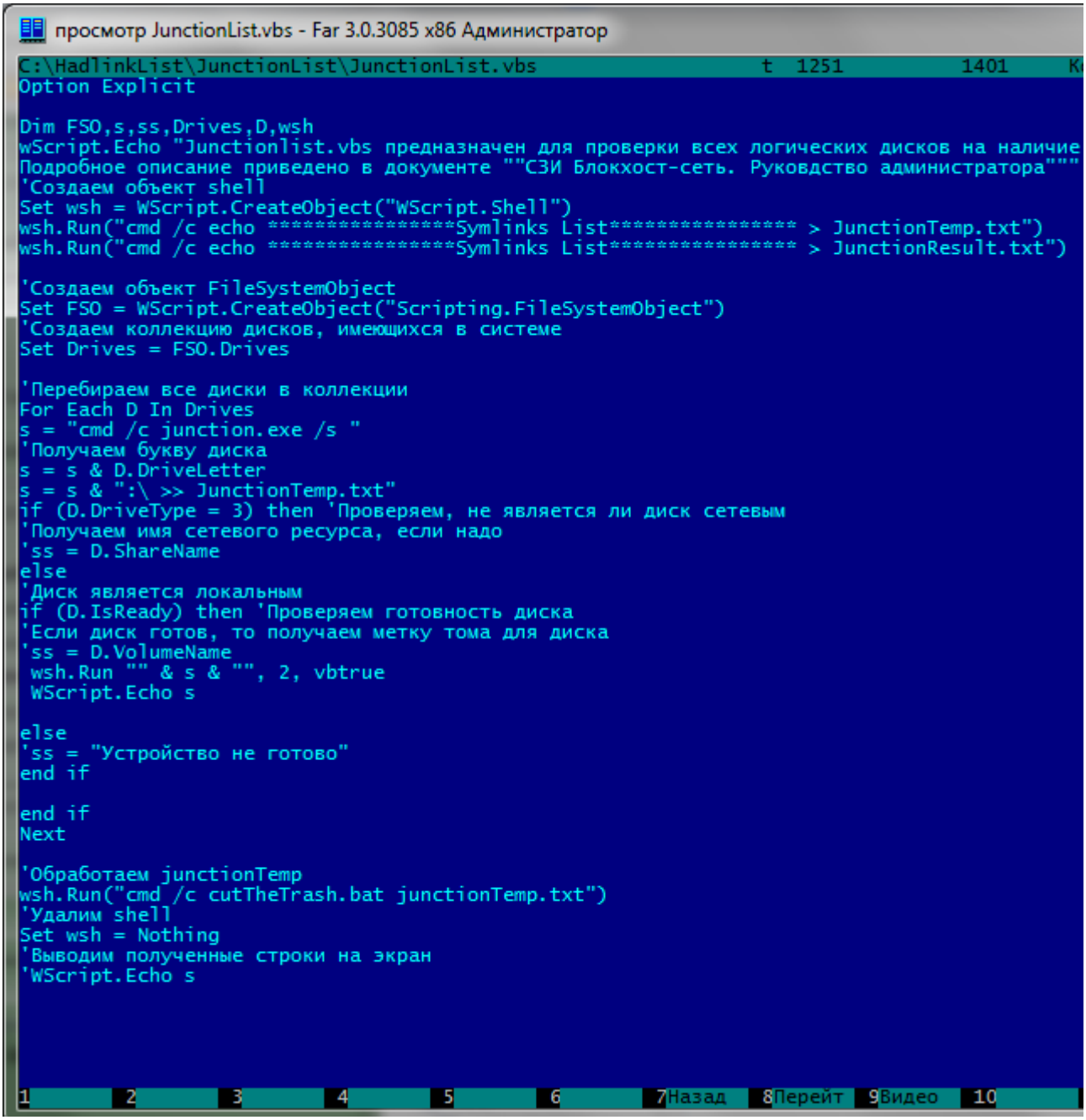


Рисунок 6.10. Содержимое файла Junctionlist.vbs

2) проверить наличие символьных ссылок:
   - *на всех логических дисках*. Для этого двойным щелчком левой кнопкой мыши вызвать файл *Junctionlist.vbs*. *Junctionlist.vbs* проверяет все логические диски на наличие символьных ссылок и при работе использует программу *junction.exe*.

При первом запуске *Junctionlist.vbs* появится окно ознакомления с лицензией программы *junction.exe* (рис. 6.12), в котором нужно нажать кнопку подтверждения. Результатом работы скрипта *Junctionlist.vbs* является файл *JunctionResult.txt* с перечнем файлов и символьных ссылок на них (рис. 6.14). После окончания проверки каждого логического диска появится окно, приведенное на рисунке 6.13.

- *в выбранной папке*. Для этого следует воспользоваться стандартной функциональностью программы *junction.exe*. Например, вызов программы из командной строки с параметрами **junction.exe /s c:\test** позволит провести проверку на наличие символьных ссылок только папки *C:\test*.

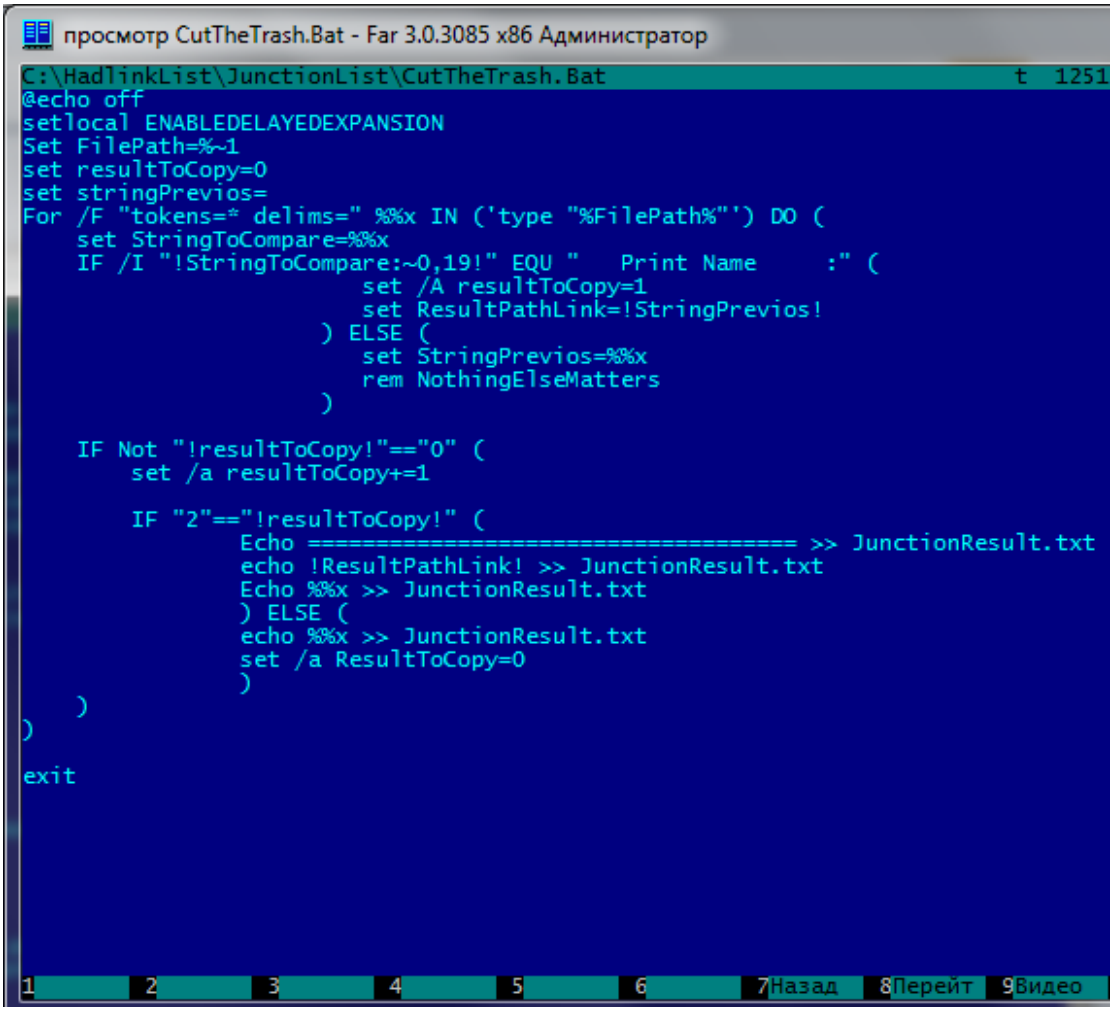


Рисунок 6.11. Содержимое файла CutTheTrash.bat при создании символьных ссылок

Рисунок 6.12. Окно ознакомления с лицензией

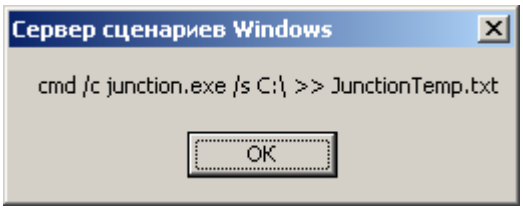


Рисунок 6.13. Окно завершения проверки диска

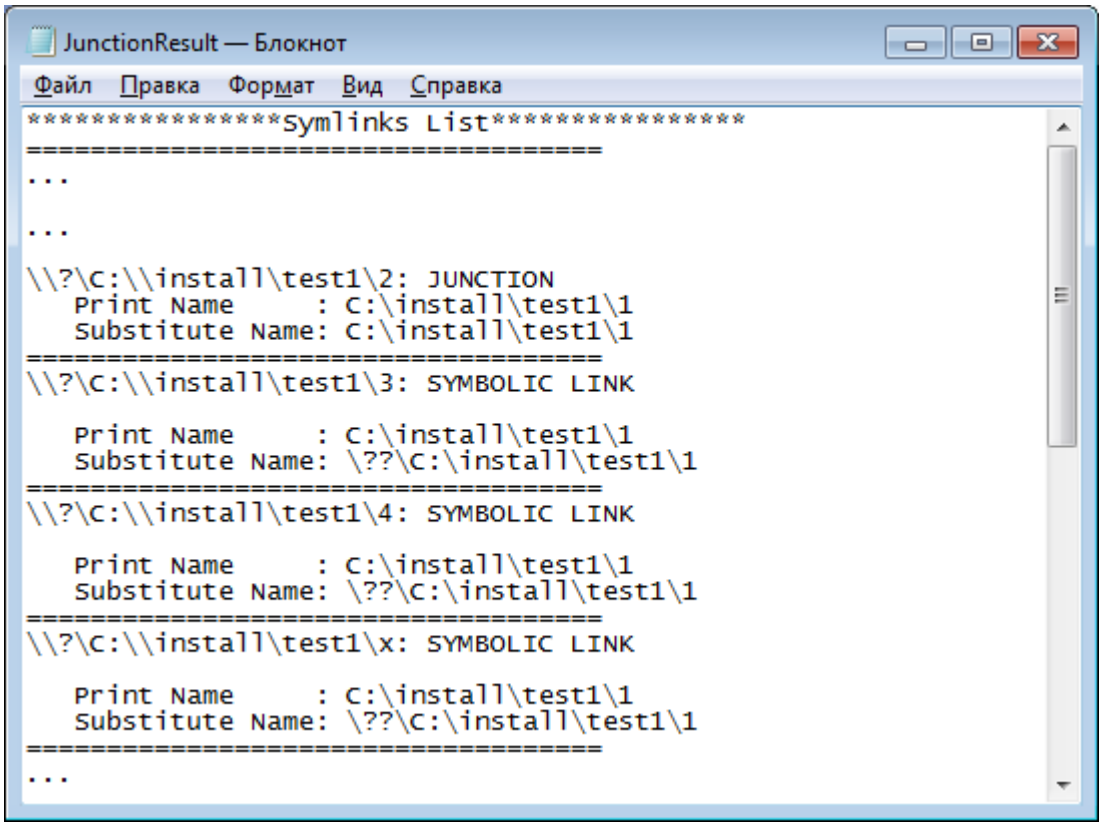


Рисунок 6.14. Пример содержимого файла JunctionResult.txt

1. Первая строка на рисунке 6.14 показывает расположение символьной ссылки (junction point или symlink);
2. В строке *Substitute Name* на рисунке 6.14 показано расположение оригинального файла, для которого создана символьная ссылка.

Установленные в СЗИ права доступа для оригинального файла будут действовать и при попытках доступа к нему по символьной ссылке.

При удалении файла с жесткого диска существующие символьные ссылки, относящиеся к данному файлу, остаются. Однако, в этом случае доступа к исходному файлу при обращении к нему по символьной ссылке не будет.

6.1.2. Разграничение доступа к отчуждаемым физическим носителям информации

В СЗИ «Блокхост-сеть 2.0» реализован механизм разграничения доступа пользователей к отчуждаемым носителям информации. Реализация механизма разграничения доступа к отчуждаемым носителям информации в СЗИ «Блокхост-сеть 2.0» заключается в предоставлении администратору безопасности возможности санкционировать доступ каждого пользователя к следующим устройствам:

- CD- и DVD-накопителям;
- USB-накопителям;
- Устройствам, подключаемым через COM-порты;
- Устройствам, подключаемым через LPT-порты.

Для разграничения доступа пользователей к отчуждаемым физическим носителям информации других типов (накопители на гибких магнитных дисках и съемные накопители на жестких магнитных дисках интерфейсов SCSI, IDE и Serial ATA) администратор безопасности может воспользоваться дискреционным или мандатным механизмом разграничения доступа, рассмотрев требуемый носитель информации как объект файловой системы.

Необходимо учитывать, что если, например, USB-накопитель добавлен в дискреционный механизм с установленными параметрами ***Гар.уд.*** и ***Аудит***, а параметры ***Чтение*** и ***Запись*** не установлены, но в настройках механизма ***Контроль портов и CD*** стоит разрешение использования USB-порта, то к данному USB-накопителю будет обеспечен полный доступ.

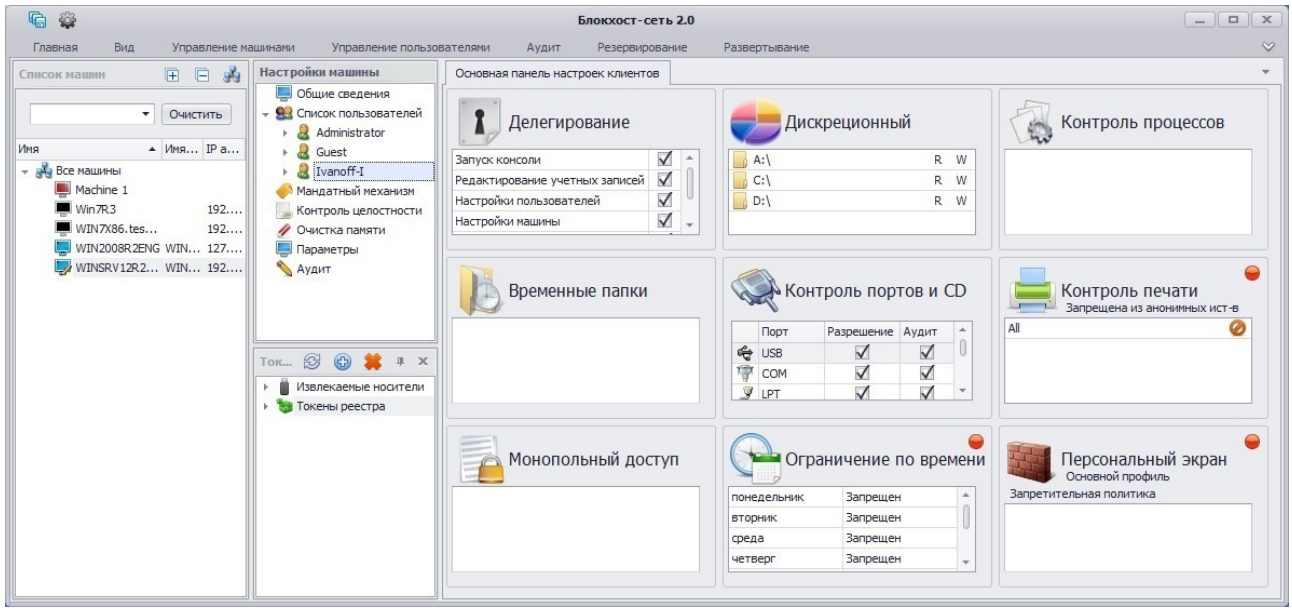
6.1.2.1. Порядок настройки механизма разграничения доступа к отчуждаемым носителям информации и подключаемым устройствам ввода-вывода

Для того чтобы установить правила доступа выбранного пользователя к отчуждаемым физическим носителям информации и подключаемым устройствам ввода-вывода, администратору безопасности необходимо:

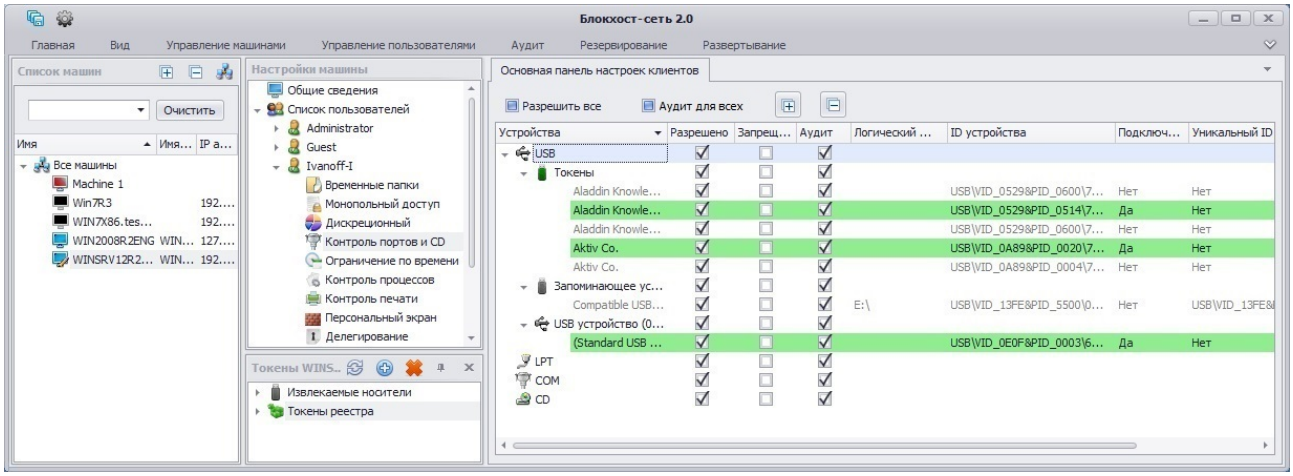
1. В окне **«Список машин»** серверной консоли администрирования выбрать рабочую станцию, для которой будет производиться настройка механизма разграничения доступа к отчуждаемым носителям информации, раскрыв пункт ***Все машины***;
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Контроль портов и CD*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Контроль***

портов и CD (рис. 6.15, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.15, б).

3. Определить доступ пользователя к портам и CD-устройствам, для чего в **Основной панели настроек клиентов** в списке портов и CD-устройств отметить требуемый параметр (***Разрешено*** или ***Запрещено***), расположенный справа от редактируемого порта или подключаемого устройства (рис. 6.15, б).
4. При необходимости возможна фиксация событий, связанных с доступом к контролируемым объектам, в журнал СЗИ «Блокхост-сеть 2.0». Для этого необходимо отметить поле ***Аудит***, расположенное справа от выбранного порта.
5. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.



а)



б)

Рисунок 6.15. Вид окна с настройками механизма контроля портов

При использовании на рабочей станции-клиенте СЗИ программ по работе с CD- и DVD-дисками (для чтения, создания, эмуляции и т.д.), например, UltraISO, установленные настройки разграничения доступа пользователей к CD- или DVD-дисководам будут применены только после перезагрузки рабочей станции.

Установка параметра ***Разрешить все*** позволяет санкционировать использование всех подключаемых к рабочей станции устройств вода-вывода – все переключатели доступа к устройствам находятся в положении ***Разрешено***. Снятие параметра ***Разрешить все*** переводит все переключатели доступа к подключаемым устройствам ввода-вывода в положение ***Запрещено***, в результате чего использование любых подключенных к рабочей станции устройств будет запрещено.

Установка параметра ***Аудит для всех*** позволяет установить переключатели ***Аудит*** для каждого из подключенных к рабочей станции устройств. Соответственно снятие параметра ***Аудит для всех*** снимет отметки в поле ***Аудит*** для каждого устройства.

Кнопки ***Развернуть все***  и ***Свернуть все***  позволяют, соответственно, раскрыть или свернуть дерево подключенных к USB-порту рабочей станции устройств.

6.1.2.2. Настройка доступа пользователя к определенным USB-устройствам

В механизме разграничения доступа пользователей к отчуждаемым носителям информации запрет/разрешение доступа к USB-устройствам может настраиваться индивидуально для каждого USB-устройства, исключая тем самым, возможность использования посторонних устройств.

В механизме ***Контроль портов и CD*** имеется два варианта идентификации USB-устройств для отображения их в списке устройств в серверной консоли администрирования СЗИ:

- **ID устройства (модель устройства)** – описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (**VID**) и продукта (**PID**). Комбинация **VID** и **PID** описывает конкретную модель, но не конкретное устройство;
- **уникальный ID** – описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (**VID**), продукта (**PID**) и **серийного номера**. Не каждое устройство имеет собственный **серийный номер.**

Для избирательного разграничения доступа к USB-устройствам необходимо раскрыть дерево устройств, подключенных к USB-порту (рис. 6.16). В результате отобразится список всех USB-устройств, которые когда-либо подключались к выбранной рабочей станции. USB-устройства, подключенные к рабочей станции в настоящее время, будут выделены зеленым цветом, а в поле ***Подключено*** будет стоять значение ***Да***. Разрешение или запрет использования конкретного USB-устройства на рабочей станции выполняется отметкой параметра ***Разрешено*** или ***Запрещено***, соответственно, напротив имени устройства. Установка одного из параметров (***Разрешено*** или ***Запрещено***) влечет за собой автоматическое снятие другого.

Для одинаковых **моделей устройств** (USB-устройств с одинаковыми **VID** и **PID**, не имеющими серийного номера) установка параметров (***Разрешено*** или ***Запрещено***) для одного из таких устройств влечет за собой автоматическую установку этого же параметра для всех устройств с такими же **VID** и **PID** из списка в серверной консоли администрирования СЗИ.

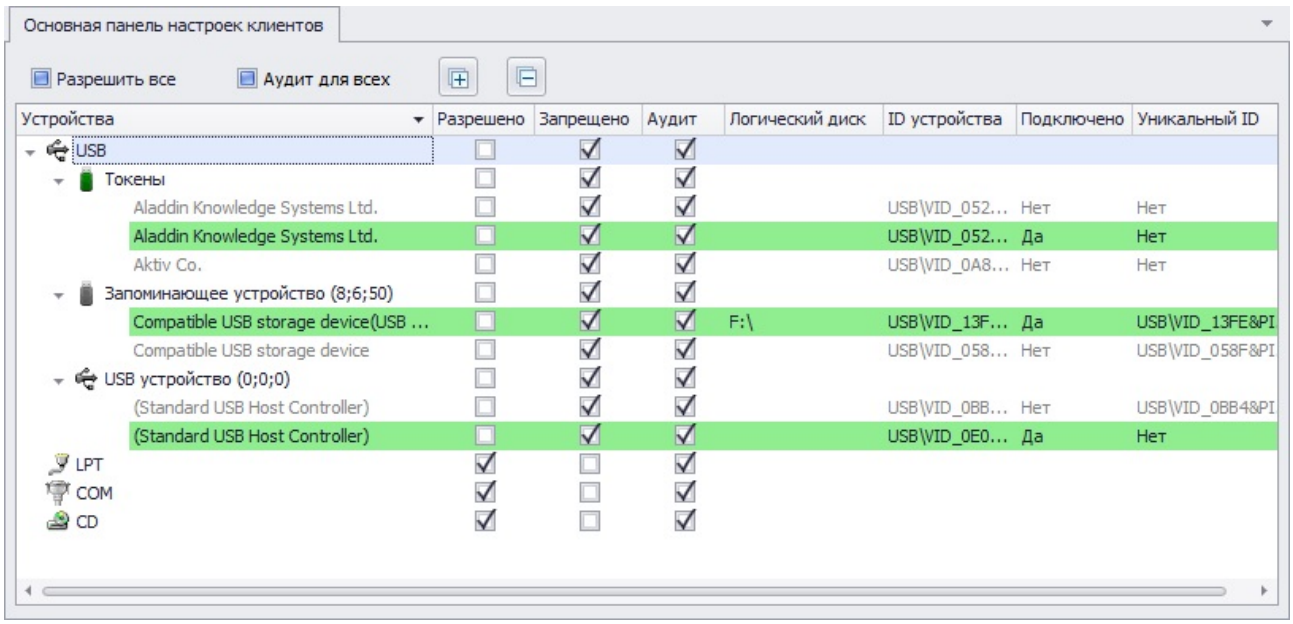


Рисунок 6.16. Полный запрет доступа к USB-устройствам

В СЗИ «Блокхост-сеть 2.0» разграничение доступа пользователей к USB-устройствам основано с использованием структуры иерархии объектов:

- На верхнем уровне находится интерфейс **USB** – установленный параметр ***Запрещено*** (***Разрешено***) в строке **USB** запрещает (разрешает) использование всех подключаемых USB-устройств.
- Затем идут классы устройств (например, на рисунках 6.15 и 6.16 к классам USB-устройств относятся ***Запоминающие устройства*** и ***Токены***) – установленный параметр ***Запрещено*** (***Разрешено***) в строке с названием класса устройства запрещает (разрешает) использование всех USB-устройств этого класса.
- На нижнем уровне находятся сами USB-устройства – установленный параметр ***Запрещено*** (***Разрешено***) в строке с именем устройства запрещает (разрешает) использование только этого устройства (модели устройства).

В зависимости от установленного параметра ***Запрещено*** (***Разрешено***) для объекта верхнего уровня иерархии изменяется и параметр дочернего объекта – он принимает значение, установленное для родительского объекта.

Если изменить установленный параметр ***Запрещено*** (***Разрешено***) одного из дочерних объектов, то для объекта верхнего уровня явно установленный параметр сбрасывается и оба поля ***Запрещено*** и ***Разрешено*** заполняются синим фоном.

В случае подключения к контролируемой рабочей станции нового USB-устройства, которое отсутствовало в списке устройств рабочей станции на момент установки прав разграничения доступа пользователя к отчуждаемым носителям информации, то доступ к такому устройству будет организован следующим образом:

1. Доступ разрешен:

- всем подключаемым USB-устройствам, если параметр ***Разрешено*** установлен для всего интерфейса **USB**;
- всем устройствам одного класса, если установлен параметр ***Разрешено*** для этого класса USB-устройств. При этом поля ***Запрещено*** и ***Разрешено*** для интерфеса **USB** будут заполнены синим цветом;

- одинаковым **моделям одного класса устройств**, если параметр ***Разрешено*** установлен для этой модели USB-устройств. При этом поля ***Запрещено*** и ***Разрешено*** для интерфеса **USB** и класса устройств будут заполнены синим цветом.

2. Доступ запрещен:

- всем подключаемым устройствам, если параметр ***Запрещено*** установлен для всего интерфейса **USB**;
- всем устройствам одного класса, если параметр ***Запрещено*** установлен для этого класса USB-устройств;
- **уникальным** устройствам, если параметр ***Запрещено*** установлен хотя бы для одного устройства данного класса;
- одинаковым **моделям устройств**, если установлен параметр ***Запрещено*** для этой модели устройств.

Пример:

Предположим, АБ необходимо разрешить пользователю **Admin** использование только одного USB-накопителя (в примере на рис. 6.17 – логический диск F:\) на контролируемой рабочей станции, при этом использование других USB-устройств на этой рабочей станции для **Admin** будет запрещено. Порядок действий АБ следующий:

1) В окне **«Список машин»** серверной консоли администрирования выбрать рабочую станцию, для которой будет производиться настройка механизма контроля портов, раскрыв пункт ***Все машины***;
2) В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, раскрыть список индивидуальных настроек пользователя **Admin** и затем выделить пункт ***Контроль портов и CD***;
3) В **Основной панели настроек клиентов** раскрыть пункт ***USB***, если он находится в свернутом состоянии, в результате отобразятся сгруппированные по типам USB-устройства, которые когда-либо подключались к контролируемой рабочей станции по USB-интерфейсу (рис. 6.17);
4) В строке ***USB*** поставить указатель в поле ***Запрещено***, при этом для всех USB-устройств редактируемой рабочей станции также будет отмечен параметр ***Запрещено***. Для фиксации событий доступа к интерфейсу в журнале событий СЗИ указатель в поле ***Аудит*** для USB-порта можно оставить;
5) Затем необходимо установить указатель в поле ***Разрешено*** для USB хост-контроллера, через который будет подключаться накопитель, и для разрешенного к использованию USB-накопителя (в примере на рис. 6.17 – это накопитель, определенный системой как логический диск *F:* из раздела ***Запоминающие устройства***, и *Standard USB Host Controller* из раздела ***USB устройства***).

Если этот USB-накопитель ранее не подключался к редактируемой рабочей станции, то перед установкой разрешений его необходимо подключить к этой рабочей станции.

6) В завершение необходимо сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

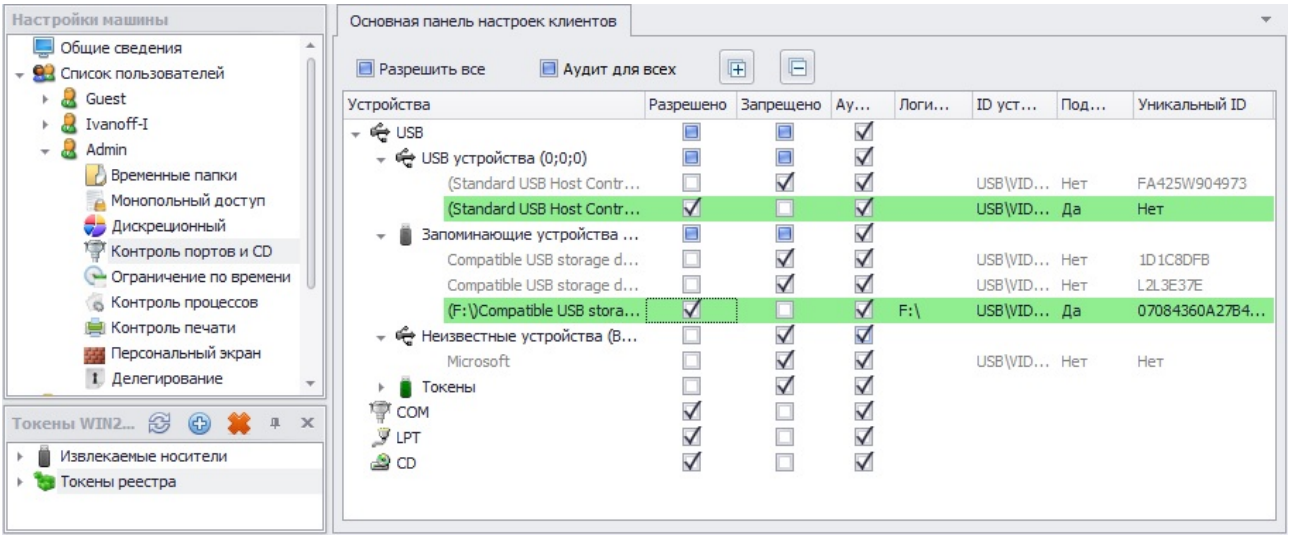


Рисунок 6.17. Настройка доступа пользователя к USB-устройствам

Следует иметь в виду, что разграничение доступа пользователя к USB-устройствам (разрешение/запрет) будет действовать только на той рабочей станции, на которой производилась настройка механизма ***Контроля портов и CD***.

USB-устройства ввода (клавиатуры и мышки) не контролируются механизмом СЗИ ***Контроль портов и CD*** и всегда разрешены к использованию.

6.1.3. Разграничение доступа к запуску процессов

В СЗИ «Блокхост-сеть 2.0» реализован механизм, который позволяет администратору безопасности санкционировать запуск пользователем определенных процессов в системе. Данный механизм позволяет создать модель защиты информации, основанную на ограничениях возможности запуска пользователем и программами исполняемых файлов в сеансе работы пользователя в ОС. Механизм разграничения доступа к запуску процессов позволяет создавать два типа моделей защиты информации.

Первый тип – **модель запрещенных процессов**, работает по принципу «разрешено все, что явно не запрещено». Такие модели основываются на предоставлении возможности администратору безопасности определения для каждого пользователя списка процессов, запрещенных к запуску. Остальные процессы, не вошедшие в этот список, контролироваться не будут, так как будут считаться разрешенными к запуску.

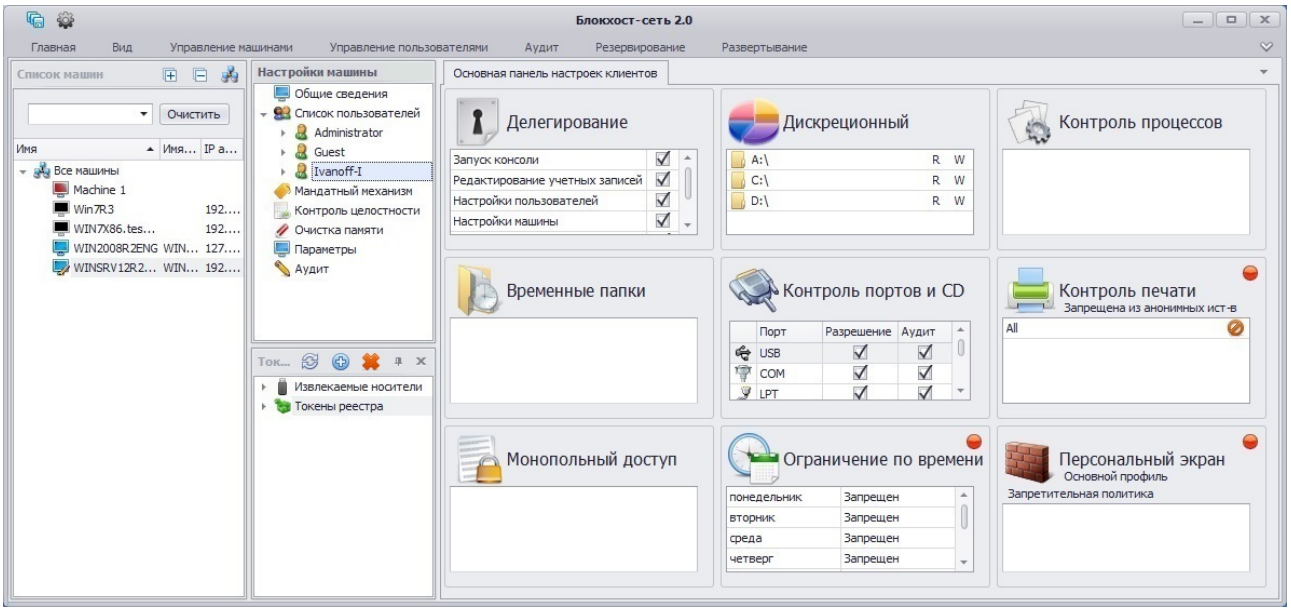
Второй тип – **модель разрешенных процессов (модель замкнутой среды)**, работает по принципу «запрещено все, что явно не разрешено». При использовании модели данного типа администратор безопасности формирует список процессов, разрешенных для запуска конкретным пользователем. СЗИ «Блокхост-сеть 2.0» отслеживает все обращения на запуск процессов и, в случае отсутствия процесса в списке разрешенных, блокирует запуск. Таким образом возможно использование замкнутой программной среды.

6.1.3.1. Создание модели запрещенных процессов

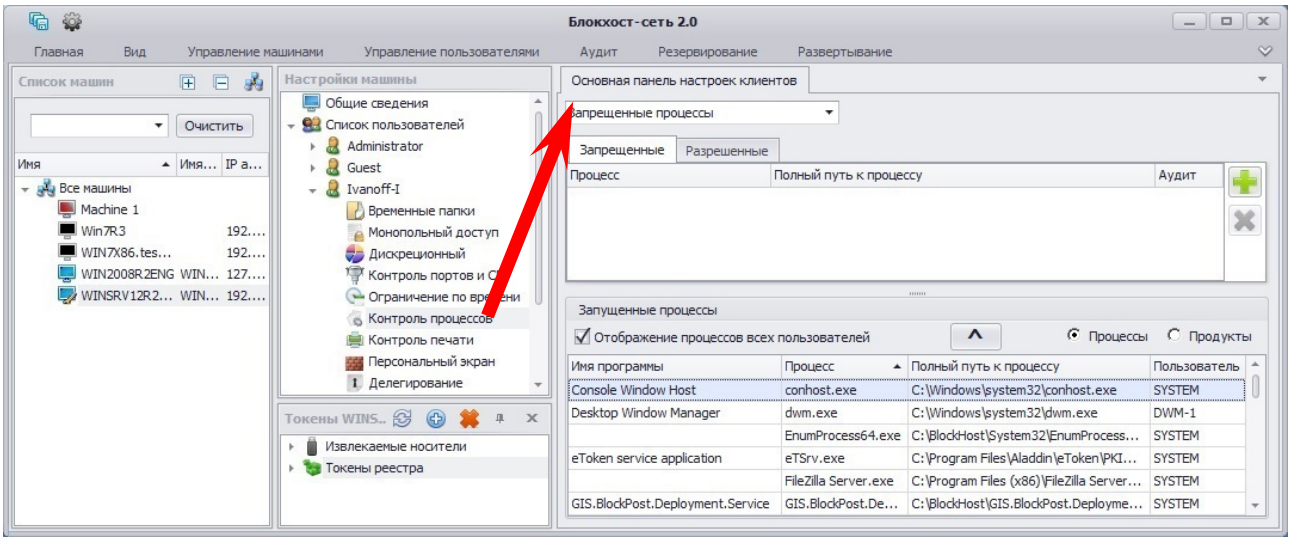
Для создания модели запрещенных процессов администратору безопасности необходимо выполнить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка модели запрещенных процессов.

2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Контроль процессов*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Контроль процессов*** (рис. 6.18, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.18, б).



а)



б)

Рисунок 6.18. Выбор механизма «Контроль процессов»

3. В **Основной панели настроек клиентов** в выпадающем списке выбрать пункт ***Запрещенные процессы*** или выбрать вкладку ***Запрещенные***.
4. Добавить запрещаемые процессы в область настроек одним из способов:
   - захватить и перетащить мышью необходимые объекты из дерева ресурсов (рис. 6.19);
   - выделить в списке запущенных процессов необходимый процесс (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить несколько процессов)

и нажав на кнопку ^ перенести выделенные процессы в список контролируемых;

- нажать кнопку ***Добавить***, и в открывшемся окне **«Выбор»** (см. рис. 6.22) выбрать нужный процесс и нажать кнопку ***Добавить***.

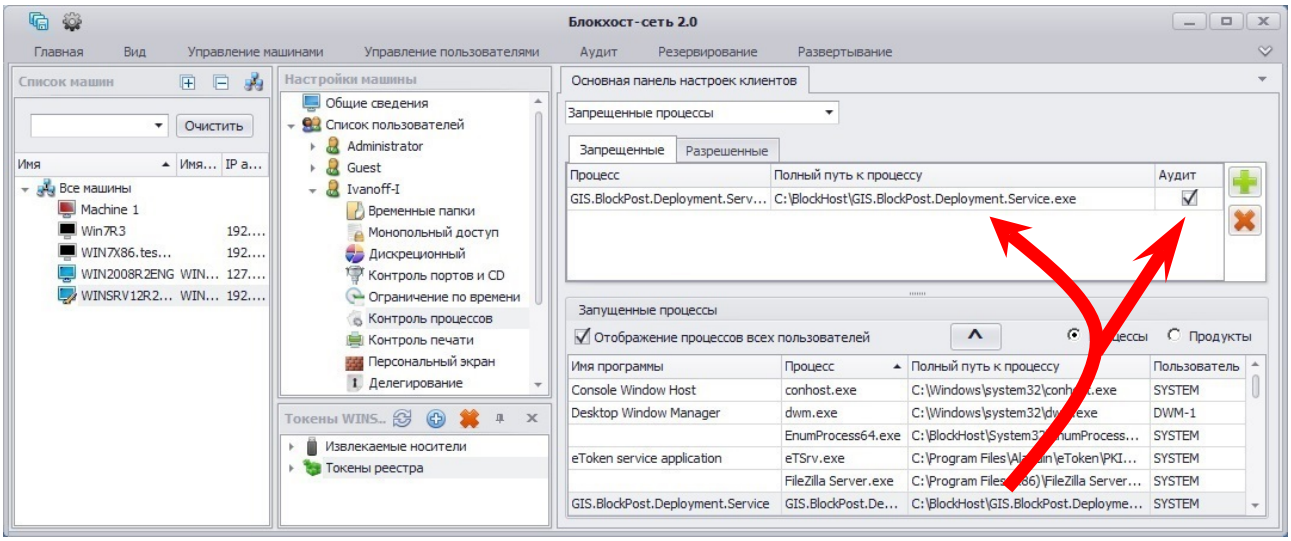


Рисунок 6.19. Добавление запрещаемых процессов

Переключатель ***Процессы↔Продукты*** в области *Запущенные процессы* позволяет отображать либо список запущенных на рабочей станции процессов (переключатель установлен в положение ***Процессы***), либо список всех исполняемых файлов из перечня установленного на рабочей станции ПО (переключатель установлен в положение ***Продукты***).

Процесс, поставленный на контроль, не пропадает из списка запущенных процессов (списка продуктов), однако строка, соответствующая контролируемому процессу, изменяет свой цвет с черного на серый. Повторное добавление процесса на контроль – невозможно.

При настройке механизма контроля процессов для пользователя, который не вошел в ОС на редактируемой рабочей станции, список запущенных процессов будет пустой (переключатель ***Процессы↔Продукты*** установлен в положение ***Процессы***). Для отображения списка всех запущенных на рабочей станции процессов необходимо установить параметр ***Отображение процессов всех пользователей***.

5. Для удаления процессов из списка контролируемых достаточно выбрать в списке запрещенных процессов требуемый процесс и нажать клавишу **<Del>** (для удаления можно также воспользоваться кнопкой ***Удалить***, расположенной справа от списка контролируемых процессов).
6. В СЗИ «Блокхост-сеть 2.0» реализована возможность фиксации событий, связанных с попытками запуска контролируемых процессов, в журнал СЗИ. При необходимости фиксации попыток запуска процессов следует в **Основной панели настроек клиентов** оставить отмеченным параметр ***Аудит***, расположенный справа от выбранного процесса.

7. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Запуск процессов, внесенных в список запрещенных для выбранного пользователя, станет для него невозможен только в том случае, если отключен ***Мягкий режим*** (подробно описан в п. 6.2.4).

6.1.3.2. Особенности работы с жесткими и символьными ссылками при настройке списка запрещенных процессов

В файловой системе NTFS существует технология привязки (Link), позволяющая одному и тому же файлу существовать в нескольких каталогах, иногда под разными именами Подобная привязка называется жесткой связью или жесткой ссылкой (hard link). Другим вариантом привязки файлов является символьная ссылка («junction point» и «symlink»). Более подробное описание жестких и символьных ссылок приведено в пункте 6.1.1.3 настоящего документа.

Для того, чтобы установить ограничение доступа к процессу, имеющему жесткие и символьные ссылки, администратору безопасности необходимо:

1. Проверить наличие жестких и символьных ссылок, относящихся к контролируемым процессам. Проверка проводится аналогично проверке наличия жестких и символьных ссылок при дискреционном разграничении доступа, описание которого приведено в пункте 6.1.1.3 настоящего документа.
2. Вместе с контролируемыми процессами добавить на контроль в настройки консоли администрирования СЗИ жесткие ссылки, относящиеся к ним.
3. Для процессов, имеющих символьные ссылки необходимо убедиться, что в настройки консоли администрирования СЗИ на контроль добавлены исходные (оригинальные) файлы процесса, а не их символьные ссылки (см. подробнее пункт 6.1.1.3 настоящего документа). Установленные в СЗИ права доступа для оригинального файла процесса будут действовать при попытках доступа к нему по символьной ссылке.

Также для ограничения запуска процессов из всех возможных мест и всеми возможными способами следует использовать механизм замкнутой программной среды, описание которого приведено ниже.

6.1.3.3. Создание модели замкнутой среды (модели разрешенных процессов)

Для создания модели замкнутой среды администратору безопасности необходимо выполнить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка модели запрещенных процессов.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Контроль процессов*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Контроль процессов*** (см. рис. 6.18, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (см. рис. 6.18, б)

3. В **Основной панели настроек клиентов** в выпадающем списке выбрать пункт ***Замкнутая среда*** или выбрать вкладку ***Разрешенные*** (рис. 6.20). При этом список разрешенных процессов, отображенный в области настроек, будет пустой:

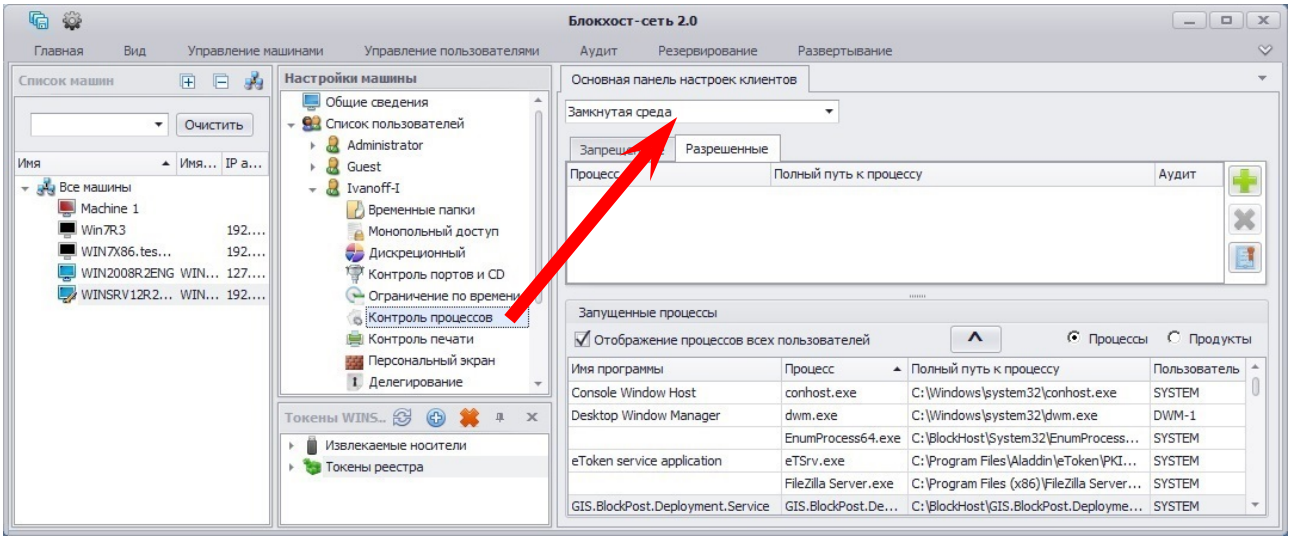


Рисунок 6.20. Создание модели замкнутой среды

4. Добавить разрешенные пользователю для запуска процессы в список контролируемых одним из перечисленных ниже способов:
   - захватить и перетащить мышью необходимые объекты из дерева ресурсов в область настроек:

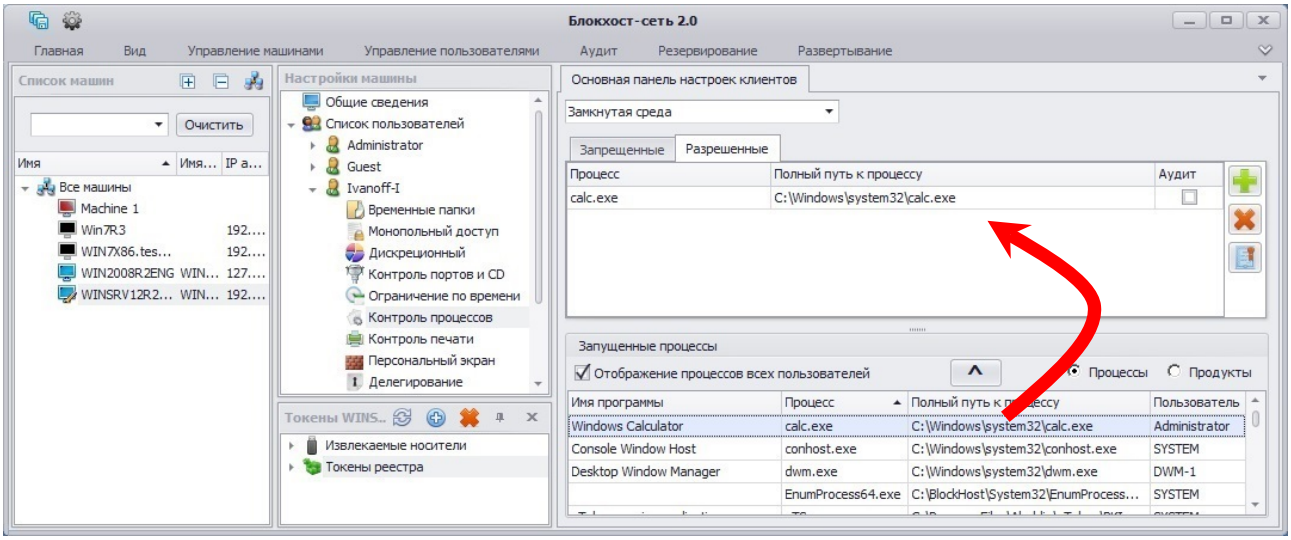


Рисунок 6.21. Добавление разрешенных процессов в список

   - выделить в списке запущенных процессов необходимый процесс (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить несколько процессов) и нажав на кнопку ^ перенести выделенные процессы в список контролируемых;
   - нажать кнопку ***Добавить*** , и в открывшемся окне **«Выбор»** (рис. 6.22) выбрать нужный процесс и нажать кнопку ***Добавить***:

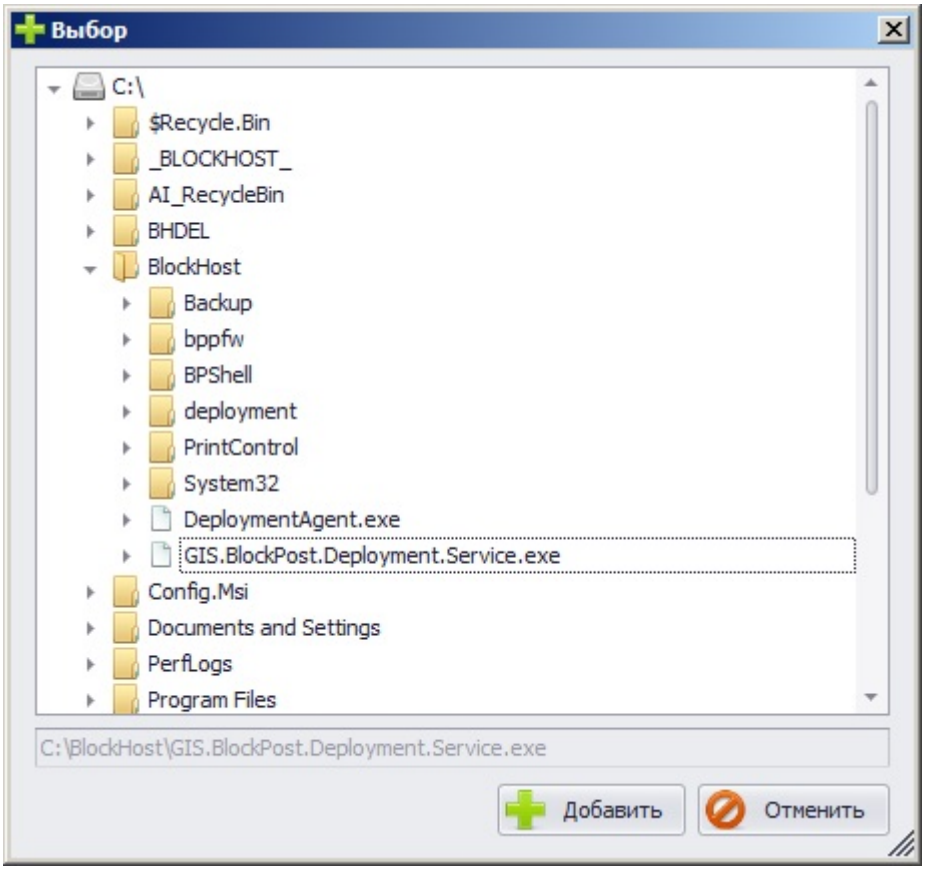


Рисунок 6.22. Окно выбора разрешенных процессов

Разрешенные для запуска процессы появятся в области настроек (рис. 6.23);

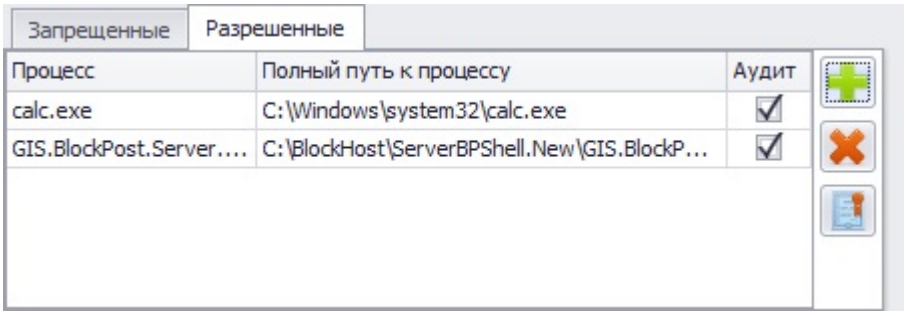


Рисунок 6.23. Отображение добавленного процесса

5. Затем необходимо установить точный перечень процессов, запускаемых в сеансе пользователя и необходимых для работы ОС (в противном случае пользователь, к которому применено ограничение, не сможет работать в системе). Для установления такого перечня нужно воспользоваться опцией ***Мягкий режим*** и выполнить следующие действия:
   - в окне **«Настройки машины»** консоли администрирования выбрать пункт ***Параметры***;
   - в **Основной панели настроек клиентов** установить указатель напротив поля ***Мягкий режим*** (рис. 6.24);

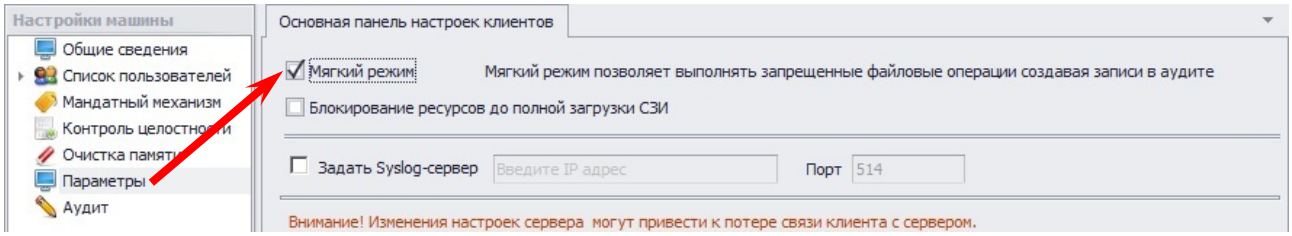


Рисунок 6.24. Включение «Мягкого режима»

- сохранить настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ;
- затем пользователь, к которому применяются ограничения, войдя в ОС на редактируемой рабочей станции, осуществляет на ней свои обычные действия (запуск приложений, работа с документами, доступ к локальным и сетевым ресурсам);
- далее АБ в серверной консоли администрирования СЗИ должен снова перейти к настройке модели разрешенных процессов выбранного пользователя на контролируемой рабочей станции и в **Основной панели настроек клиентов** нажать кнопку ***Сформировать замкнутую среду***  (см. рис. 6.21);
- начнется процесс загрузки сообщений аудита, который в зависимости от количества событий может занять продолжительное время (рис. 6.25);

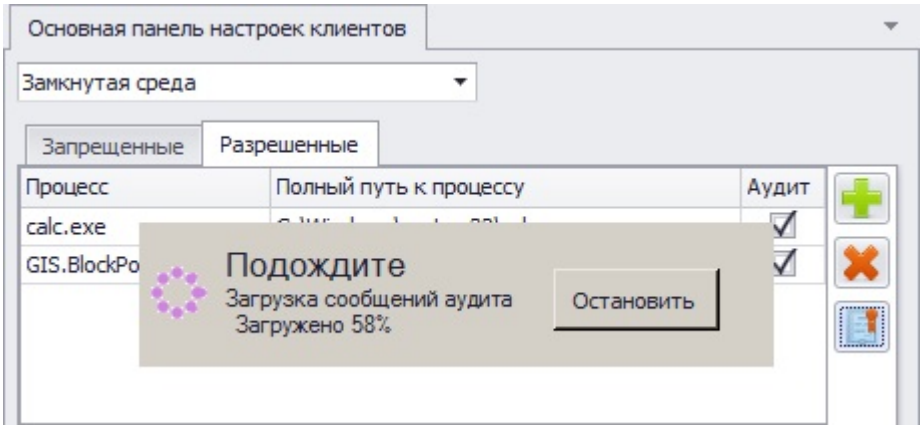


Рисунок 6.25. Процесс загрузки сообщений аудита при формировании замкнутой среды

- в появившемся окне **«Формирование среды»** указать промежуток времени, в течение которого происходила фиксация действий пользователя, и нажать кнопку ***ОК***:

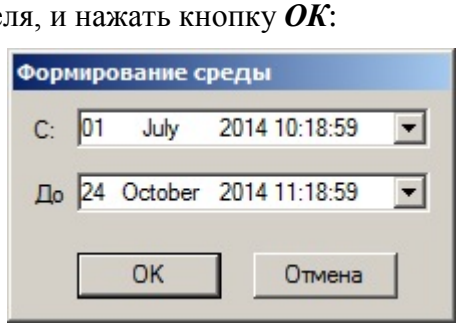


Рисунок 6.26. Окно «Формирование среды»

- в области контролируемых процессов появятся все процессы, которые были запущены во время сеанса работы пользователя на рабочей станции:

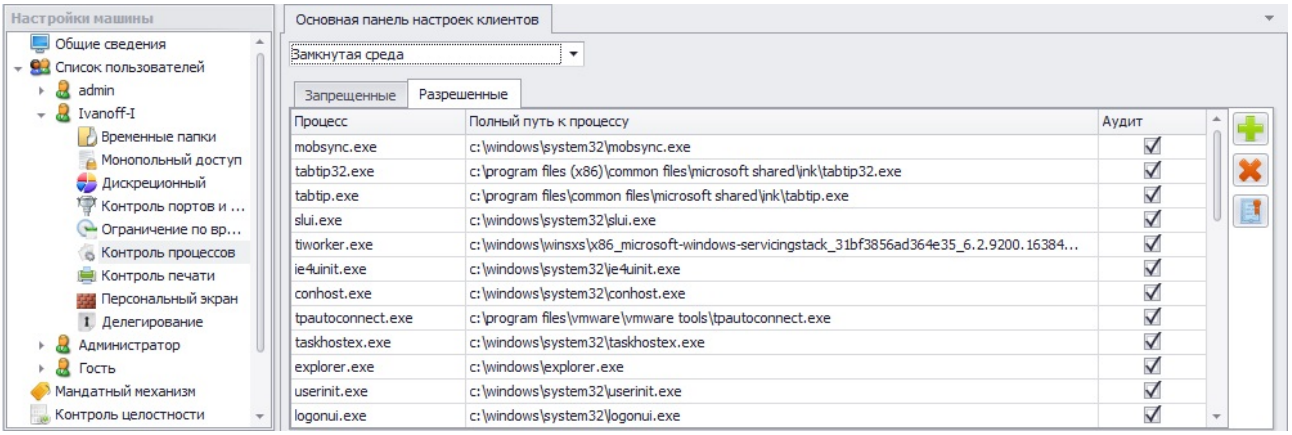


Рисунок 6.27. Список процессов, разрешенных к запуску пользователем

- При необходимости можно откорректировать этот список, удалив ненужные процессы, для чего необходимо выделить процесс (для выделения нескольких процессов можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и нажать клавишу **<Del>** или кнопку ***Удалить*** , расположенную справа от списка контролируемых процессов;
- Также можно разрешить фиксацию событий доступа к контролируемым объектам (запуска процессов) в журнал событий СЗИ «Блокхост-сеть 2.0», оставив отмеченным параметр ***Аудит***, расположенный справа от выбранного процесса;
- затем отключить опцию ***Мягкий режим*** на настраиваемой рабочей станции, выбрав в окне **«Настройки машины»** консоли администрирования пункт ***Параметры*** и сняв указатель с поля ***Мягкий режим*** в **Основной панели настроек клиентов** (рис. 6.24);

6. Сохранить настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

После создания списка разрешенных процессов пользователь сможет запускать только процессы, добавленные в список. Запуск процессов, отсутствующих в списке (например, игры, Internet и пр.), будет запрещен.

6.1.4. Разграничение времени доступа в систему

Механизм разграничения времени доступа в систему предназначен для установления ограничений по времени на использование пользователями защищаемых СВТ. Данный механизм позволяет осуществить разграничение времени:

- Входа пользователей в систему.
- Нахождения пользователей в системе.

Разграничение времени доступа в систему осуществляется на основании сравнения текущего дня недели и времени (с точностью до часа) с заданными администратором безопасности настройками СЗИ для данного пользователя.

6.1.4.1. Порядок настройки механизма разграничения времени работы пользователя в системе

Для настройки механизма разграничения времени доступа пользователей в ОС защищаемой рабочей станции администратору безопасности необходимо выполнить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма разграничения времени доступа пользователей в систему.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Ограничение по времени*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Ограничение по времени*** (рис. 6.28, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.28, б).
3. В **Основной панели настроек клиентов** установить параметр ***Включить временные ограничения*** (рис. 6.28, б).

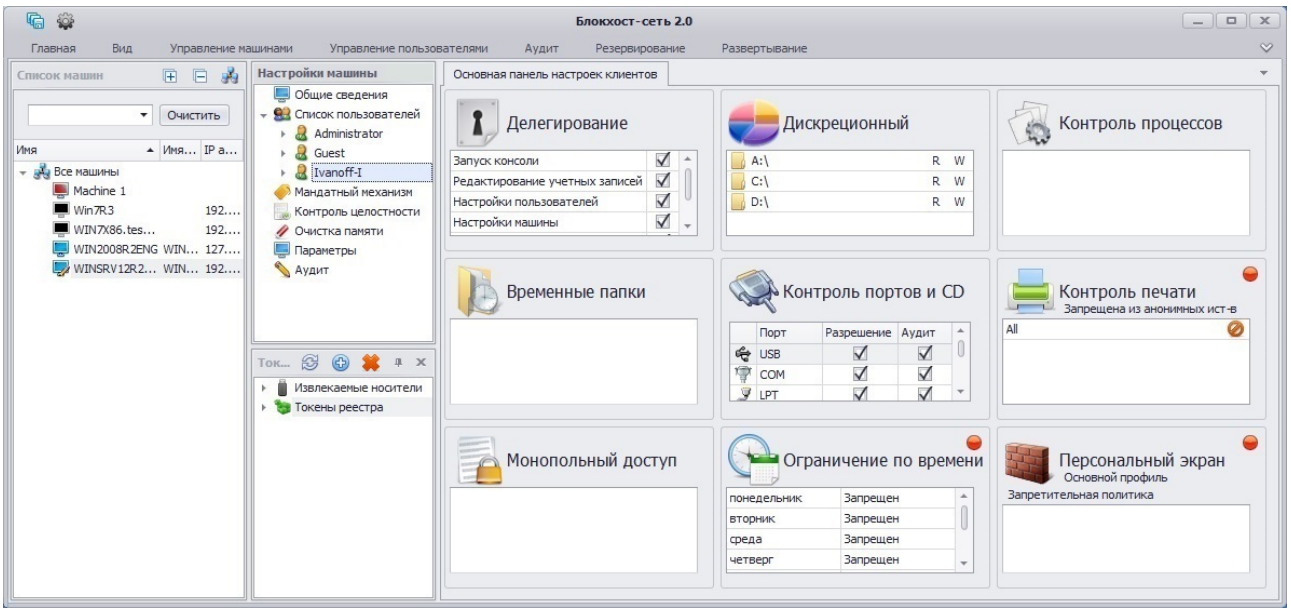
   По умолчанию механизм разграничения времени работы пользователя в системе отключен, т.е. всем добавленным в СЗИ пользователям разрешена работа в ОС контролируемой рабочей станции в любое время.

4. Установить время, в которое работа на рабочей станции пользователю будет запрещена. Для этого левой кнопкой мыши отметить соответствующие временные интервалы для каждого из дней недели. Красным цветом отмечаются промежутки времени, в которые работа запрещена, зеленым – разрешена (рис. 6.28, в).

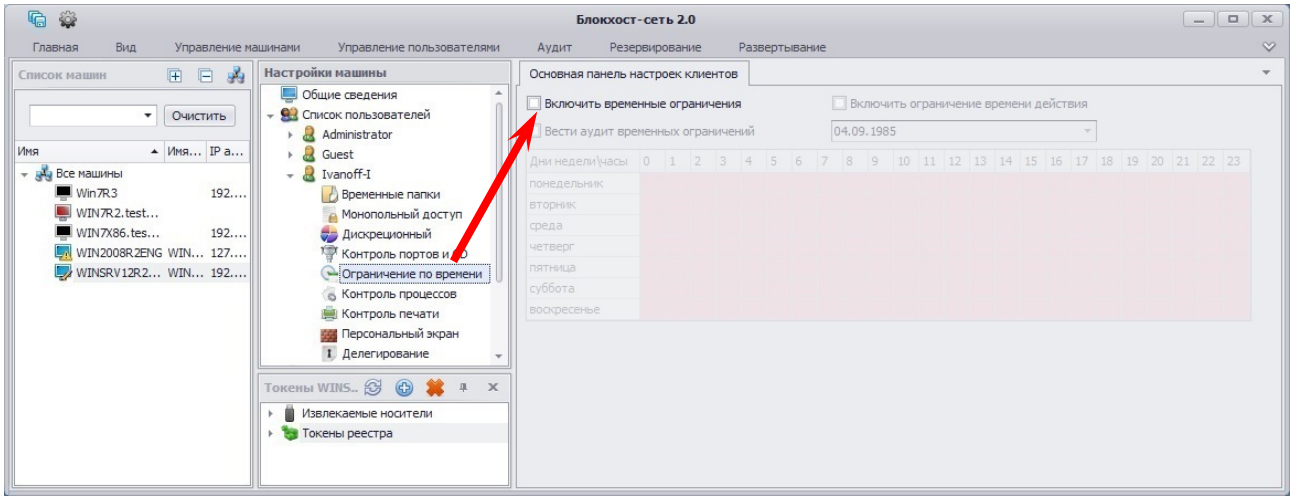
   При настройке механизма разграничения времени работы пользователей в серверной консоли администрирования СЗИ **невозможно** установить два интервала времени, в течение которых работа пользователя разрешена. Например, с 9 до 13 часов и с 14 до 18 часов, запрещая, таким образом, время работы пользователя с 13 до 14 часов.

5. При необходимости можно разрешить фиксацию попыток входа пользователей в систему в несанкционированное время. Для этого в области настроек необходимо выбрать пункт ***Вести аудит временных ограничений***.
6. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

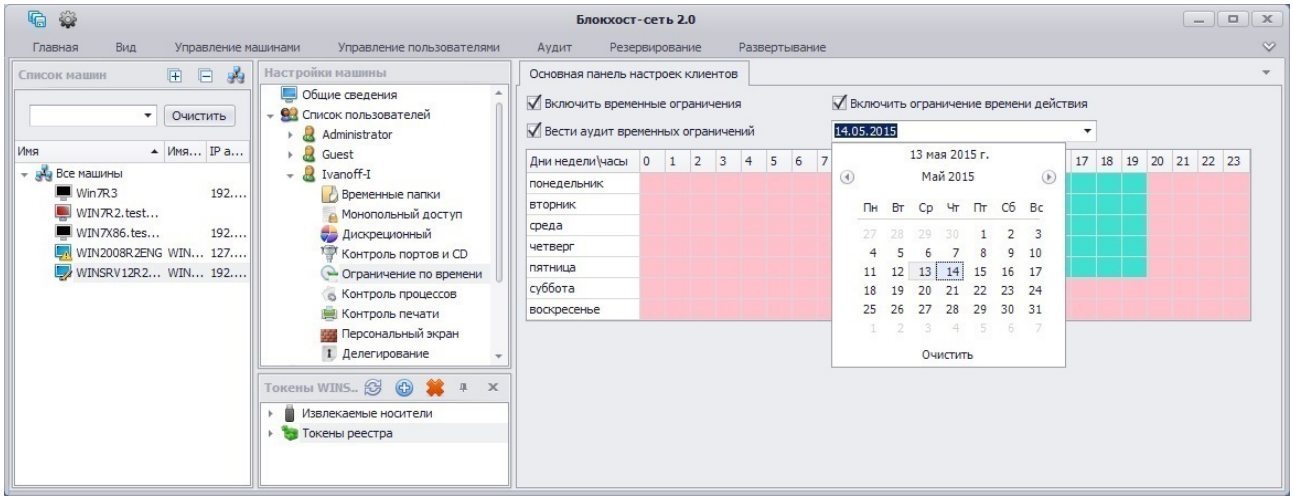
При настройке механизма разграничения времени работы пользователя на контролируемой рабочей станции администратор безопасности должен учесть, что для одного и того же дня недели время начала работы не может превышать время окончания работы.



а)



б)



в)

Рисунок 6.28. Настройка временных ограничений

Установка параметра ***Включить ограничение времени действия*** (рис. 6.28, в) позволяет указать дату, после окончания которой (в 23 часа 59 минут указанной даты) перестанут действовать, установленные для пользователя настройки механизма разграничения времени работы на рабочей станции.

При включенном механизме разграничения доступа пользователя в систему указанный пользователь не сможет войти в систему в запрещенное время – процесс входа пользователя в ОС закончится ошибкой с отображением сообщения: *Только администратор может войти в это время в систему*. После троекратной неудачной попытки входа пользователя в ОС рабочая станция будет автоматически перезагружена.

Во время работы пользователя на рабочей станции, с включенным механизмом разграничения доступа пользователя в систему, за пять минут до окончания разрешенного периода времени работы пользователя в ОС появится предупреждающее сообщение (рис. 6.29) о принудительном завершении работы ОС. Для исключения случайной потери данных пользователь должен сохранить все несохраненные данные и осуществить выход из системы.

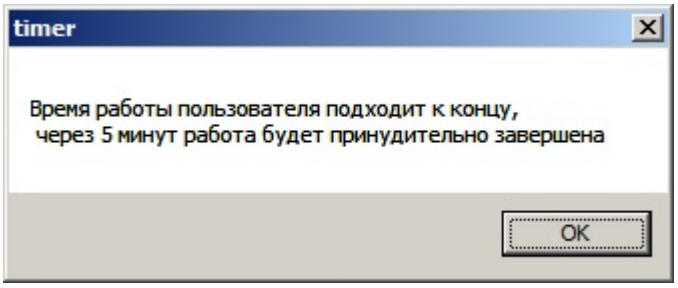


Рисунок 6.29. Предупреждение об окончании времени работы пользователя в ОС

В случае продолжения работы пользователя в системе, по окончании периода разрешенного времени будет осуществлено автоматическое завершение сеанса работы пользователя в ОС. При этом работа всех запущенных приложений также будет завершена – все несохраненные данные будут утеряны.

6.1.5. Настройки мандатного механизма разграничения доступа

В СЗИ «Блокхост-сеть 2.0» реализован механизм мандатного (полномочного) разграничения доступа. Реализация мандатного механизма заключается в возможности присвоения администратором безопасности субъектам (пользователям) и объектам (ресурсам) классификационных меток, отражающих их место в иерархии системы разграничения доступа. Посредством этих меток субъектам и объектам назначаются классификационные уровни (уровни уязвимости, категории конфиденциальности и т.п.).

Общий принцип работы мандатного механизма основан на взаимосвязи субъектов доступа (пользователей), объектов доступа (объектов файловой системы) и классификационных уровней (значений мандатных меток). Доступ субъекта к объекту санкционируется лишь в том случае, если выполняется ряд условий. Условия доступа субъектов к объектам для СЗИ «Блокхост-сеть 2.0» приведены в таблице 6.1.2.

При присвоении объекту мандатной метки (определении классификационного уровня объекта) соблюдается правило наследования, т.е. все вложенные в него объекты (любой степени вложенности) получают тот же классификационный уровень только в том случае, если им не определен никакой другой уровень.

Значения меток мандатного механизма определяются администратором безопасности исходя из требований политики безопасности. Мандатная метка может принимать целочисленные значения в диапазоне от 1 до 255. Таким образом, в распоряжении администратора безопасности находятся 255 классификационных уровней.

В СЗИ «Блокхост-сеть 2.0» субъекты могут осуществлять следующие виды доступа к объектам:

- доступ на *чтение*. Субъект может читать информацию из объекта, если его мандатная метка не меньше, чем мандатная метка объекта, к которому выполняется попытка доступа. Субъект может осуществлять копирование объекта при условии строгого равенства мандатной метки субъекта, мандатной метки копируемого объекта и мандатной метки объекта файловой системы, в который производится копирование;
- доступ на *запись*. Пользователь может осуществлять запись в объект, только если значение мандатной метки пользователя равна значению мандатной метки объекта.

Для выполнения операции записи пользователю, имеющему большее значение мандатной метки, необходимо выполнить вход в систему с тем значением, которое соответствует значению ресурса, открываемого на запись.

Если пользователь вошел в систему со значением мандатной метки, меньше значения мандатной метки папки, то просмотр содержимого или запись в папку невозможна.

Таблица 6.1.2 – Условия доступа субъектов к объектам при мандатном механизме разграничения доступа СЗИ «Блокхост-сеть 2.0»

Вид доступа	Соотношение мандатных меток субъекта (МС) и объекта (МО)
Чтение	**МС ≥ МО**
Запись	**МС = МО**

Порядок создания мандатных меток и их сопоставление ресурсам рабочей станции описаны в пункте 6.2.1. настоящего документа.

6.1.5.1. Сетевой мандатный режим

В сетевой версии СЗИ «Блокхост-сеть 2.0» администратор безопасности может задать мандатные метки для всех пользователей и всех сетевых ресурсов рабочих станций, входящих в защищенную сеть СЗИ от НСД «Блокхост-сеть 2.0».

Значения меток мандатного механизма устанавливаются администратором безопасности исходя из требований политики безопасности принятой в организации. Мандатная метка может принимать целочисленные значения в диапазоне от 1 до 255. Таким образом, в распоряжении администратора безопасности находятся 255 классификационных уровней.

6.1.5.2. Работа мандатного механизма разграничения доступа в сети, защищенной СЗИ от НСД «Блокхост-сеть 2.0»

На сервер СЗИ в момент запуска служб СЗИ на контролируемой рабочей станции отправляется имя рабочей станции, вошедшей в сеть, а также после входа пользователя в ОС рабочей станции – имя пользователя и значение мандатной метки, с которой он вошел на рабочую станцию.

Поэтапный процесс подключения клиента к сети СЗИ от НСД «Блокхост-сеть 2.0» приведен на рисунках 6.30 – 6.34.

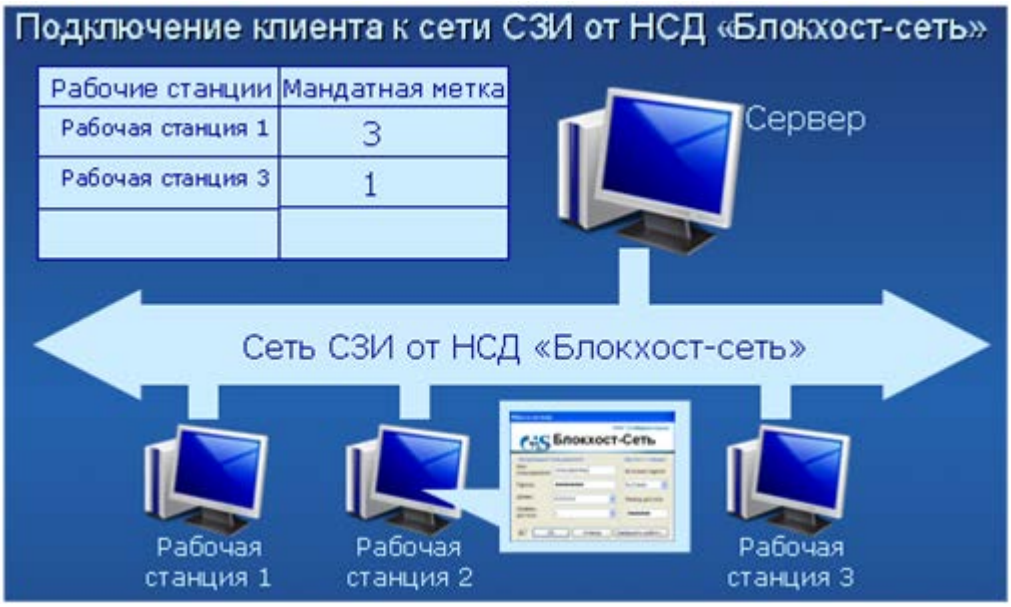


Рисунок 6.30. Состояние сети СЗИ от НСД «Блокхост-сеть 2.0» до включения клиента

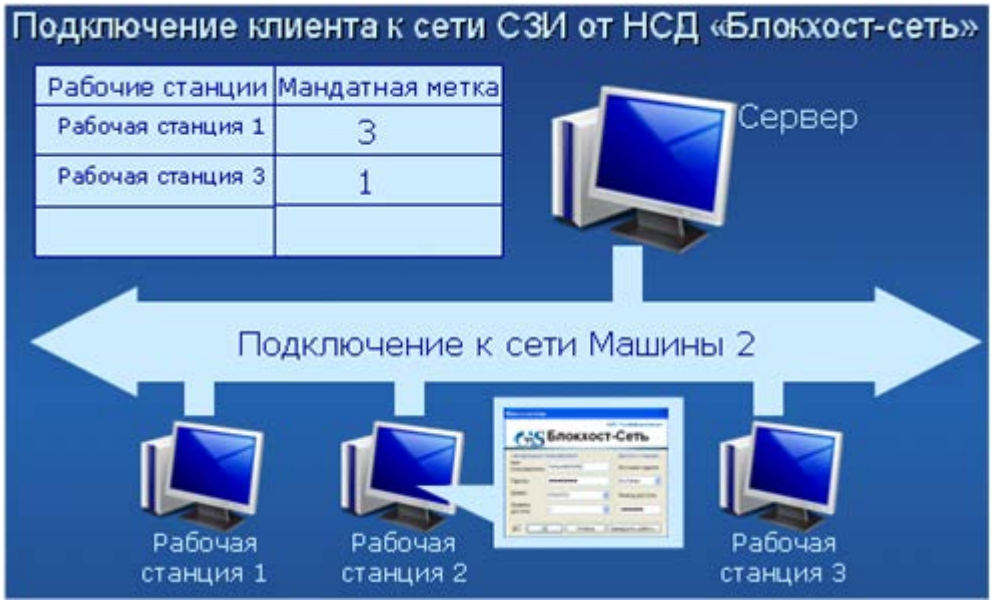


Рисунок 6.31. Подключение клиента к сети СЗИ от НСД «Блокхост-сеть 2.0»

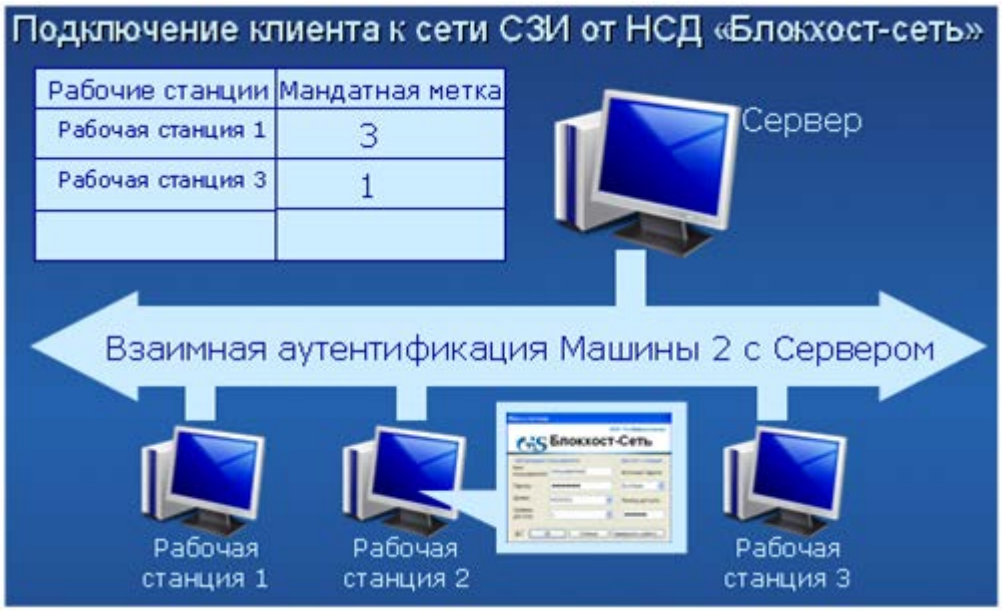


Рисунок 6.32. Процесс аутентификации клиента в сети СЗИ от НСД «Блокхост-сеть 2.0»

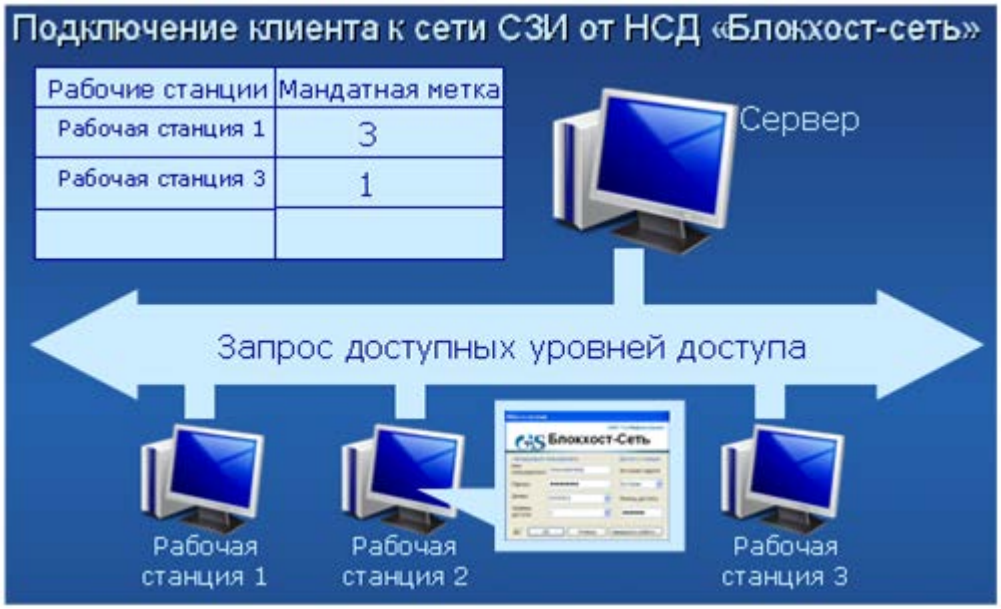


Рисунок 6.33. Передача сведений об уровне доступа клиента в сеть СЗИ от НСД «Блокхост-сеть 2.0»

Рисунок 6.34. Состояние сети СЗИ от НСД «Блокхост-сеть 2.0» после включения клиента

При обращении пользователя к ресурсам, находящимся на удаленной рабочей станции, происходит проверка, находится ли эта рабочая станция в сети, защищенной СЗИ от НСД «Блокхост-сеть 2.0». Если удаленная рабочая станция не зарегистрирована на сервере СЗИ, то доступ к ней будет запрещен. В том случае, если удаленная рабочая станция подключена к серверу СЗИ от НСД «Блокхост-сеть 2.0», то доступ к ней будет разрешен. Затем на удаленной рабочей станции будет произведено сравнение мандатных меток запрашиваемого объекта и субъекта, запрашивающего доступ к нему.

Схема работы мандатного механизма разграничения доступа на рабочих станциях-клиентах СЗИ «Блокхост-сеть 2.0» при доступе пользователей к сетевым ресурсам рабочих станций приведена на рисунках 6.35 – 6.37.

Рисунок 6.35. Результат попытки доступа к объекту для субъекта с меньшей мандатной меткой

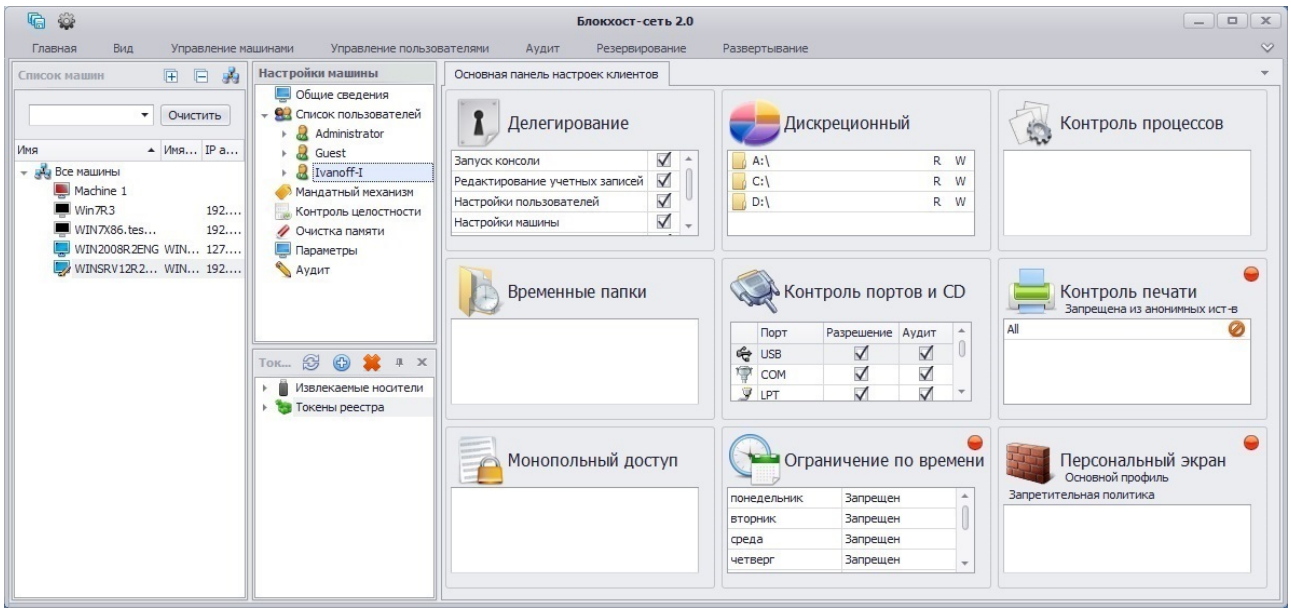
Рисунок 6.36. Результат попытки доступа к объекту для субъекта с равной мандатной меткой

Рисунок 6.37. Результат попытки доступа к объекту для субъекта с большей мандатной меткой

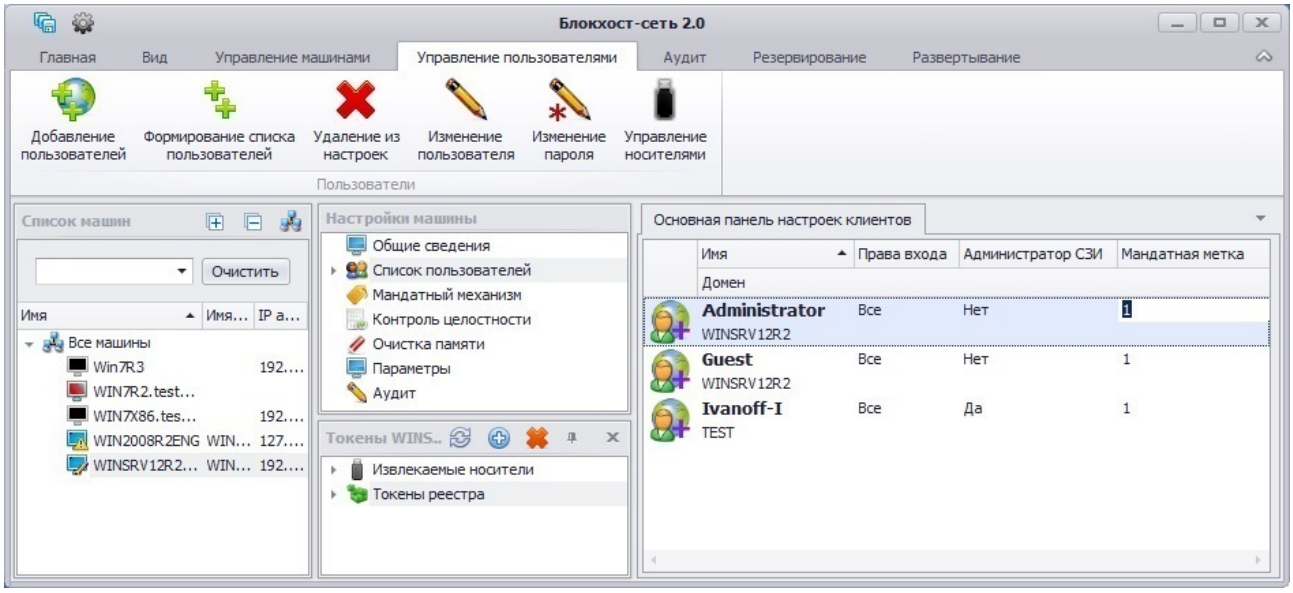
6.1.5.3. Установка и изменение мандатных меток пользователей

Для работы с конфиденциальными ресурсами пользователи должны иметь соответствующий уровень доступа, задаваемый числовым значением мандатной метки. Присвоение пользователю мандатной метки выполняется в следующей последовательности:

1. В окне **«Список машин»** консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для пользователя которой будет производиться изменение мандатной метки.
2. В окне **«Настройки машины»**, выбрать пункт ***Список пользователей*** или щелкнуть в **Основной панели настроек клиентов** по названию механизма ***Список пользователей*** (рис. 6.38, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.38, б).



а)



б)

Рисунок 6.38. Изменение мандатных меток пользователей

3. В **Основной панели настроек клиентов** выделить пользователя, для которого определяется (переопределяется) значение мандатной метки и выбрать пункт меню ***Управление пользователями→ Изменение пользователя***.
4. В открывшемся окне **«Изменение пользователя»** в поле ***Мандатная метка*** установить требуемое значение метки:

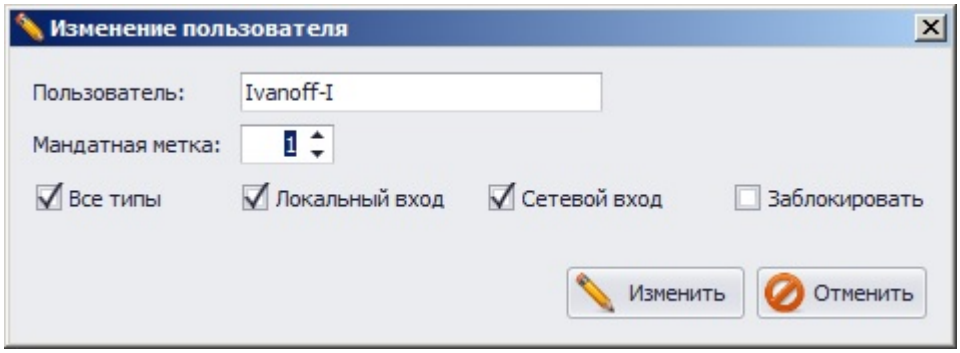


Рисунок 6.39. Диалоговое окно изменения пользователя

5. После нажатия кнопки ***Изменить*** данному пользователю будет поставлено в соответствие указанное в п. 4 значение мандатной метки. Нажатие кнопки ***Отменить*** вместо кнопки ***Изменить*** в окне **«Изменение пользователя»** позволит администратору безопасности выйти из окна без изменения параметров пользователя.
6. Изменить значение мандатной метки можно также и в **Основной панели настроек клиентов**. Для этого необходимо установить курсор в поле ***Мандатная метка*** выбранного пользователя и ввести необходимое значение мандатной метки (см. рис. 6.38, б).
7. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

По умолчанию всем пользователям при добавлении в список пользователей СЗИ присваивается мандатная метка со значением ***1***.

6.1.6. Временные папки

Некоторые приложения, например, такие как MS Word, Excel, входящие в пакет программ Microsoft Office, для улучшения быстродействия своей работы и с целью сохранности данных создают временные файлы. Для работы с такими временными файлами, приложениям, создавшим их, требуется полный доступ к каталогам, в которых эти файлы создаются. Если мандат вошедшего пользователя и метка каталога, в котором приложения создают временные файлы, будут отличаться, такие приложения не смогут полноценно работать.

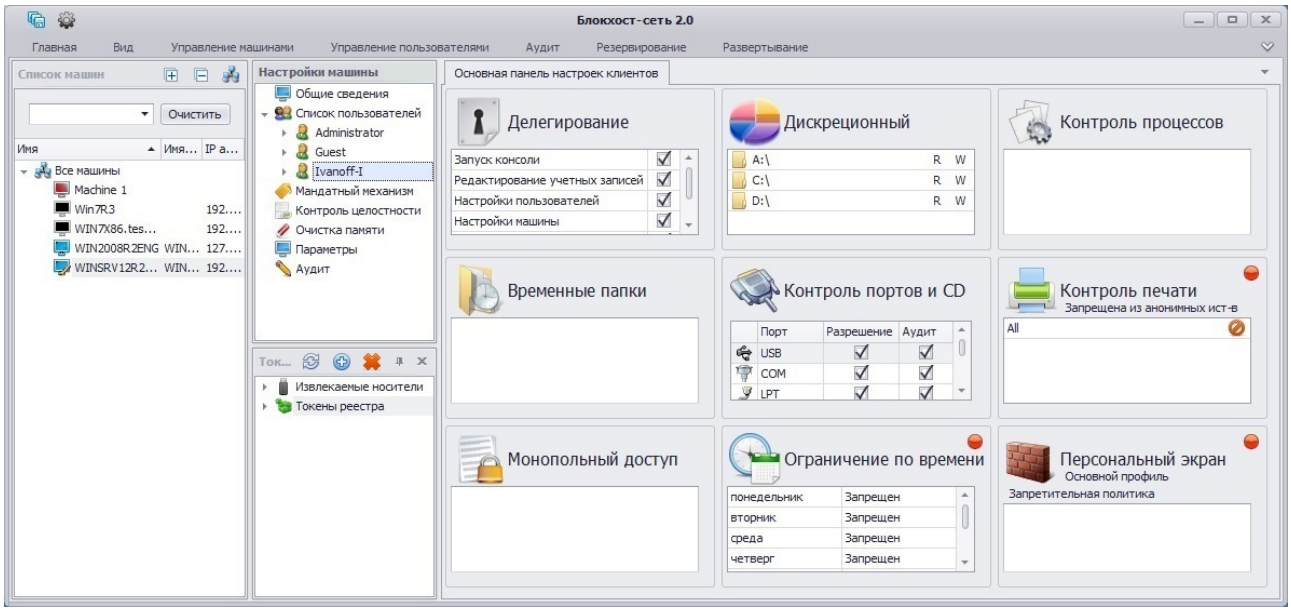
В СЗИ «Блокхост-сеть 2.0» существует возможность назначения **динамической мандатной метки**, равной мандату вошедшего пользователя, объектам файловой системы, определенным в СЗИ как ***Временные папки***. В результате такого назначения мандатных меток приложения получат полный доступ к этим папкам, независимо от метки родительского ресурса.

Следует иметь ввиду, что содержимое ***Временных папок*** затирается СЗИ «Блокхост-сеть 2.0» по завершению сеанса работы пользователя. Необходимо быть внимательным при настройке этого механизма, чтобы в процессе работы СЗИ не была удалена нужная информация.

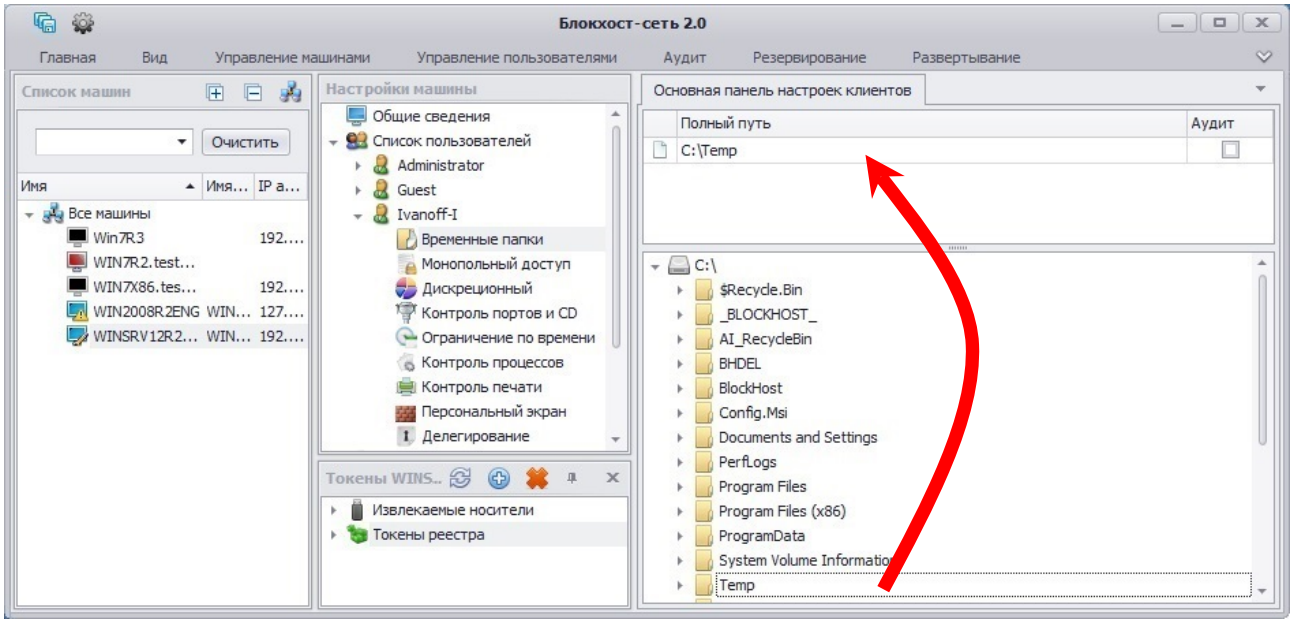
Настройка механизма ***Временных папок*** осуществляется индивидуально для каждого пользователя и выполняется в следующем порядке:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для пользователей которой будет производиться настройка механизма доступа к временным папкам.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Временные папки*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Временные папки*** (рис. 6.40, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.40, б)**.**

3. В **Основной панели настроек клиентов** добавить ресурсы на контроль, захватив и перетащив мышью необходимые объекты из дерева ресурсов рабочей станции (рис. 6.40, б).
4. Также можно настроить фиксацию событий доступа приложений к контролируемым объектам в журнал событий СЗИ «Блокхост-сеть 2.0», отметив параметр ***Аудит***, расположенный справа от выбранного каталога.



а)



б)

Рисунок 6.40. Настройка механизма временных папок

5. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Для определения каталогов, которые используются приложениями для работы с временными файлами, можно воспользоваться возможностями механизма СЗИ ***Мягкий режим***:

1. Включить механизм ***Мягкий режим*** на редактируемой рабочей станции (подробнее см. пункт 6.2.4 «Механизм мягкого режима» настоящего документа).
2. На контролируемой рабочей станции осуществляется вход в систему под учетной записью пользователя, для которого выполняется настройка механизма временных папок, с назначенной ему мандатной меткой.
3. Пользователь выполняет обычные операции на ПК (запуск приложений, работа с документами, доступ к локальным и сетевым ресурсам).
4. Затем в серверной консоли администрирования СЗИ администратору необходимо открыть журнал аудита контролируемой рабочей станции (пункт ***Аудит*** окна **«Настройки машины»**) и просмотреть все действия пользователя, начиная с момента его входа в систему. Подробности события можно увидеть, дважды щелкнув левой кнопкой мыши по строке события.
5. Обратить внимание на отраженные в журнале ошибки, связанные с доступом к тем или иным объектам (категория сообщения ***File Access***), и среди ошибок выделить каталоги, доступ приложений к которым был запрещен.
6. Затем в окне **«Настройки машины»** редактируемой рабочей станции, раскрыв пункт ***Список пользователей,*** двойным щелчком выбрать пользователя, для которого будет производиться настройка, и выделить пункт ***Временные папки***.
7. В **Основной панели настроек клиентов** добавить указанные ресурсы на контроль, захватив и перетащив мышью необходимые объекты из дерева ресурсов рабочей станции
8. Выключить ***Мягкий режим***.
9. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить,*** или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

6.1.7. Файлы монопольного доступа

Некоторые приложения в своей работе требуют монопольного режима доступа к файлам, с которыми они работают. В СЗИ «Блокхост-сеть 2.0» под файлами ***Монопольного доступа*** понимаются файлы, необходимые для работы таких приложений, в режиме полного доступа, независимо от мандата вошедшего пользователя. Указанным файлам присваивается **динамическая мандатная метка**, равная мандату вошедшего пользователя.

У приложения MS Word, из пакета Microsoft Office, такими файлами являются, например, для ОС Windows 7:
«C:\ProgramData\Microsoft\OFFICE\DATA\opa11.dat» (для MS Word 2003)
«C:\ProgramData\Microsoft\OFFICE\DATA\opa12.dat» (для MS Word 2007)
«C:\Users\<User_name>\AppData\Roaming\Microsoft\Templates\Normal.dotm» (для MS Word 2010).
В различных версиях Microsoft Office конечные пути и имена указанных файлов могут отличаться.

Для определения файлов монопольного доступа и последующего добавления их на контроль в СЗИ администратору безопасности необходимо выполнить следующие действия:

1. Включить механизм ***Мягкий режим*** на редактируемой рабочей станции (подробнее см. пункт 6.2.4 «Механизм мягкого режима» настоящего документа).

2. На контролируемой рабочей станции осуществляется вход в систему под учетной записью пользователя с назначенной мандатной меткой.
3. Пользователь выполняет обычные операции на ПК (запуск приложений, работа с документами, доступ к локальным и сетевым ресурсам).
4. Затем в серверной консоли администрирования СЗИ администратору безопасности необходимо открыть журнал аудита контролируемой рабочей станции (пункт ***Аудит*** окна **«Настройки машины»**) и просмотреть все действия пользователя, начиная с момента его входа в систему. Подробности события можно увидеть, дважды щелкнув левой кнопкой мыши по строке события.
5. Обратить внимание на отраженные в журнале ошибки, связанные с доступом к тем или иным объектам (категория сообщения ***File Access***), и среди ошибок выделить файлы, доступ приложений к которым был запрещен.
6. Затем в окне **«Настройки машины»** для редактируемой рабочей станции, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и выбрать пункт ***Монопольный доступ*** (рис. 6.41).
7. В **Основной панели настроек клиентов** добавить ресурсы на контроль, захватив и перетащив мышью необходимые объекты из дерева ресурсов рабочей станции.
8. Также можно настроить фиксацию событий доступа приложений к контролируемым объектам в журнал событий СЗИ «Блокхост-сеть 2.0», отметив параметр ***Аудит***, расположенный справа от выбранного файла.
9. Выключить **«Мягкий режим»**.
10. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

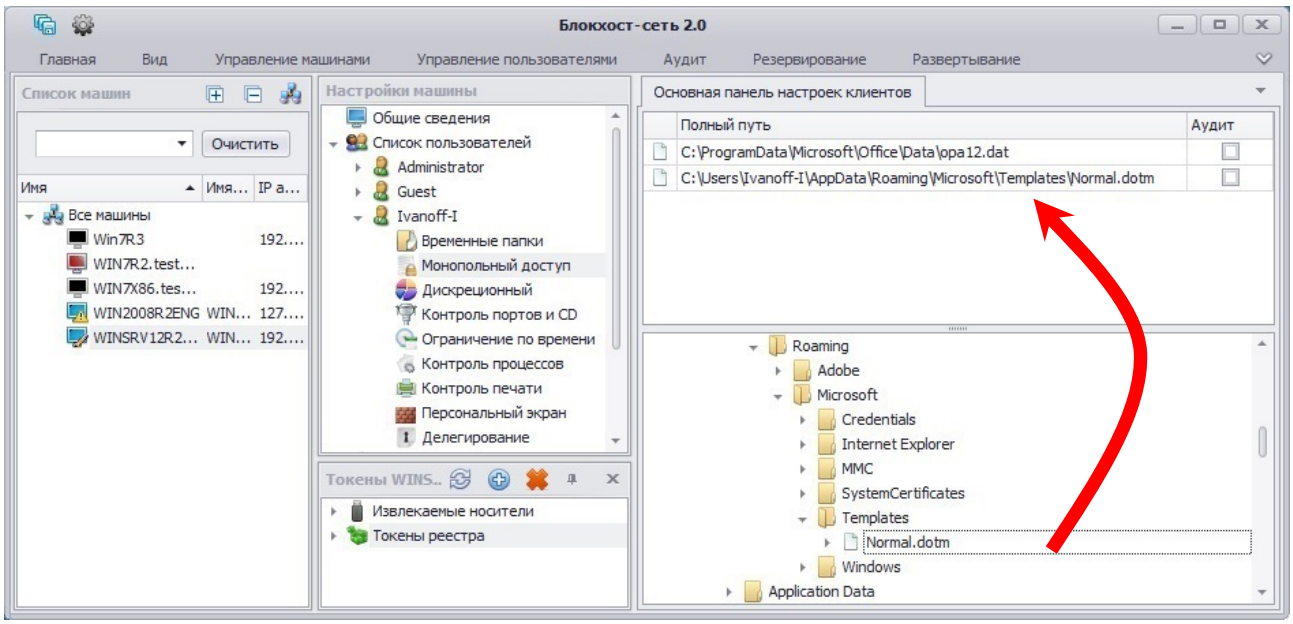


Рисунок 6.41. Выбор файлов для монопольного доступа

6.1.8. Разграничение доступа к администрированию СЗИ «Блокхост-сеть 2.0»

Для разделения функциональных обязанностей администратор безопасности может санкционировать администрирование СЗИ пользователями в полном объеме (в серверной или локальной консолях) или частично (в локальной консоли). Для этого необходимо воспользоваться механизмом разграничения доступа к администрированию СЗИ «Блокхост-сеть 2.0». Администратор безопасности из локальной консоли может делегировать выполнение следующих действий пользователей по администрированию СЗИ:

- запуск оболочки (доступ к консоли администрирования);
- управление учетными записями пользователей: добавление, удаление, изменение учетных записей пользователей, заведенных в СЗИ «Блокхост-сеть 2.0» (администрирование вкладки ***Пользователи*** локальной консоли администрирования);
- настройка дискреционного механизма разграничения доступа пользователей к объектам файловой системы (администрирование вкладки ***Дискреционный*** локальной консоли администрирования);
- настройка механизма разграничения доступа пользователей к отчуждаемым физическим носителям информации (администрирование вкладки ***Контроль портов и CD*** локальной консоли администрирования);
- настройка механизма разграничения доступа пользователей к запуску процессов (администрирование вкладки ***Контроль процессов*** локальной консоли администрирования);
- настройка механизма разграничения времени входа пользователей в систему (администрирование вкладки ***Временны́е ограничения*** локальной консоли администрирования);
- настройка временных папок (администрирование вкладки ***Вре́менные папки*** локальной консоли администрирования);
- настройка файлов монопольного доступа (администрирование вкладки ***Файлы монопольного доступа*** локальной консоли администрирования);
- настройка механизма разграничения доступа пользователей к сетевым ресурсам (администрирование вкладки ***Персональный экран*** локальной консоли администрирования);
- настройка механизма маркировки документов при печати (администрирование вкладки ***Контроль печати*** локальной консоли администрирования);
- управление идентификаторами входа (администрирование вкладки ***Идентификаторы входа*** локальной консоли администрирования);
- настройка механизма мандатного разграничение доступа к объектам файловой системы — сопоставление ресурсов файловой системы существующим меткам мандатного механизма (администрирование вкладки ***Мандатный механизм*** локальной консоли администрирования);
- настройка механизма контроля целостности (администрирование вкладки ***Контроль целостности*** локальной консоли администрирования);
- настройка механизма очистки памяти (администрирование вкладки ***Очистка памяти*** локальной консоли администрирования);

- настройка механизма регистрации событий (администрирование вкладки ***Аудит*** локальной консоли администрирования);
- настройка системных параметров удаленной рабочей станции: задание мягкого режима, загрузка настроек, настройка автовхода (администрирование вкладки ***Система*** локальной консоли администрирования).

Все действия администратора по изменению настроек механизма разграничения доступа пользователей к администрированию СЗИ фиксируются в журналах аудита рабочих станций, на которых происходит настройка этого механизма.

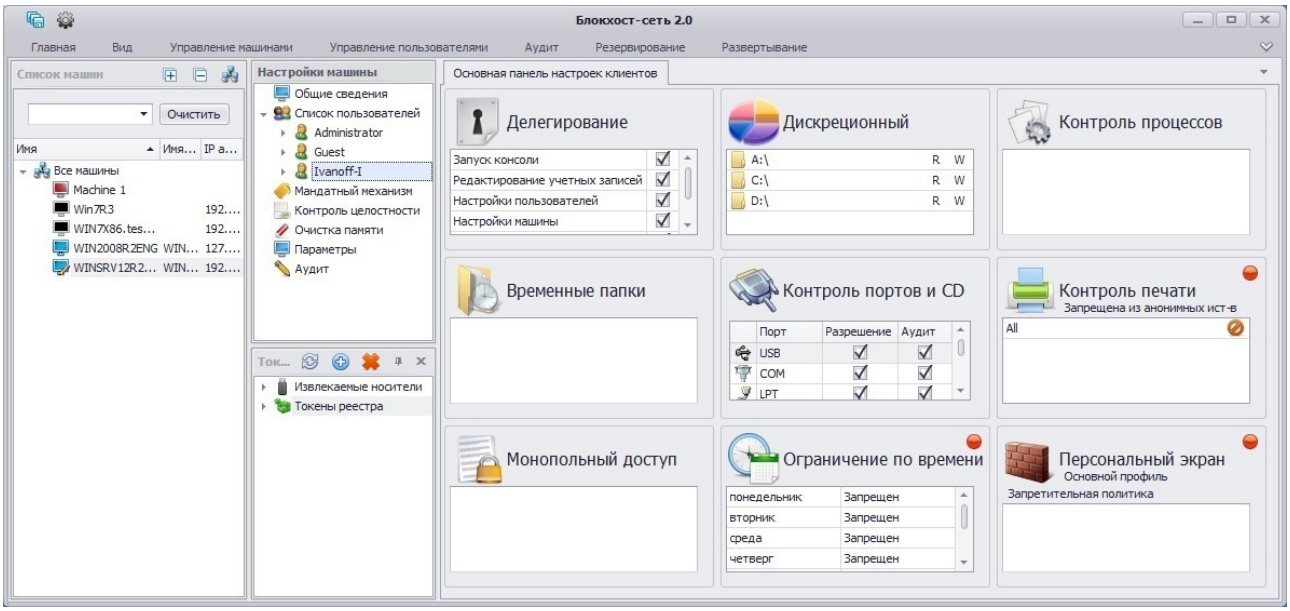
6.1.8.1. Порядок настройки механизма разграничения доступа к администрированию СЗИ «Блокхост-сеть 2.0»

Настройка механизма разграничения доступа пользователей к администрированию СЗИ различается для клиентских рабочих станций и сервера СЗИ.

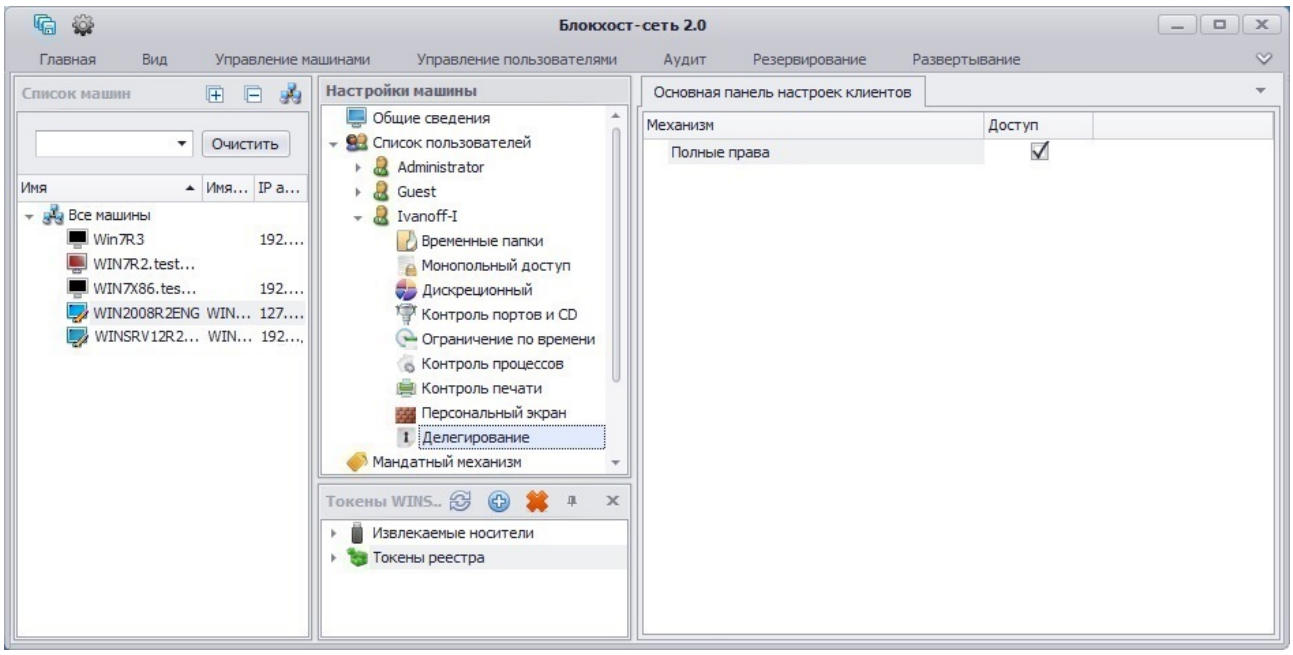
Для предоставления доступа пользователей к администрированию СЗИ «Блокхост-сеть 2.0» на сервере СЗИ администратору безопасности необходимо:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать сервер СЗИ.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Делегирование*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Делегирование*** (рис. 6.42, а). В обоих случаях в ***Основной панели настроек клиентов*** откроются настройки выбранного механизма (рис. 6.42, б).
3. В **Основной панели настроек клиентов** установить параметр ***Полные права***.
4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

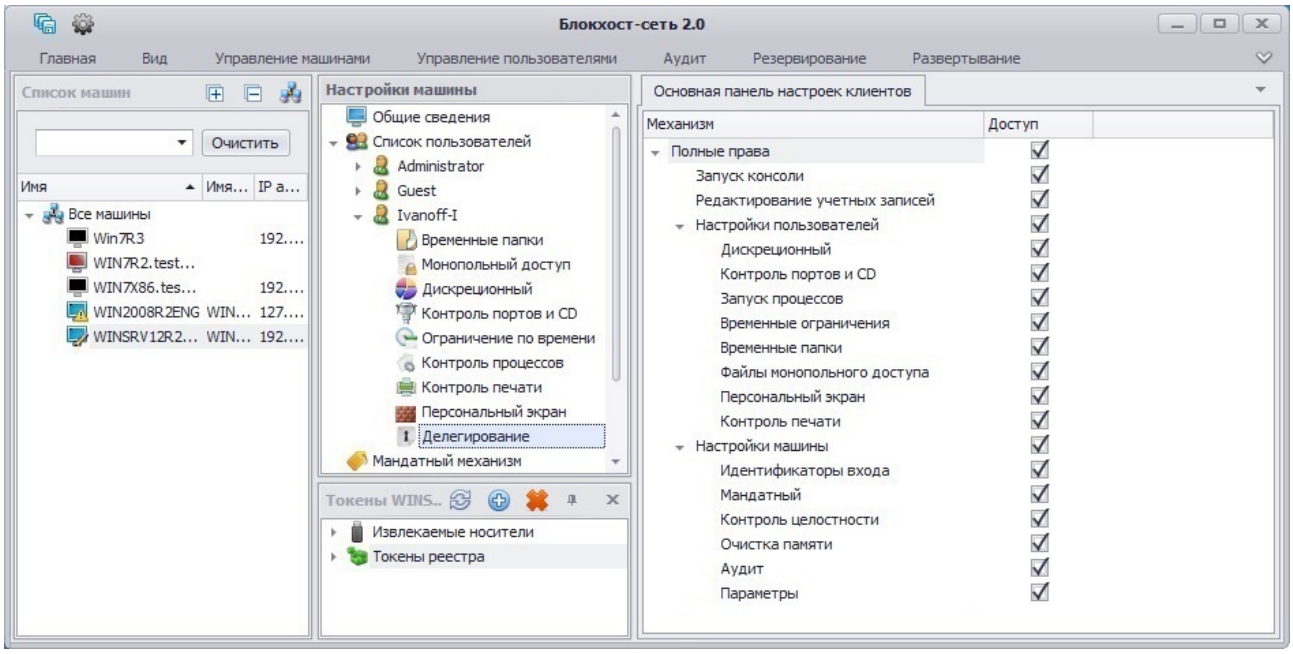
Разграничение доступа пользователей к администрированию отдельных механизмов СЗИ на сервере СЗИ возможно только из локальной консоли.



а)



б)



в)

Рисунок 6.42. Настройка полномочий администратора СЗИ

Для разграничения доступа к администрированию СЗИ «Блокхост-сеть К» на клиентских рабочих станциях администратору безопасности необходимо:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка разграничения доступа пользователей к администрированию СЗИ из локальной консоли.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Делегирование*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Делегирование*** (рис. 6.42, а). В обоих случаях в ***Основной панели настроек клиентов*** откроются настройки выбранного механизма (рис. 6.42, в).

3. В **Основной панели настроек клиентов** выбрать пункты, соответствующие санкционируемым действиям пользователя по администрированию механизмов СЗИ в локальной консоли рабочей станции.
4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

6.1.9. Разграничение доступа к сетевым ресурсам и фильтрация сетевого трафика

Персональный межсетевой экран в составе СЗИ «Блокхост-сеть 2.0» реализует:

- защиту ПК, функционирующего автономно или подключенного к ЛВС, от НСД к его ресурсам из внешних источников;
- разграничение доступа пользователя ПК к ресурсам сети;
- фильтрацию сетевого трафика.

Ограничение доступа пользователей ПК к сетевым ресурсам осуществляется на основе правил запретительной или разрешительной политики.

Согласно РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997 г.) в персональном межсетевом экране реализованы следующие возможности:

- фильтрация на сетевом уровне на основе сетевых адресов отправителя и получателя;
- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств (IGMP и ICMP протоколы);
- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов;
- возможность регистрации и учета фильтруемых пакетов.

Профиль персонального МЭ включает:

- *общие настройки профиля* (например, фильтрация по протоколам IGMP и ICMP, фильтрация по типам ICMP-протокола, регистрация запрещенных/разрешенных пакетов) – они не зависят от выбранного типа политики;
- *настройки правил фильтрации*, которые обеспечивают фильтрацию сетевого трафика в зависимости от вида выбранной политики (разрешительной или запретительной) и включают различные правила разграничения доступа к сетевым ресурсам и фильтрации сетевого трафика (IP-адрес и порт источника, IP-адрес и порт узла назначения, возможность фильтрации по интерфейсу рабочей станции, фильтрация по флагам TCP-протокола, фильтрация по TTL (времени жизни пакета), а также – признаки активности правила и регистрация в журнале аудита). IP-адреса и порты узлов могут задаваться перечислением или диапазоном. Фильтрация сетевого трафика осуществляется на уровне ядра ОС Windows. Механизм фильтрации трафика реализуется отдельным драйвером, взаимодействующим с интерфейсом АБ.

Разрешительная политика (работает по принципу «запрещено все, что явно не разрешено») реализуется на основе создания правил доступа к сетевым ресурсам, к которым

пользователю разрешен доступ. Доступ к остальным сетевым ресурсам, которые явно не указаны в правилах доступа, будет запрещен.

Запретительная политика (работает по принципу «разрешено все, что явно не запрещено») реализуется на основе создания правил доступа к сетевым ресурсам, к которым пользователю доступ запрещен. Доступ к остальным сетевым ресурсам, которые явно не указаны в правилах доступа, будет разрешен.

В персональном экране предусмотрена возможность регистрации всех пакетов для каждого пользователя. В зависимости от настроек персонального экрана может производиться аудит каждого правила, а также – регистрация прохождения неразрешенных и незапрещенных пакетов.

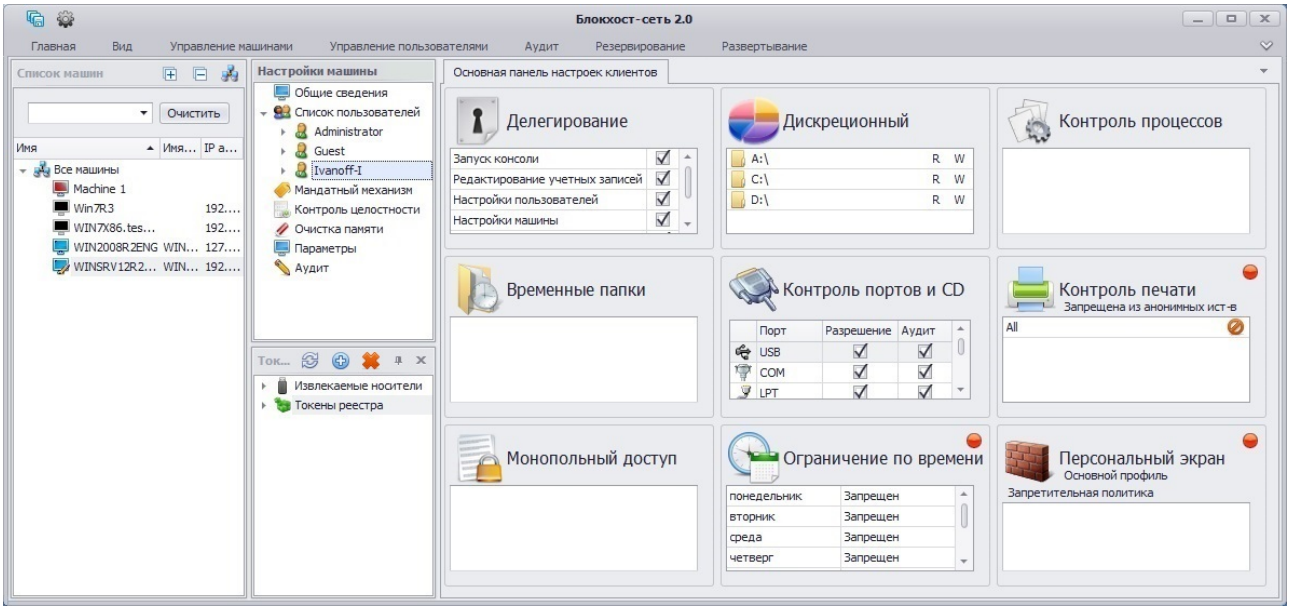
Установленные правила разграничения доступа и фильтрации трафика активны, когда на соответствующем ПК в ОС зашел пользователь, для которого они были заданы.

6.1.9.1. Порядок настройки персонального межсетевого экрана

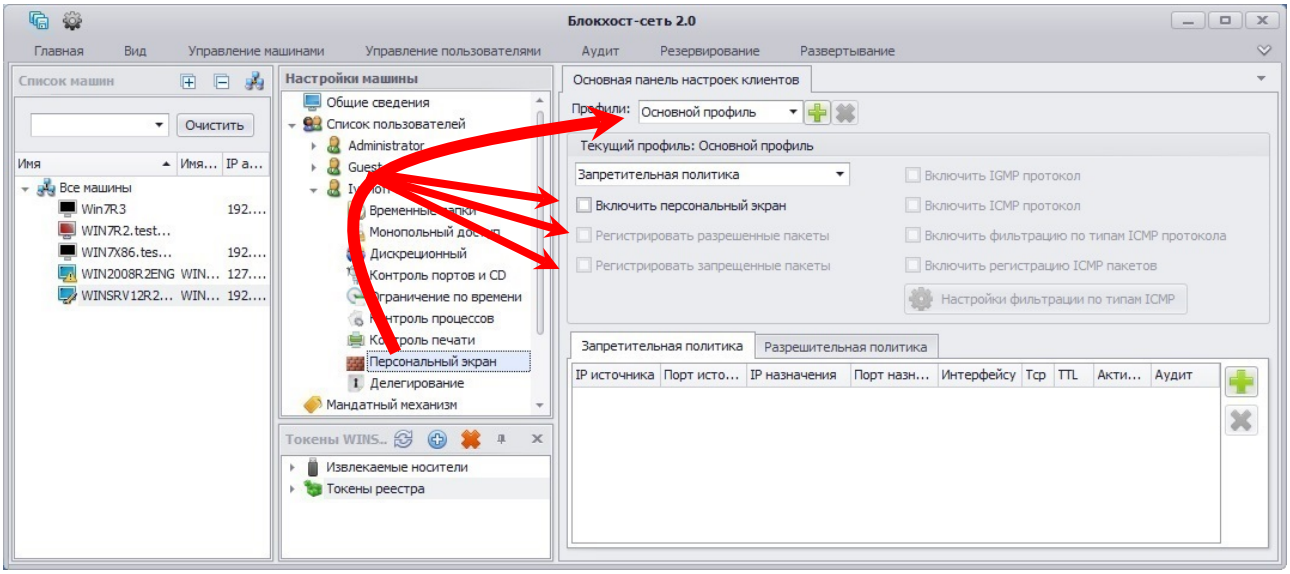
Настройка персонального МЭ заключается в создании одного или нескольких профилей для пользователя ПК. Каждый профиль МЭ включает в себя *общие настройки* профиля, применяемые независимо от типа выбранной политики, *и настройки правил* фильтрации, которые обеспечивают фильтрацию сетевого трафика в зависимости от вида выбранной политики – разрешительной или запретительной.

Для настройки персонального МЭ администратору безопасности необходимо осуществить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка персонального межсетевого экрана.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Персональный экран*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Персональный экран*** (рис. 6.43, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.43, б).



а)



б)

Рисунок 6.43. Настройка персонального межсетевого экрана

3. В области настроек задать *общие настройки профиля персонального МЭ* (рис. 6.43, б):
   - «*Наименование профиля*». Необходимо добавить профиль персонального МЭ (для выбранного пользователя может быть создан один или несколько профилей). Для этого необходимо нажать кнопку ***Добавить***  , находящуюся правее поля ***Профили***, в открывшемся окне **«Добавить профиль»** (рис. 6.44) ввести имя профиля и нажать кнопку ***Добавить*** (по умолчанию в системе создан пустой профиль с именем *Основной профиль*, который также может использоваться при создании правил фильтрации сетевого трафика). Для удаления созданного профиля следует выбрать его в выпадающем списке поля ***Профили*** и нажать кнопку ***Удалить***  (рис. 6.43, б). Нельзя удалить единственный существующий профиль;

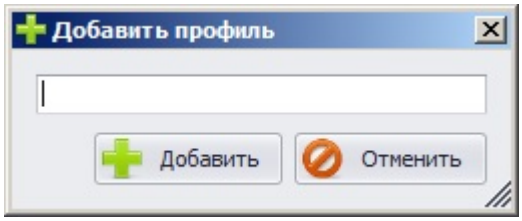


Рисунок 6.44. Окно создания профиля персонального экрана

   - из выпадающего списка выбрать тип политики, согласно которой для данного профиля будет осуществляться контроль доступа к сетевым ресурсам. Возможные варианты: ***Разрешительная политика*** или ***Запретительная политика***;
   - для активации персонального МЭ (применения созданных настроек профиля персонального МЭ после входа пользователя в ОС) необходимо отметить пункт ***Включить персональный экран***;

При включении персонального МЭ, после входа соответствующего пользователя в ОС Windows XP иконка персонального экрана в области уведомлений изменит вид с  на  .

- для регистрации всех событий, связанных с доступом пользователя к разрешенным сетевым ресурсам, необходимо включить опцию ***Регистрировать разрешенные пакеты***;
- для регистрации всех событий, связанных с доступом пользователя к запрещенным сетевым ресурсам, необходимо включить опцию ***Регистрировать запрещенные пакеты***;
- при необходимости фильтрации сетевых пакетов по протоколу IGMP установить опцию ***Включить IGMP протокол***;
- при необходимости фильтрации сетевых пакетов по протоколу ICMP установить опцию ***Включить ICMP протокол***. После выбора этого пункта станут активными пункты ***Включить фильтрацию по типам ICMP протокола***, ***Включить регистрацию ICMP пакетов*** и кнопка ***Настройки фильтрации по типам ICMP***, при нажатии на которую появится окно выбора настроек ICMP (рис. 6.45);
- при необходимости включить фильтрацию по типам ICMP-пакетов, выбрать опцию ***Включить фильтрацию по типам ICMP протокола***. Фильтрация осуществляется в соответствии с параметрами заданными в окне **«Настройки ICMP»** (рис. 6.45);
- при необходимости можно регистрировать в журнале аудита типы фильтруемых ICMP-пакетов, выбрав в области настроек опцию ***Включить регистрацию ICMP пакетов*** (рис. 6.43, б).

Перечисленные выше настройки являются общими для редактируемого профиля персонального МЭ и не зависят от типа выбранной политики.

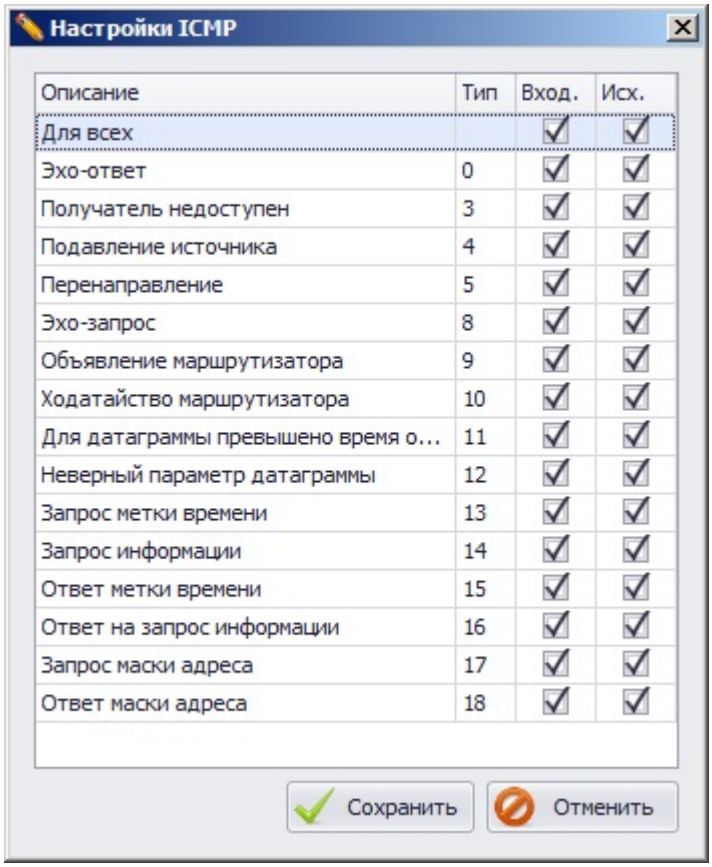


Рисунок 6.45. Настройка фильтрации по типам ICMP-протокола

Настройка разрешительной политики

Разрешительная политика может содержать одно или несколько правил фильтрации сетевого трафика. К прохождению будут разрешены только пакеты соответствующие установленным правилам фильтрации сетевого трафика. Для настройки разрешительной политики следует:

1. В **Основной панели настроек клиентов** выбрать пункт выпадающего списка ***Разрешительная политика***.
2. Для добавления правила разрешительной политики нажать на кнопку ***Добавить***  , находящуюся справа в области создания правил.
3. В открывшемся окне **«Настройки правила»** указать параметры разрешающего правила доступа к сетевым ресурсам и фильтрации сетевого трафика:

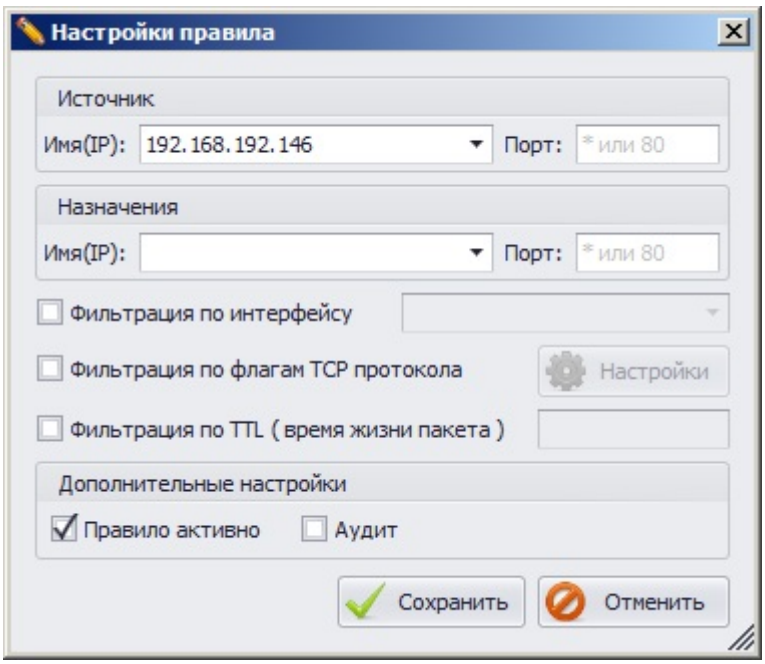


Рисунок 6.46. Окно добавления правила в политику

Возможные настройки в окне **«Настройки правила»**:

- *Источник.* Введенные параметры позволяют активировать фильтрацию по IP-адресу и номеру порта отправителя. Поля ***Имя*** и ***Порт*** не могут быть пустыми.
- *Назначения*. Введенные параметры позволяют активировать фильтрацию по IP-адресу и номеру порта получателя. Поля ***Имя*** и ***Порт*** не могут быть пустыми.

> При указании имен узлов фильтрации не следует использовать DNS-имена рабочих станций. В поля ***Имя(IP)*** *Источника* и *Назначения* можно вводить маску подсети в формате `1.1.1.1/1`, а также диапазон, например `192.168.0.5-25`. Ввод символа <*> в поле ***Порт*** будет обозначать выбор всех портов.

- *Фильтрация по интерфейсу*. Параметр позволяет указать сетевой интерфейс редактируемой рабочей станции, по которому должна производиться фильтрация сетевого трафика при выполнении данного правила.

> Данный параметр предполагает фильтрацию по IP-адресу выбранного сетевого подключения – при изменении IP-адреса сетевого адаптера (например, при использовании в локальной сети сервера DHCP) правило будет по-прежнему осуществлять фильтрацию по IP-адресу, присвоенному сетевому адаптеру в момент создания правила.

- *Фильтрация по флагам TCP протокола.* Параметр позволяет активировать фильтрацию TCP-пакетов по типам флагов TCP протокола. При выборе этого параметра станет активной кнопка ***Настройки***, нажатие на которую открывает окно **«Настройки фильтрации TCP пакетов»**, в котором следует отметить необходимые флаги TCP-пакетов (рис. 6.47).
- *Фильтрация по TTL (время жизни пакета).* Выбор данного параметра позволяет осуществлять фильтрацию пакетов по их времени жизни (TTL). К прохождению будут разрешены TCP-пакеты, время жизни (TTL) которых равно введенному в соответствующее поле окна **«Настройки правила»** значению. Прохождение остальных TCP-пакетов будет заблокировано.

- *Дополнительные настройки:*
  1) *Правило активно***.** Параметр предназначен для применения (активации) сохраненных администратором настроек правила персонального МЭ при входе пользователя в систему.
  2) *Аудит.* При необходимости регистрации событий, относящихся к данному правилу, следует отметить этот параметр.

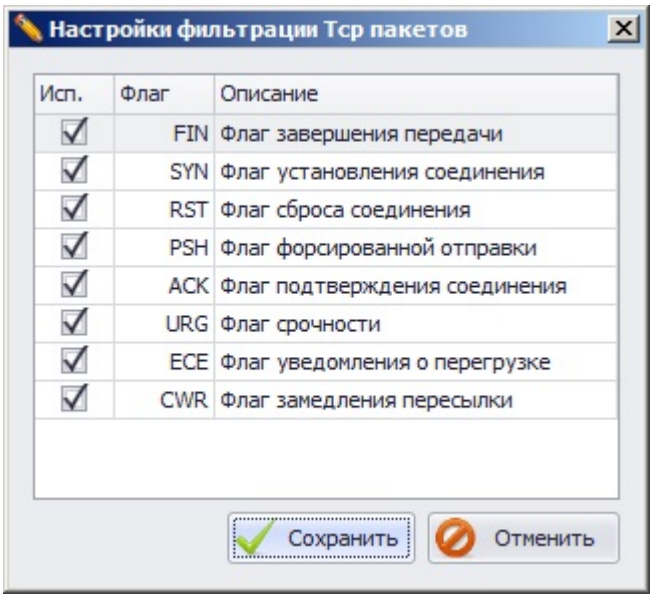


Рисунок 6.47. Выбор настроек TCP

4. Для сохранения созданного правила следует в окне **«Настройки правила»** нажать кнопку ***Сохранить***. В области создания правил появится два правила фильтрации (рис. 6.48) – одно созданное администратором и второе, созданное автоматически, в котором значения параметров *Источника* и *Назначения* установлены так, чтобы было возможно обратное прохождение сетевых пакетов через МЭ. В случае отсутствия необходимости в обратном прохождении сетевых пакетов, созданное автоматически правило можно удалить.
5. Для создания еще одного правила фильтрации сетевого трафика следует повторить п.п. 2 – 4 данного подраздела. Нажатие на кнопку ***Отменить*** в окне **«Настройки правила»** приведет к выходу из окна без добавления правил фильтрации.
6. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

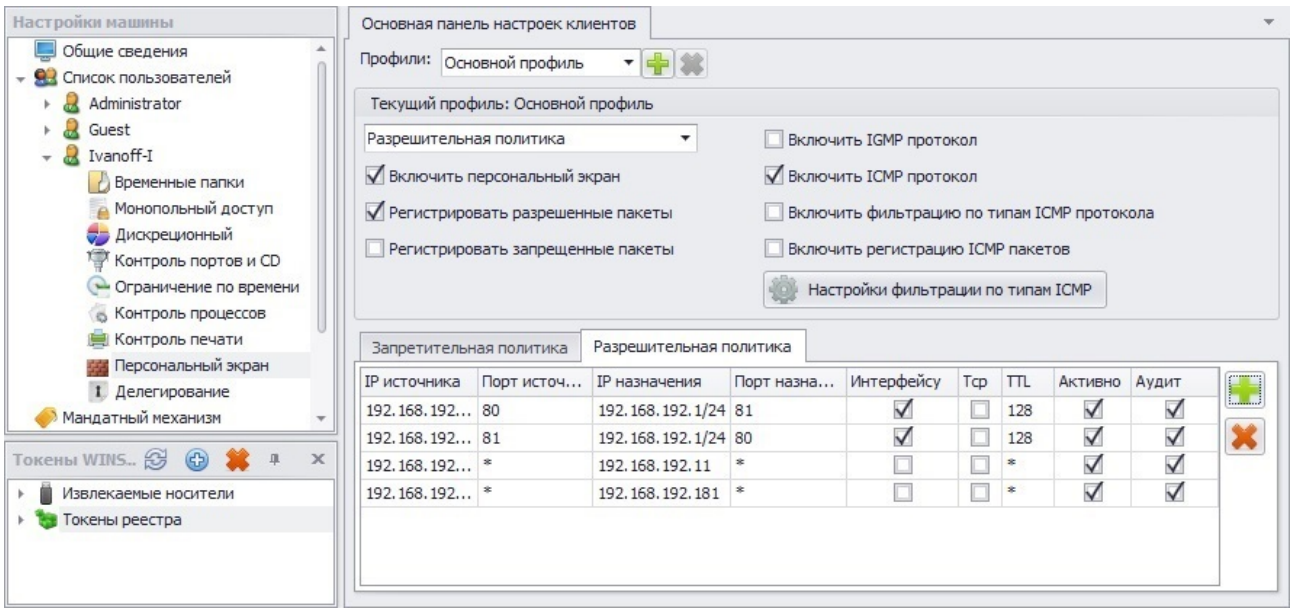


Рисунок 6.48. Настройка разрешительной политики

Для изменения существующих правил фильтрации сетевого трафика следует выбрать необходимое правило из списка и дважды щелкнуть по нему левой кнопкой мыши. В открывшемся окне **«Настройки правила»** можно изменить параметры, описанные в пункте 3 данного подраздела.

Для удаления существующего правила фильтрации сетевого трафика достаточно выделить в области настроек требуемое правило (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить сразу несколько правил) и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Удалить*** , находящейся справа в области создания правил).

При использовании ***Разрешительной политики*** на редактируемой рабочей станции к прохождению будут разрешены только пакеты соответствующие установленным правилам фильтрации сетевого трафика.

Настройка запретительной политики

Настройка запретительной политики производится аналогично настройке разрешительной политики, с той лишь разницей, что создаваемые правила будут запрещать пользователю доступ к сетевым ресурсам и осуществлять фильтрацию указанного сетевого трафика. К прохождению будут запрещены только пакеты соответствующие установленным правилам фильтрации сетевого трафика.

Подробно описание работы с персональным МЭ приведено в документе «СЗИ «Блокхост-сеть 2.0». Персональный межсетевой экран. Руководство администратора безопасности».

6.1.10. Механизм контроля печати

Механизм контроля печати предназначен для решения следующих задач:

- контроль процесса печати документов из любых приложений;
- определение пользователя, домена (которому принадлежит пользователь), а также процесса, из которого производится печать;
- внесение дополнительных полей в распечатываемый документ (верхний и нижний колонтитул, изображения);

- ведение аудита процесса печати на контролируемой рабочей станции.

Список приложений, с использованием которых пользователю разрешен или запрещен вывод документов на печать, а также необходимость регистрации событий, связанных с процессом печати, определяется политикой безопасности и задается администратором безопасности в консоли администрирования СЗИ «Блокхост-сеть 2.0».

Механизм контроля печати СЗИ «Блокхост-сеть 2.0» поддерживает три режима работы:

1. **Режим базового аудита печати** – осуществляется регистрация печати документов с указанием даты и времени совершенной печати, имени принтера, имени пользователя, наименования рабочей станции, размера документа, количества страниц, наименования и метки распечатанного документа.

2. **Режим аудита и разграничения доступа к приложениям** – осуществляется регистрация печати документов с указанием даты и времени совершенной печати, имени принтера, имени пользователя, наименования рабочей станции, имени приложения из которого производилась печать, размера документа, количества страниц, наименования и метки распечатанного документа. А также осуществляется разграничение возможности печати из контролируемых приложений.

3. **Режим маркировки документов** – осуществляется автоматическая маркировка каждого листа (страницы) документа при его печати. Происходит регистрация печати документов с указанием даты и времени совершенной печати, имени принтера, имени пользователя, наименования рабочей станции, имени приложения из которого производилась печать, размера документа, количества страниц, наименования и метки распечатанного документа, а также осуществляется разграничение возможности печати из контролируемых приложений.

6.1.10.1. Режим базового аудита печати

6.1.10.1.1. Ограничения использования режима базового аудита печати

СЗИ «Блокхост-сеть 2.0» при работе механизма контроля печати в режиме базового аудита печати имеет следующие ограничения:

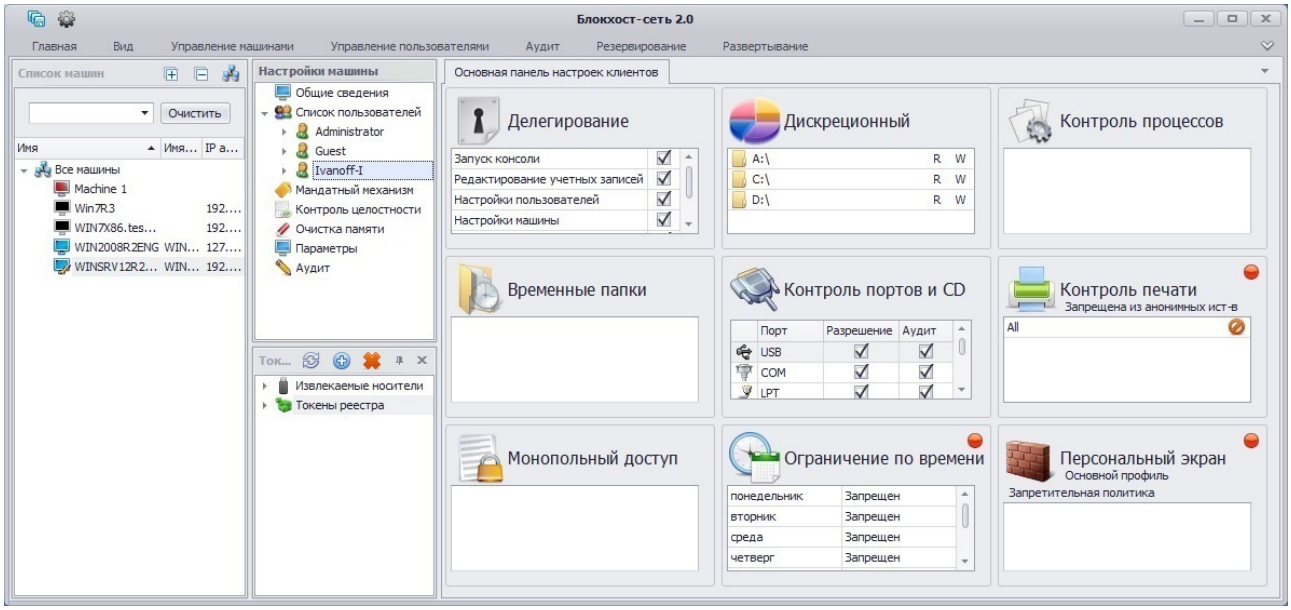
1) не ведется аудит печати на принтерах общего доступа (локальных принтерах рабочих станций, доступ к которым предоставлен пользователям сети).

6.1.10.1.2. Настройка СЗИ в режиме базового аудита печати

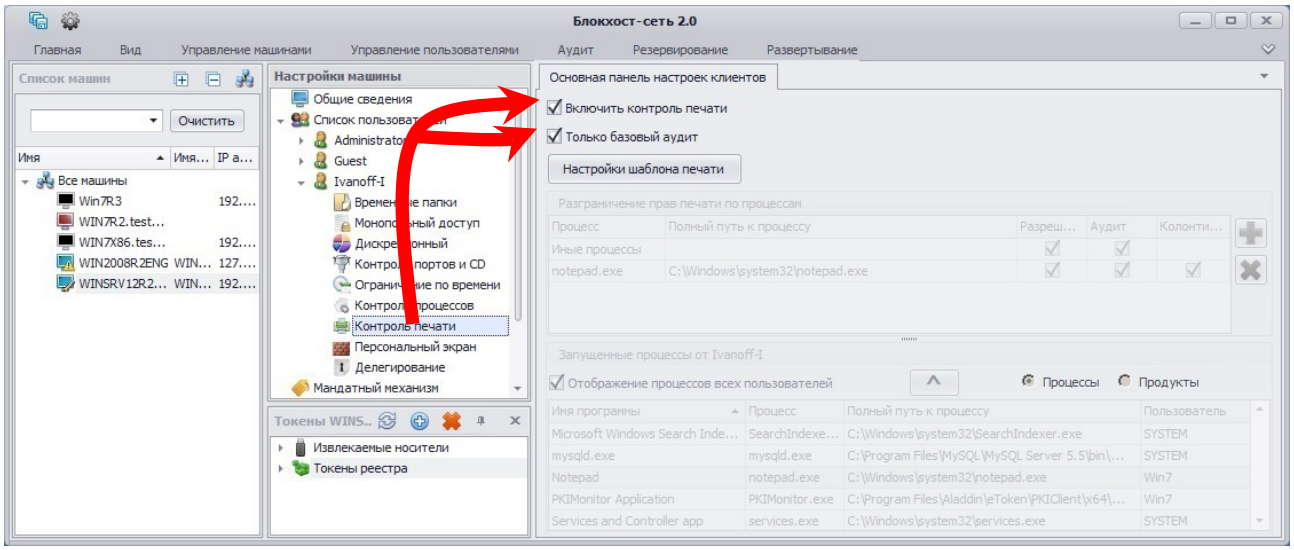
В настройках механизма контроля печати СЗИ «Блокхост-сеть 2.0» есть возможность включить только аудит событий связанных с печатью документов, не запрещая пользователю саму возможность печати. Для того чтобы включить только аудит печати администратору безопасности необходимо осуществить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля печати.
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Контроль печати*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Контроль печати*** (рис. 6.49, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.49, б).

3. В **Основной панели настроек клиентов** включить механизм контроля печати, выбрав пункт ***Включить контроль печати*** и отметить параметр ***Только базовый аудит*** (рис. 6.49, б).
4. Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.



а)



б)

Рисунок 6.49. Включение режима базового аудита печати

При включении параметра ***Только базовый аудит*** никакие настройки, кроме настройки шаблона печати, будут недоступны для редактирования (см. рис. 6.49, б). При такой настройке механизма контроля печати СЗИ пользователь будет иметь возможность печати всех возможных документов из любого приложения. При этом информация об успешно произведенной печати будет заноситься в журнал аудита СЗИ. Подробнее о настройке механизма контроля печати в режиме разграничения доступа к приложениям см. пункт 6.1.10.2.2 настоящего документа.

6.1.10.1.3. Особенности работы СЗИ в режиме базового аудита печати

1) Если в окне **«Редактирование настроек шаблона печати»** включены какие либо опции, они будут применены ко всем распечатываемым документам из любых приложений (Подробнее о настройке механизма маркировки документов см. п. 6.1.10.3.2 настоящего документа).

2) Внимание пользователей принтеров Hewlett-Packard: При установленной опции ***Только базовый аудит*** для возможности наложения штампов в распечатываемый документ, необходимо чтобы в системе был установлен стандартный драйвер принтера, который устанавливается через опцию ***Добавить принтер*** в апплете панели управления ОС Windows **Устройства и принтеры**. В том случае, если установлен универсальный драйвер принтера HP, маркировка документов в режиме базового аудита выполняться не будет.

6.1.10.2. Режим аудита печати и разграничения доступа к приложениям

6.1.10.2.1. Ограничения использования режима аудита печати и разграничения доступа к приложениям

СЗИ «Блокхост-сеть 2.0» при работе механизма контроля печати в режиме аудита печати и разграничения доступа к приложениям имеет следующие ограничения:

1) запрещается включение механизма контроля печати СЗИ на рабочих станциях с установленным DLP-агентом Symantec Data Loss Prevention – при включении механизма контроля печати происходит аварийное завершение процесса explorer.exe;

2) для устойчивого функционирования АРМ с установленным СКЗИ «КриптоПро CSP» версия сборки СКЗИ должна быть 3.9.8293 или 4.0.9589 (Gauss) и выше;

3) поддерживается работа с печатающими устройствами, для которых установлены драйвера поддержки PCL (работа механизма контроля печати с печатающими устройствами, для которых установлены драйвера поддержки PostScript не гарантируется – возможность печати на подобных устройствах может быть заблокирована);

4) в семействе Windows 8/8.1 не поддерживается работа с приложениями, использующими metro-интерфейс;

5) блокируется возможность печати из браузера Mozilla Firefox;

6) блокируется возможность печати содержимого страницы браузера Internet Explorer (версия 11) при включенном контроле учетных записей (UAC).

6.1.10.2.2. Настройка СЗИ в режиме аудита печати и разграничения доступа к приложениям

Для настройки СЗИ в режиме аудита печати и разграничения документов администратору безопасности необходимо осуществить следующие действия:

5. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля печати.
6. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей,*** двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Контроль печати*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Контроль печати*** (рис. 6.49, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.49, б).

7. В **Основной панели настроек клиентов** включить механизм контроля печати, выбрав пункт ***Включить контроль печати*** (рис. 6.50).

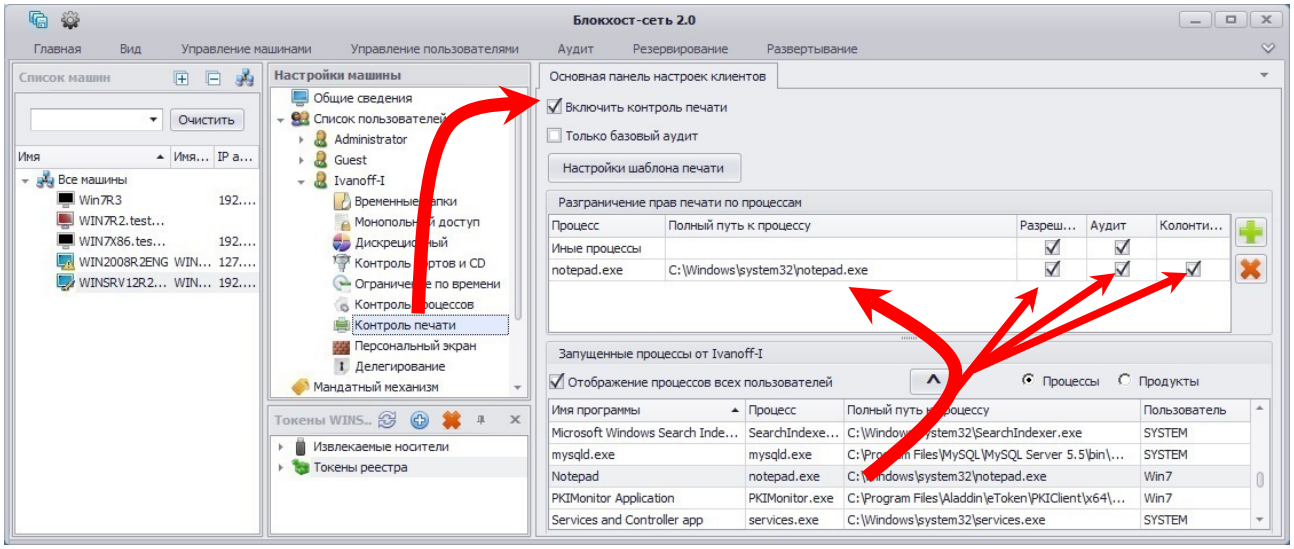


Рисунок 6.50. Настройка механизма контроля печати

8. В **Основной панели настроек клиентов** добавить на контроль объекты, захватив и перетащив мышью из списка запущенных процессов в область *Разграничение прав печати по процессам* необходимые процессы. Также необходимые процессы в область *Разграничение прав печати по процессам* можно добавить, выделив их в списке запущенных процессов (для выделения нескольких процессов можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и нажав кнопку  , расположенную над списком запущенных процессов. Для добавления процесса на контроль, если он не запущен в настоящее время, необходимо воспользоваться кнопкой ***Добавить***  , после нажатия на которую откроется окно **«Выбор»** (рис. 6.51). В окне **«Выбор»** необходимо раскрыть структуру каталогов контролируемого компьютера, выбрать исполняемый файл и нажать кнопку ***Добавить***.

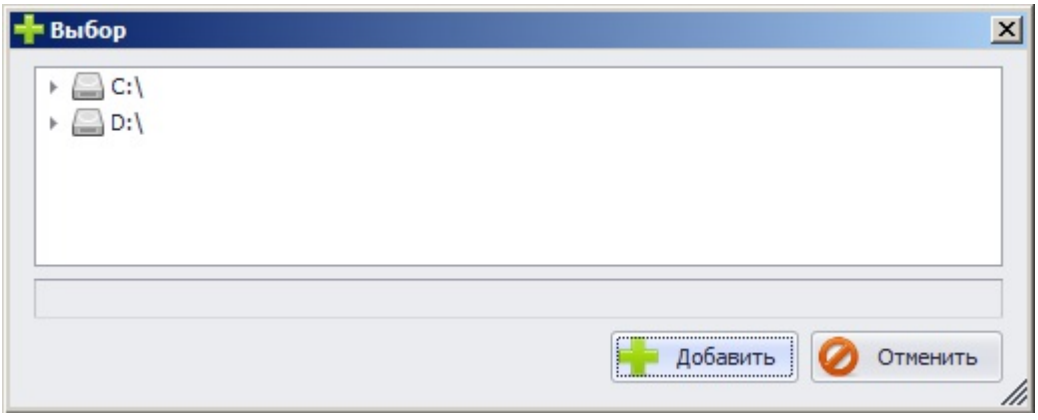


Рисунок 6.51. Окно выбора файлов.

Элемент *Иные процессы* в области *Разграничение прав печати по процессам* означает все процессы ПК, для которых может происходить контроль печати (а не только запущенные в данный момент). По умолчанию этот элемент уже добавлен на контроль с установленными параметрами ***Разрешение*** и ***Аудит***. Удалить его из списка контролируемых объектов невозможно.

Переключатель ***Процессы↔Продукты*** позволяет отображать в области *Запущенные процессы* либо список запущенных на рабочей станции процессов (переключатель установлен в положение ***Процессы***), либо список всех исполняемых файлов из перечня установленного на рабочей станции ПО, которое поддерживается механизмом контроля печати (переключатель установлен в положение ***Продукты***).

Процесс, поставленный на контроль, не пропадает из списка запущенных процессов (списка продуктов), однако строка, соответствующая контролируемому процессу, изменяет свой цвет с черного на серый. Повторное добавление процесса на контроль – невозможно.

При настройке механизма контроля печати для пользователя, который не вошел в ОС на контролируемой рабочей станции, список запущенных процессов будет пустой (переключатель ***Процессы↔Продукты*** установлен в положение ***Процессы***). Для отображения списка всех запущенных процессов необходимо установить параметр ***Отображение процессов всех пользователей***.

9. Для того чтобы разрешить приложению вывод на печать, необходимо отметить поле ***Разрешение***, расположенное справа от выбранного объекта. Для того чтобы запретить приложению вывод на печать, необходимо снять отметку с поля ***Разрешение*** или не отмечать его. По умолчанию, при добавлении процесса (приложения) на контроль, параметры ***Разрешение*** и ***Аудит*** установлены.
10. Для сохранения событий печати из контролируемого приложения в журнал СЗИ «Блокхост-сеть 2.0» необходимо в области *Разграничение прав печати по процессам* отметить поле ***Аудит***, расположенное справа от выбранного объекта (рис. 6.50).
11. Для удаления процесса из списка контролируемых достаточно выделить в области *Разграничение прав печати по процессам* требуемый процесс (для выделения нескольких процессов можно воспользоваться клавишами **<Ctrl>** или **<Shift>**) и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Удалить***  , расположенной справа от списка контролируемых процессов).
12. Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

6.1.10.2.3. Особенности настройки СЗИ в режиме аудита печати и разграничения доступа к приложениям

Печать с использованием принтеров общего доступа

В работе механизма контроля печати с использованием принтеров общего доступа (локальных принтеров рабочих станций, доступ к которым предоставлен пользователям сети) имеются особенности:

Корректная печать из контролируемого приложения (процесса) возможна, только если установлены оба параметра ***Разрешение*** и ***Колонтитулы***.

В остальных случаях распечатать документ на принтере общего доступа будет невозможно.

6.1.10.3. Режим маркировки документов при печати

6.1.10.3.1. Ограничения использования режима маркировки документов при печати

СЗИ «Блокхост-сеть 2.0» при работе механизма контроля печати в режиме маркировки документов при печати имеет следующие ограничения

1) все ограничения, перечисленные при работе механизма контроля печати СЗИ в режиме аудита и разграничения доступа к приложениям (см. п. 6.1.10.2.1 настоящего документа), за исключением печати на принтерах общего доступа (печать на принтерах общего доступа при установке параметров ***Разрешение*** и ***Колонтитулы*** возможна);

2) печать цветного текста и/или изображения происходит в черно-белом варианте.

6.1.10.3.2. Настройка механизма маркировки документов

В СЗИ «Блокхост-сеть 2.0» реализована возможность выборочного назначения маркировки документов при печати для разных приложений. Для настройки механизма контроля печати с маркировкой распечатываемого документа из контролируемого приложения администратору безопасности необходимо выполнить следующие действия в серверной консоли администрирования:

1. Последовательно выполнить пункты 1 – 6 пункта 6.1.10.2.2 настоящего документа.
2. Для отображения колонтитулов на документе, распечатываемом из контролируемого приложения, необходимо отметить поле ***Колонтитулы***, расположенное справа от выбранного приложения (см. рис. 6.50, б).
3. Для настройки содержимого колонтитулов, выводимых при печати документа из контролируемого приложения, необходимо в **Основной панели настроек клиентов** нажать кнопку ***Настройки шаблона печати***.
4. В открывшемся окне **«Редактирование настроек шаблона печати»** (рис. 6.52) следует выбрать необходимые маркеры (отметив соответствующие поля) и определить их содержание. Список маркеров и их описание указан ниже.

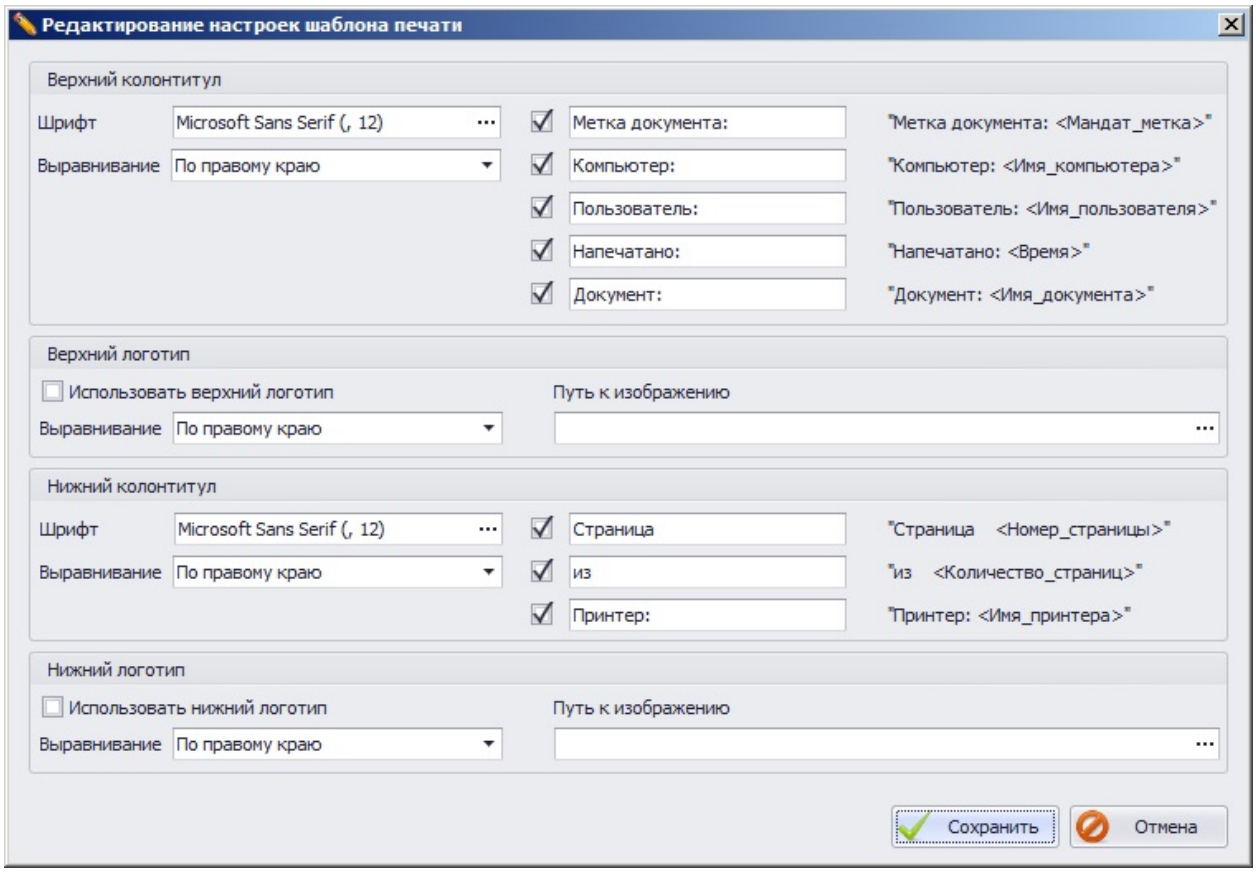


Рисунок 6.52. Настройки шаблона печати

5. После окончания настройки шаблона печати следует нажать кнопку ***Сохранить*** в окне **«Редактирование настроек шаблона печати»**.
6. Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

В результате произведенных настроек механизма контроля печати СЗИ, в том числе и шаблона печати, при печати документ будет выглядеть следующим образом (рис. 6.53).

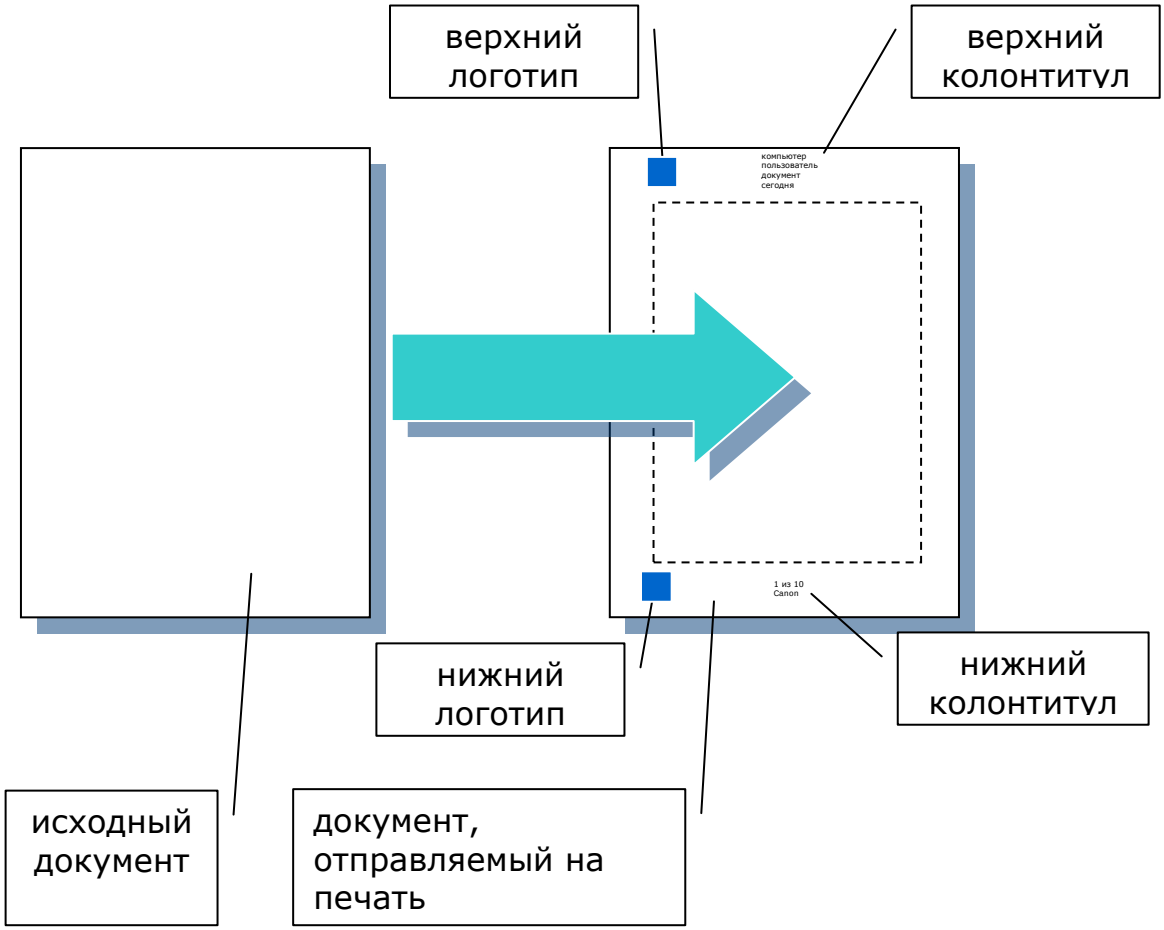


Рисунок 6.53. Результат применения шаблона печати

Список маркеров шаблона печати и их описание:

- **Верхний колонтитул.**
  - ***Шрифт***. Для выбора шрифта, которым будет напечатан верхний колонтитул, нажать кнопку настройки шрифта ***«…»***. В открывшемся стандартном окне Windows **«Шрифт»** можно выбрать шрифт, начертание, размер шрифта, видоизменение, цвет шрифта и набор символов.
  - ***Выравнивание***. Необходимо выбрать, каким образом верхний колонтитул будет размещен на странице. Возможные варианты: ***По левому краю***, ***По центру***, ***По правому краю***.
  - ***Метка документа.*** Позволяет добавить в верхний колонтитул мандатную метку документа, выводимого на печать. Обозначение мандатной метки документа можно оставить заданным по умолчанию (***Метка документа:***), изменить или удалить, оставив поле пустым. Для

применения этого шаблона необходимо отметить параметр ***"Метка документа"***.

- ***Компьютер***. Позволяет добавить в верхний колонтитул имя рабочей станции, с которой была произведена печать. Обозначение рабочей станции в текстовом поле можно оставить заданным по умолчанию (***Компьютер:***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Компьютер"***.
- ***Пользователь***. Позволяет добавить в верхний колонтитул имя пользователя, под учетной записью которого была произведена печать. Обозначение пользователя в текстовом поле можно оставить заданным по умолчанию (***Пользователь:***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Пользователь"***.
- ***Напечатано***. Позволяет добавить в верхний колонтитул дату вывода документа на печать. Обозначение в текстовом поле можно оставить заданным по умолчанию (***Напечатано:***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Напечатано"***.
- ***Документ***. Позволяет добавить в верхний колонтитул имя файла документа, который был отправлен на печать. Обозначение документа в текстовом поле можно оставить заданным по умолчанию (***Документ:***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Документ"***.

❖ **Верхний логотип**

- ***Использовать верхний логотип.*** Позволяет добавить логотип в верхний колонтитул документа, выводимого на печать.
- ***Выравнивание***. Позволяет выбрать каким образом верхний логотип будет размещен на странице. Возможные варианты: ***По левому краю***, ***По центру***, ***По правому краю***.
- ***Путь к изображению***. Позволяет выбрать файл изображения, которое будет использовано в качестве логотипа в верхнем колонтитуле. Максимальный размер изображения: 300 пикселей по ширине и 200 пикселей по высоте. Возможные форматы изображений для логотипа: *.bmp, *.jpg, *.png, *.tiff, *.emf, *.gif. В поле ***Путь к изображению*** можно вручную ввести полный путь к файлу изображения или нажать кнопку выбора изображения ***«…»***, в появившемся окне **«Выбор»** (см. рис. 6.51) указать графический файл, который будет использоваться в качестве верхнего логотипа, и нажать кнопку ***Добавить***. После этого полный путь к файлу изображения будет указан в поле ***Путь к изображению***.

❖ **Нижний колонтитул**

- ***Шрифт.*** Для изменения шрифта по умолчанию, которым будет напечатан нижний колонтитул, в поле ***Шрифт*** следует нажать кнопку настройки шрифта ***«…»***. В открывшемся стандартном окне Windows **«Шрифт»** можно выбрать шрифт, начертание, размер шрифта, видоизменение, цвет шрифта и набор символов.
- ***Выравнивание.*** Следует выбрать, каким образом нижний колонтитул будет размещен на странице. Возможные варианты: ***По левому краю***, ***По центру***, ***По правому краю***.

- ***Страница***. Позволяет добавить в нижний колонтитул номер текущей страницы, выводимой на печать. Обозначение страницы в текстовом поле можно оставить заданным по умолчанию (***Страница***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Страница"***.
- ***из***. Позволяет добавить в нижний колонтитул общее количество страниц, отправленных на печать. Обозначение этого поля можно оставить заданным по умолчанию (***из***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"из"***.
- ***Принтер***. Позволяет добавить в нижний колонтитул имя принтера, на котором производится печать. Обозначение принтера в текстовом поле можно оставить заданным по умолчанию (***Принтер:***), изменить или удалить, оставив поле пустым. Для применения этого шаблона необходимо отметить параметр ***"Принтер"***.

❖ **Нижний логотип**

- ***Использовать нижний логотип.*** Позволяет добавить логотип в нижний колонтитул документа, выводимого на печать.
- ***Выравнивание.*** Позволяет выбрать, каким образом нижний логотип будет размещен на странице. Возможные варианты: ***По левому краю***, ***По центру***, ***По правому краю***.
- ***Путь к изображению.*** Позволяет выбрать файл изображения, которое будет использовано в качестве логотипа в нижнем колонтитуле. Максимальный размер изображения: 300 пикселей по ширине и 200 пикселей по высоте. Возможные форматы изображений для логотипа: *.bmp, *.jpg, *.png, *.tiff, *.emf, *.gif. В поле ***Путь к изображению*** можно вручную ввести полный путь к файлу изображения или нажать кнопку выбора изображения ***«…»***, в появившемся окне **«Выбор»** (см. рис. 6.51) указать графический файл, который будет использоваться в качестве нижнего логотипа, и нажать кнопку ***Добавить***. После этого полный путь к файлу изображения будет указан в скобках в поле ***Путь к изображению***.

6.1.10.3.3. Особенности настройки СЗИ в режиме маркировки документов при печати

Настройка для печати из Microsoft Word при включенном мандатном механизме

Для корректной работы механизма контроля печати СЗИ при печати из приложений Microsoft Word, если пользователь вошел в систему с мандатной меткой отличной от **1**, дополнительно необходимо произвести следующие настройки:

1) в настройках приложения MS Office включить макросы (приведен пример включения макросов в приложении MS Word 2007):
   - в окне **«Параметры Word»** (***Файл →Параметры***) перейти на вкладку **Центр управления безопасностью**;
   - во вкладке **Центр управления безопасностью** нажать кнопку ***Параметры центра управления безопасностью***;
   - в открывшемся окне **«Центр управления безопасностью»** перейти на вкладку **Параметры макросов**;
   - во вкладке **Параметры макросов** установить указатель напротив параметра ***Включить все макросы***;

- последовательно нажать кнопку ***ОК*** в окнах **«Центр управления безопасностью»** и **«Параметры Word»**.

2) в **Основной панели настроек клиентов** серверной консоли администрирования СЗИ для выбранного пользователя отметить параметр ***Включить контроль печати***;
3) добавить в область *Разграничение прав печати по процессам* приложение Microsoft Word и установить для него параметры ***Разрешение*** и ***Аудит***. Например, для печати из Microsoft Word 2007 необходимо добавить объект Winword.exe, расположенный в папке C:\Program Files\Microsoft Office\Office12 (для 32-bit ОС) и C:\Program Files (x86)\Microsoft Office\Office12 (для 64-bit ОС).

Для пакета MS Office должна быть включена поддержка VBA (инсталлируется в процессе установки пакета, если сделан соответствующий выбор).

Маркировка документов при печати из 32-битных приложений в 64-битных ОС

При настройке механизма контроля печати в серверной консоли администрирования при постановке на контроль 32-битного приложения автоматически на контроль добавляется процесс **splwow64.exe**, предназначенный для печати из 32-битных приложений в 64-разрядных ОС. При этом если установить параметр ***Колонтитулы*** для любого 32-битного приложения, то автоматически параметр ***Колонтитулы*** будет установлен для всех 32-битных приложений, поставленных на контроль в механизме контроля печати, а также и для процесса **splwow64.exe**.

Настройка печати при отображении в распечатанном документе нечитаемых символов

При включенном в режиме маркировки документов механизме контроля печати СЗИ в некоторых распечатываемых из Adobe Acrobat Reader XI или Internet Explorer документах вместо текста могут выводиться нечитаемые символы. Также нечитаемые символы могут выводиться при печати xps-документов.

Для возможности корректной распечатки такого документа из *Adobe Acrobat Reader XI* необходимо отправлять этот документ на печать «как изображение». Для этого необходимо в диалоговом окне печати документа нажать кнопку ***Дополнительно*** (***Advanced***) и в открывшемся окне установить параметр ***Печатать как изображение*** (***Print As Image***). После этого документ будет корректно распечатан.

Для возможности корректной печати такого документа из Internet Explorer необходимо включить для Internet Explorer отдельный режим обработки заданий на печать (порядок включения режима см. п. 6.1.10.4.1. настоящего документа).

Для возможности корректной печати xps-документов необходимо включить отдельный режим обработки заданий на печать для приложения **Средство просмотра XPS** (файл **xpsrchvw.exe**).

6.1.10.4. Решение проблем, возникающих в работе механизма контроля печати

В работе некоторых приложений, установленных на компьютере, могут наблюдаться проблемы их совместного функционирования с механизмом контроля печати СЗИ, работающим в режимах аудита печати и разграничения доступа к приложениям (см. пункт 6.1.10.2 настоящего документа) и маркировки документов (см. пункт 6.1.10.3 настоящего документа). Поскольку, при использовании механизма контроля печати в этих режимах, на контроль автоматически ставятся все процессы, из которых может происходить печать, то

для корректной работы таких приложений необходимо выполнить дополнительные настройки механизма контроля печати СЗИ:

1. Активировать для «проблемных» приложений отдельный режим обработки заданий на печать (см. п. 6.1.10.4.1 настоящего документа);

2. Если приложение, с отдельным режимом обработки заданий печати, продолжает работать некорректно – исключить его из списка контролируемых механизмом контроля печати СЗИ (см. п. 6.1.10.4.2 настоящего документа). При этом на них не будет распространяться действие механизма контроля печати СЗИ: запрет печати из приложения, применение шаблона печати и аудит печати.

6.1.10.4.1 Настройка отдельного режима обработки заданий на печать

Для устранения возможных ошибок печати документов из некоторых приложений, необходимо перевести их в отдельный режим обработки заданий на печать. Для этого необходимо выполнить следующие действия в серверной консоли администрирования СЗИ:

1. В настройках механизма контроля печати пользователя (см. рис. 6.54) добавить на контроль приложения, для которых будет действовать отдельный режим печати механизма контроля печати СЗИ;
2. Установить параметры ***Разрешение*** и ***Отложенный контроль***, расположенные в строке справа от выбранного объекта (рис. 6.54);
3. При необходимости отметить параметры ***Аудит*** и ***Колонтитулы***;
4. Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Настройки вступят в силу после выхода интерактивного пользователя из системы с последующим входом, либо перезагрузки редактируемой рабочей станции.

В результате станет возможна корректная работа с приложениями, для которых отмечен параметр ***Отложенный контроль***, включая печать со всеми указанными в настройках механизма контроля печати параметрами (аудит, колонтитулы).

Такой способ подходит, когда от программы не зависят типы открываемых файлов, которые можно печатать через контекстное меню, что в ином случае приводит к пропуску печати в обход механизма контроля печати СЗИ.

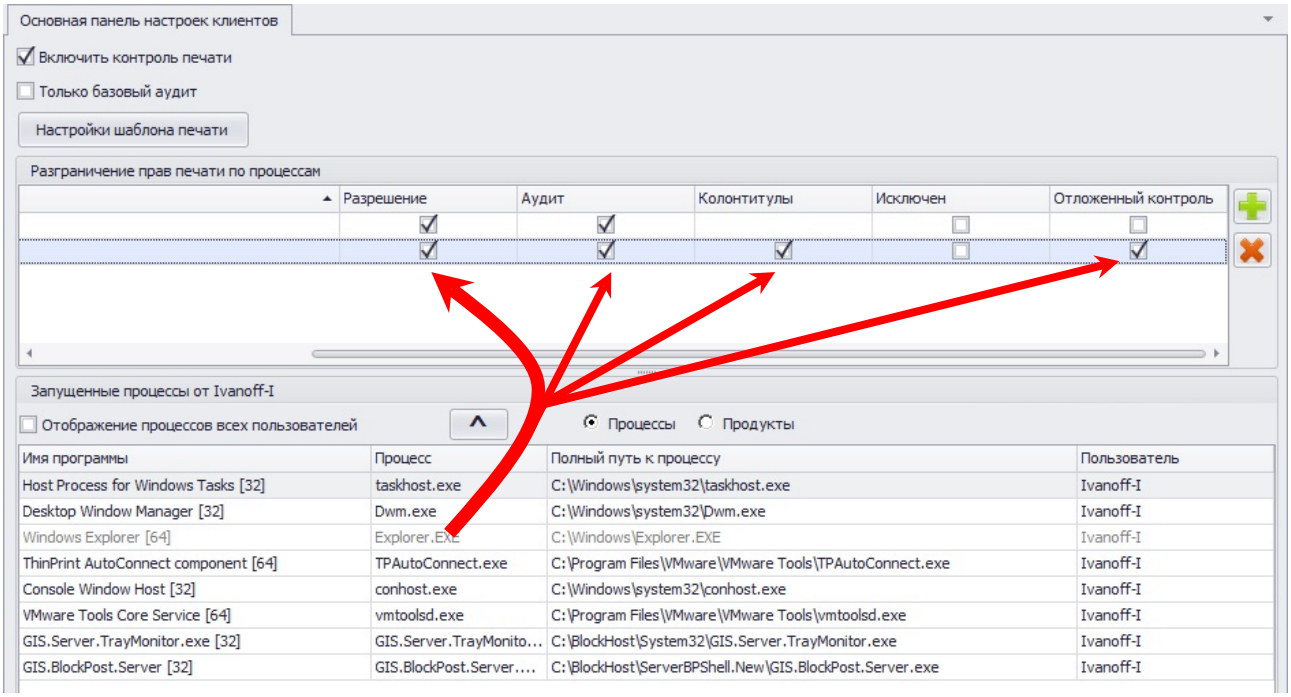


Рисунок 6.54. Приложения с отдельным режимом обработки заданий на печать

6.1.10.4.2 Исключение приложений из механизма контроля печати

Для исключения приложений из списка контролируемых механизмом контроля печати СЗИ необходимо в серверной консоли администрирования СЗИ выполнить следующие действия:

1. В настройках механизма контроля печати пользователя добавить в область *Разграничение прав печати по процессам* приложения, которые не будут контролироваться механизмом контроля печати СЗИ;
2. Установить параметр ***Исключен***, расположенный в строке справа от выбранного объекта (рис. 6.55);
3. Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Настройки вступят в силу после выхода интерактивного пользователя из системы с последующим входом, либо перезагрузки редактируемой рабочей станции.

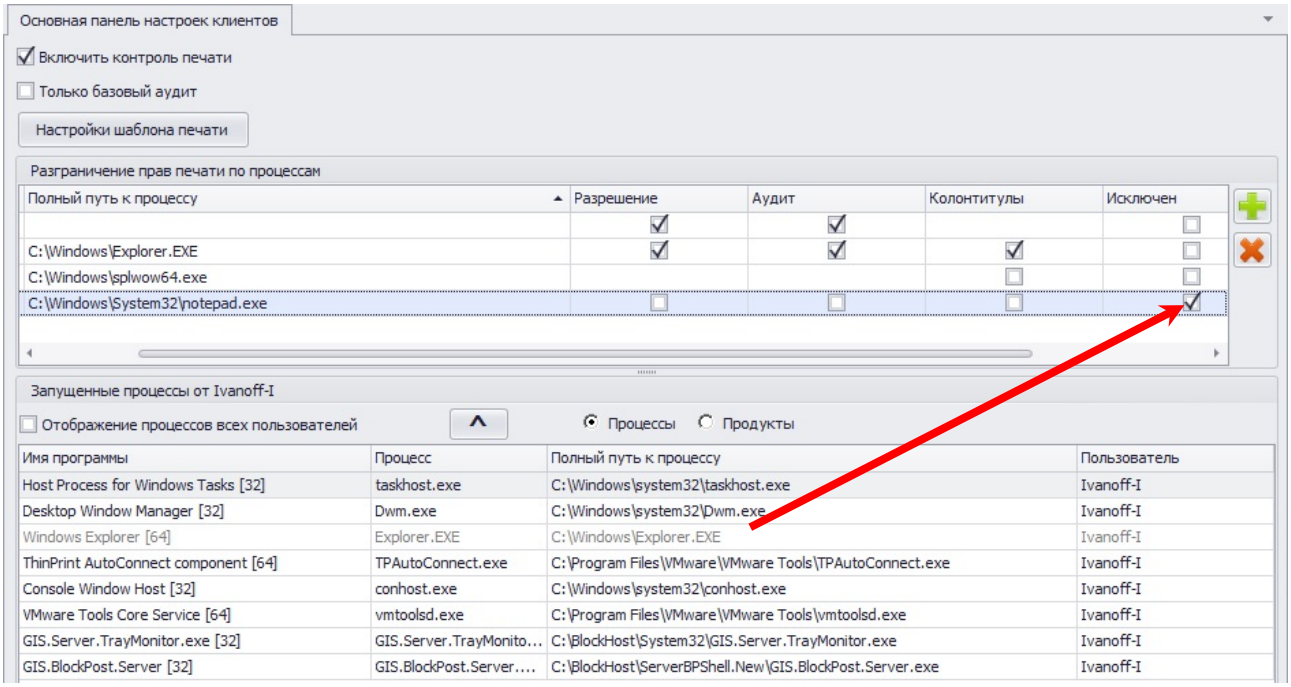


Рисунок 6.55. Приложения, добавленные в исключения механизма контроля печати

В результате на приложения, для которых отмечен параметр ***Исключен***, не будет распространяться действие механизма контроля печати СЗИ: запрет печати из приложения, применение шаблона печати и аудит печати.

6.1.11. Репликация индивидуальных механизмов разграничения доступа

В СЗИ «Блокхост-сеть 2.0» существует возможность репликации (копирования) индивидуальных механизмов разграничения доступа, настроенных для одного из пользователей, и на других пользователей, в том числе и на пользователей других рабочих станций. Использование механизма копирования настроек СЗИ существенно облегчает задачу администратора безопасности по выполнению однотипных настроек индивидуальных механизмов разграничения доступа для разных пользователей.

Для того, чтобы реплицировать настройки индивидуального механизма СЗИ администратору безопасности необходимо:

1. В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все машины***, выбрать рабочую станцию, настройки индивидуального механизма разграничения доступа пользователя которой будут копироваться;
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, настройки механизма СЗИ которого будут переноситься, и затем выделить необходимый механизм;
3. Выбрать пункт меню ***Главная →Копировать***. В результате в буфер обмена будут скопированы настройки выбранного механизма СЗИ указанного пользователя;
4. Затем в окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для пользователя которой будут установлены скопированные настройки механизма СЗИ;
5. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, выделить пользователя, для которого будут устанавливаться настройки. Для

репликации механизма СЗИ сразу для всех пользователей выбранной рабочей станции необходимо выделить пункт ***Список пользователей***;

6. Выбрать пункт меню ***Главная →Вставить***. В результате у обоих пользователей настройки скопированного механизма СЗИ будут идентичны:
7. При необходимости повторить операцию репликации выбранного механизма СЗИ и для других пользователей.

Для репликации следующего пользовательского механизма СЗИ следует заново пройти шаги, описанные в п.п. 1 – 6.

6.2. Настройка системных механизмов защиты информации

Системные механизмы защиты информации являются механизмами, общими для всех пользователей на компьютере. В состав системных механизмов входят: механизм мандатного разграничения доступа, механизм контроля целостности, механизм очистки памяти и механизм мягкого режима.

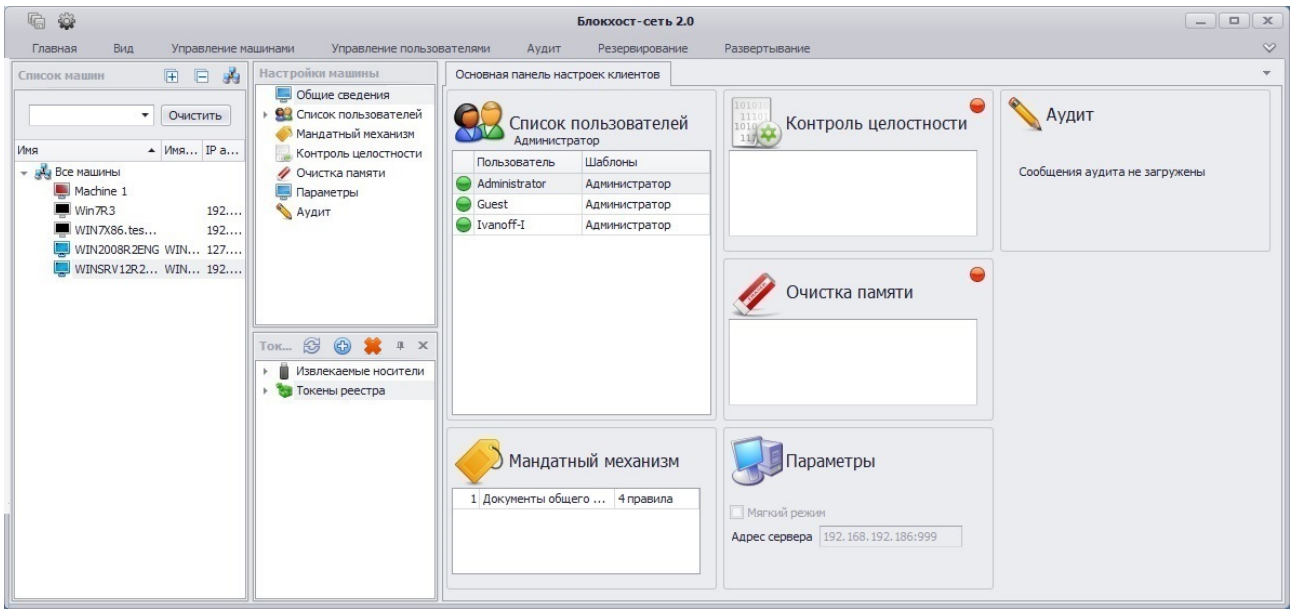
Произведенные настройки системных механизмов разграничения доступа вступают в силу после перезагрузки ОС на контролируемой рабочей станции. Следует учесть, что если администратор отправит рабочую станцию на перезагрузку командой из серверной консоли администрирования (***Управление машинами →Перезагрузить***), то перезагрузка ОС начнется без каких-либо предупреждений для пользователя и несохраненные данные могут быть потеряны. Чтобы этого избежать, можно дождаться, когда пользователь сам завершит работу ПК (например, в конце рабочего дня) и при последующей загрузке ОС новые настройки вступят в силу.

6.2.1. Мандатный механизм разграничения доступа

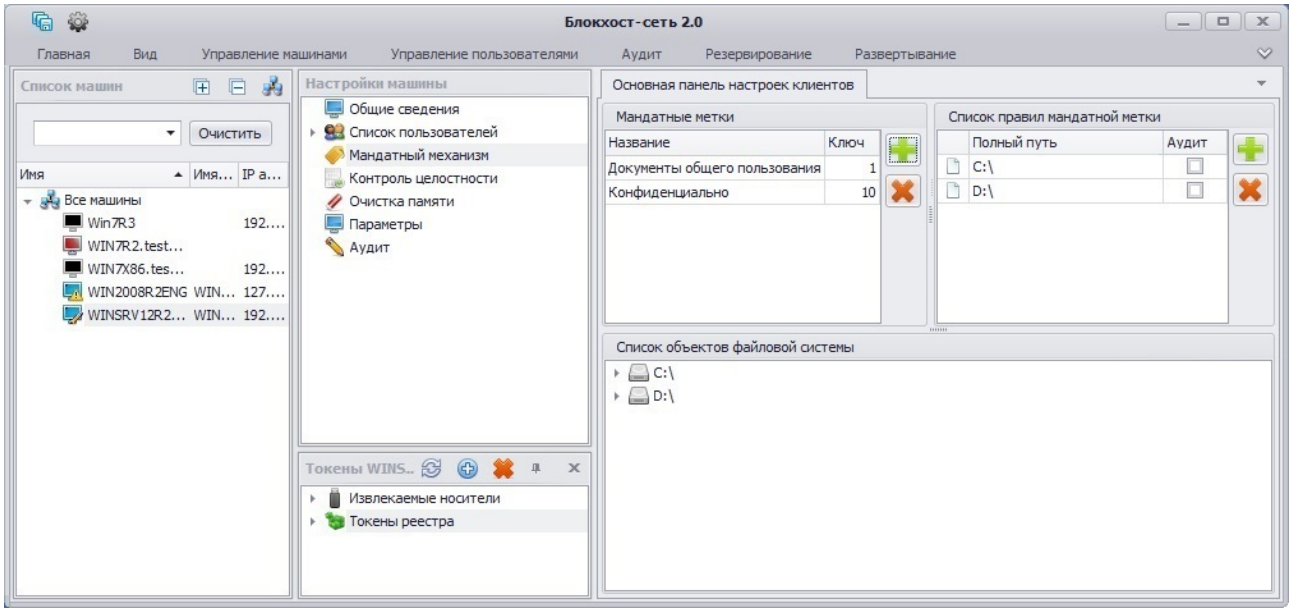
Настройка мандатного механизма разграничения доступа в СЗИ «Блокхост-сеть 2.0» заключается в сопоставлении списка защищаемых ресурсов (объектов файловой системы) значениям созданных мандатных меток.

Для того, чтобы перейти к настройке мандатного механизма разграничения доступа администратору безопасности следует:

1. В окне **«Список машин»** консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка мандатного механизма разграничения доступа.
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Мандатный механизм*** (рис. 6.56, а) или в окне **«Настройки машины»** выбрать пункт ***Мандатный механизм***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.56, б).



а)



б)

Рисунок 6.56. Настройка мандатного механизма в консоли администрирования СЗИ

Все дальнейшие действия по созданию, изменению или удалению мандатных меток происходят во вкладке **Основная панель настроек клиентов** редактируемой рабочей станции.

6.2.1.1. Создание мандатных меток

В СЗИ «Блокхост-сеть 2.0» в процессе инсталляции создается мандатная метка *Документы общего пользования* со значением **1**. Этой метке по умолчанию сопоставляются все ресурсы (объекты файловой системы жестких дисков и подключаемых накопителей), которые присутствуют на рабочей станции в момент установки клиентской части СЗИ.

Для создания мандатной метки в СЗИ «Блокхост-сеть 2.0» администратору безопасности необходимо:

1. В **Основной панели настроек клиентов** в области *Мандатные метки* нажать кнопку ***Добавить*** .

2. В открывшемся окне **«Добавление мандатной метки»** (рис. 6.57) в соответствующих полях указать числовое значение и имя мандатной метки.

> В поле ***Метка*** возможен ввод только цифр. При вводе в поле ***Метка*** числа, равного или больше 256 рядом с полем появится пиктограмма ошибки (см. пример на рис. 6.58). В этом случае при наведении курсора на пиктограмму появится всплывающее описание ошибки – *Номер мандатной метки должен быть меньше 256.*

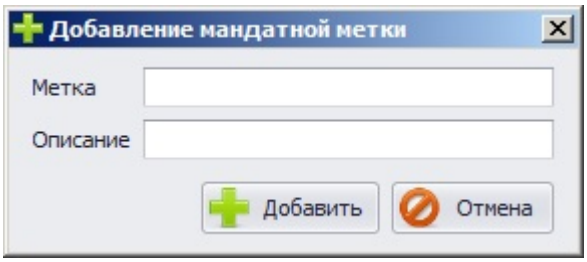


Рисунок 6.57. Окно создания мандатной метки

3. В окне **«Добавление мандатной метки»** нажать кнопку ***Добавить***. Добавленная метка отобразится в области *Мандатные метки* (см. рис. 6.56, б). Нажатие кнопки ***Отмена*** в окне **«Добавление мандатной метки»** позволит администратору выйти из окна без создания метки.
4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

В случае, если значение и/или описание мандатной метки повторяют уже существующие, в окне **«Добавление мандатной метки»** появится пиктограмма ошибки , при наведении курсора на которую отобразится текст ошибки (на рис. 6.58 приведен пример создания метки с существующим номером).

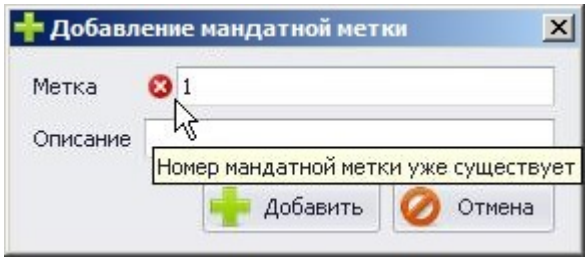


Рисунок 6.58. Сообщение об ошибке создания мандатной метки

6.2.1.2. Сопоставление метке списка ресурсов

Для сопоставления мандатной метке ресурсов системы (определения классификационного уровня объектов файловой системы) администратору безопасности необходимо выполнить следующие действия:

1. В **Основной панели настроек клиентов** в области *Мандатные метки* (рис. 6.56, б) выделить из списка мандатных меток ту метку, для которой будет производиться сопоставление ресурсов;
2. В области *Список объектов файловой системы* выделить необходимый объект (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько объектов) и при помощи мыши перетащить его из дерева ресурсов в область *Список правил мандатной метки* (рис. 6.59).

Для сопоставления файловых объектов выделенной мандатной метке можно также воспользоваться кнопкой ***Добавить*** , после нажатия на которую откроется окно **«Выбор»** (см. пример на рис. 6.50). В окне **«Выбор»** необходимо раскрыть структуру каталогов контролируемого компьютера, выбрать необходимый ресурс (файл или каталог) и нажать кнопку ***Добавить***.

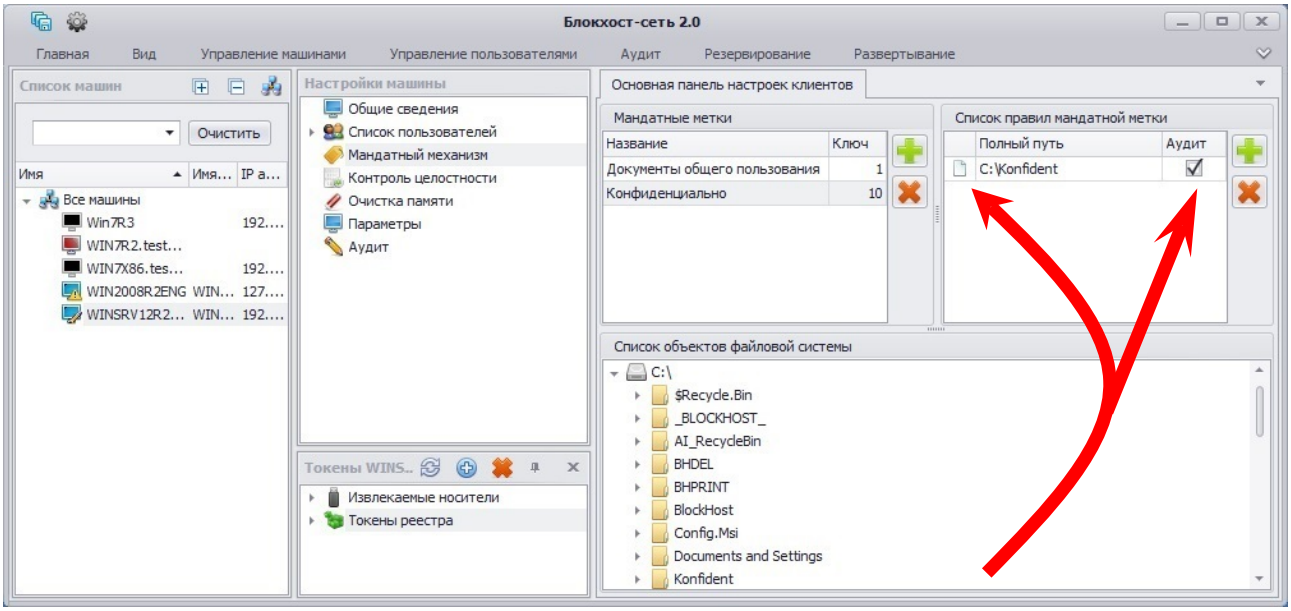


Рисунок 6.59. Добавление ресурса

3. Для удаления ресурсов из списка достаточно выделить в области *Список правил мандатной метки* требуемый объект (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько объектов) и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Удалить*** , расположенной справа от списка объектов);
4. При необходимости администратор безопасности может разрешить фиксацию событий, связанных с попытками доступа к контролируемому объекту, в журнал СЗИ «Блокхост-сеть 2.0». Для этого в области *Список правил мандатной метки* необходимо установить отметку в поле ***Аудит***, расположенное справа от выбранного объекта файловой системы (рис. 6.59);
5. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

По умолчанию, если администратор безопасности не сопоставлял мандатную метку объекту и объект не является вложенным (любой степени вложенности) в другой объект, которому ранее была сопоставлена мандатная метка, всем ресурсам соответствует метка *Документы общего пользования* со значением ***1***.

При попытке добавления в список объектов, сопоставляемых редактируемой метке, файлового ресурса, которому ранее администратор безопасности уже сопоставил другую мандатную метку, откроется окно с запросом об изменении мандатной метки добавляемого ресурса (рис. 6.60). При необходимости переназначения мандатной метки такого ресурса следует нажать кнопку ***Да***. Нажатие кнопки ***Отмена*** в окне **«Добавление мандатного доступа»** оставит метку добавляемого файлового ресурса без изменений.

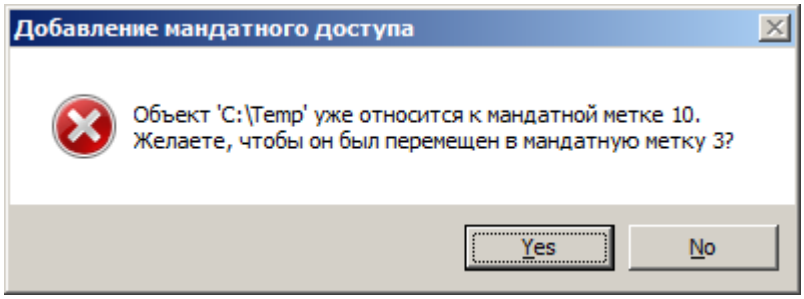


Рисунок 6.60. Переназначение мандатной метки файлового ресурса

6.2.1.3. Особенности работы с жесткими и символьными ссылками при настройке мандатного механизма разграничения доступа

В файловой системе NTFS существует технология привязки (Link), позволяющая одному и тому же файлу существовать в нескольких каталогах, иногда под разными именами. Подобная привязка называется жесткой связью или жесткой ссылкой (hard link). Другим вариантом привязки файлов является символьная ссылка («junction point» и «symlink). Более подробное описание жестких и символьных ссылок приведено в пункте 6.1.1.3 настоящего документа.

Для того, чтобы установить мандатное разграничение доступа для объекта, имеющего жесткие и символьные ссылки, администратору безопасности необходимо:

1. Проверить наличие жестких и символьных ссылок, относящихся к контролируемым объектам. Проверка проводится аналогично проверке наличия жестких и символьных ссылок при дискреционном разграничении доступа, описание которого приведено в пункте 6.1.1.3 настоящего документа.
2. В настройках консоли администрирования СЗИ присвоить одинаковые мандатные метки контролируемым объектам (файлам и папкам) и жестким ссылкам, относящимся к ним.
3. Для объектов, имеющих символьные ссылки необходимо убедиться, что в настройки консоли администрирования СЗИ на контроль добавлены исходные (оригинальные) файлы и папки, а не их символьные ссылки (см. подробнее пункт 6.1.1.3 настоящего документа). Установленные в СЗИ права доступа для оригинального объекта (файла или папки) будут действовать при попытках доступа к нему по символьной ссылке.

6.2.1.4. Изменение мандатных меток

Администратор безопасности может при необходимости изменять следующие параметры мандатной метки: ее имя (описание) и числовое значение классификационного уровня. Данные параметры изменяются без ущерба для списка сопоставленных метке ресурсов.

Для изменения параметров существующей мандатной метки администратор безопасности должен:

1. В **Основной панели настроек клиентов** в области *Мандатные метки* (рис. 6.56, б) щелкнуть два раза левой кнопкой мыши по имени той метки, параметры которой будут изменяться.
2. В открывшемся окне **«Изменение мандатной метки»** изменить требуемые параметры мандатной метки:

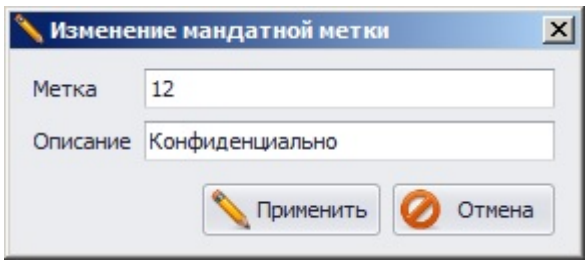


Рисунок 6.61. Диалоговое окно изменения мандатной метки

3. После корректировки параметров мандатной метки, для присвоения ей новых значений необходимо нажать кнопку ***Применить***. Список объектов, ранее сопоставленных данной метке, останется без изменений. Нажатие кнопки ***Отмена*** вместо кнопки ***Применить*** в окне **«Изменение мандатной метки»** позволит администратору выйти из окна без изменения характеристик метки.
4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Возможность изменения параметров мандатной метки позволяет существенно упростить процедуру корректировки классификационного уровня для группы объектов файловой системы. Администратору безопасности вместо удаления одной метки, создания другой и сопоставления с ней группы объектов достаточно изменить числовое значение выбранной метки.

6.2.1.5. Реализация неиерархических категорий при использовании мандатного принципа контроля доступа

Реализацию неиерархических категорий при использовании мандатного принципа контроля доступа можно рассмотреть на следующем примере.

На ЭВМ имеется 2 локальных диска *C:* и *D:*, на каждом из которых расположены папки с одинаковыми мандантами метками:

- диск *C:* содержит папку *Конфиденциально* со значением мандатной метки **2** (*C:\M2*) и папку *Секретно* со значением мандатной метки **3** (*C:\M3*);
- диск *D:* содержит папку *Конфиденциально* со значением мандатной метки **2** (*D:\M2*) и папку *Секретно* со значением мандатной метки **3** (*D:\M3*).

На ЭВМ работают 4 пользователя:

- пользователю **User C2** присвоено значение мандатной метки, равное **2**;
- пользователю **User C3** присвоено значение мандатной метки, равное **3**;
- пользователю **User D2** присвоено значение мандатной метки, равное **2**;
- пользователю **User D3** присвоено значение мандатной метки, равное **3**.

Рассматриваемый пример приведен для случая, когда пользователи работают за ЭВМ с максимальным значением мандатной метки.

Пользователи **User C2** и **User C3** должны иметь доступ только к папкам на диске *C:*, а пользователи **User D2** и **User D3** – только к папкам на диске *D:* (в соответствии с их мандатными метками).

Решение данной задачи достигается путем сочетания мандатного и дискреционного механизмов разграничения доступа.

Матрицы разграничения доступа при настройке мандатного и дискреционного механизмов приведены в таблицах 6.2.1 и 6.2.2 соответственно.

Таблица 6.2.1 - Матрица разграничения доступа при настройке мандатного механизма разграничения доступа

СУБЪЕКТЫ	**ОБЪЕКТЫ**			
	C:\M2 (мандатная метка= 2)	**C:\M3 (мандатная метка = 3)**	**D:\M2 (мандатная метка= 2)**	**D:\M3 (мандатная \метка = 3)**
User C2 (мандатная метка = **2**)	rw	-	rw	-
User C3 (мандатная метка = **3**)	r	rw	r	rw
User D2 (мандатная метка = **2**)	rw	-	rw	-
User D3 (мандатная метка = **3**)	r	rw	r	rw

Таблица 6.2.2 - Матрица разграничения доступа при настройке дискреционного механизма разграничения доступа

	C:	**D:**
User C2	rw	-
User C3	rw	-
User D2	-	rw
User D3	-	rw

Итоговая матрица разграничения доступа, полученная в результате сочетания мандатного и дискреционного механизмов разграничения доступа, приведена в таблице 6.2.3.

Таблица 6.2.3 - Итоговая матрица разграничения доступа

СУБЪЕКТЫ	**ОБЪЕКТЫ**			
	C:\M2 (мандатная метка= 2)	**C:\M3 (мандатная метка = 3)**	**D:\M2 (мандатная метка= 2)**	**D:\M3 (мандатная \метка = 3)**
User C2 (мандатная метка = **2**)	rw	-	-	-
User C3 (мандатная метка = **3**)	r	rw	-	-
User D2 (мандатная метка = **2**)	-	-	rw	-
User D3 (мандатная метка = **3**)	-	-	r	rw

Таким образом, неиерархические категории в СЗИ реализуются путем сочетания мандатного и дискреционного механизмов разграничения доступа.

6.2.1.6. Удаление мандатных меток

Для удаления мандатной метки администратору безопасности необходимо:

1. В **Основной панели настроек клиентов** в разделе *Мандатные метки* (рис. 6.56, б) выбрать мандатную метку и нажать кнопку ***Удалить***  (либо воспользоваться клавишей **<Del>**). Выбранная мандатная метка будет удалена.

2. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Все ресурсы, которые были сопоставлены удаленной метке (т.е. имеющие классификационный уровень, равный числовому значению данной метки), высвобождаются. Ниже приведены варианты изменения классификационного уровня высвободившегося ресурса:

- Если высвободившийся ресурс является вложенным в объект файловой системы, причем классификационный уровень этого объекта отличен от **1**, то классификационный уровень высвободившегося ресурса будет равен классификационному уровню объекта, в который вложен ресурс.
- Если высвободившийся ресурс не является вложенным в объект файловой системы, обладающий отличным от **1** классификационным уровнем, то классификационный уровень высвободившегося ресурса будет равен **1** (высвободившийся ресурс автоматически будет сопоставлен метке по умолчанию *Документы общего доступа*).

Мандатную метку *Документы общего доступа* удалить нельзя. При попытке удаления этой метки откроется окно с сообщением об ошибке удаления метки со значением **1**.

6.2.2. Контроль целостности

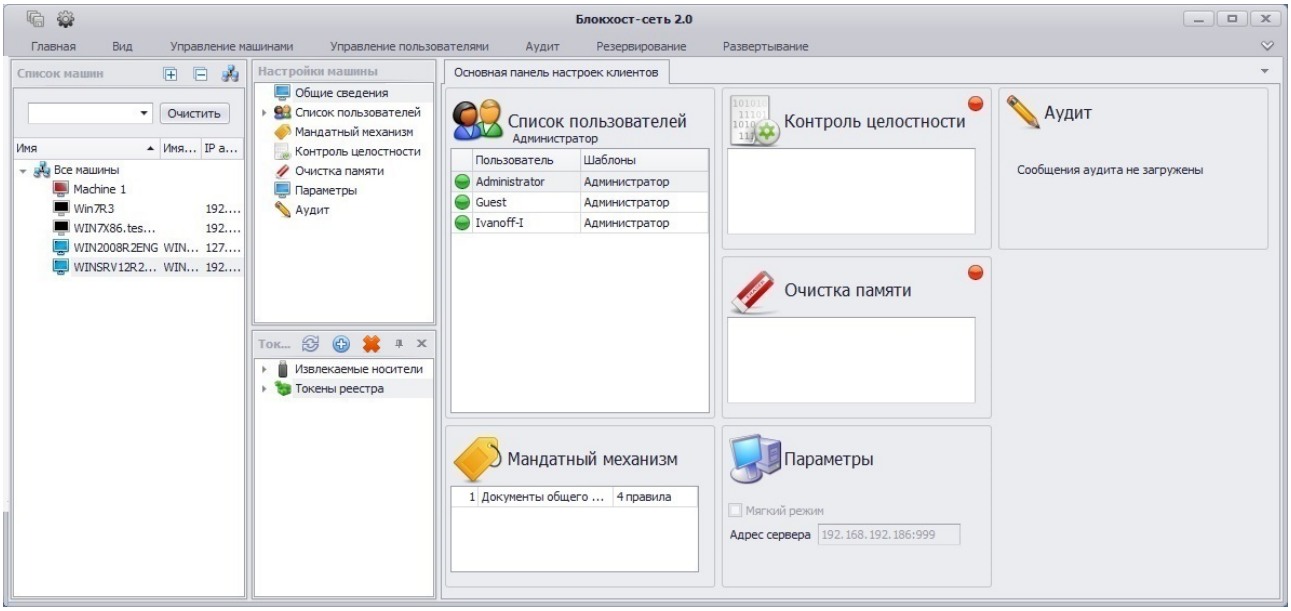
Механизм контроля целостности представляет собой защитное средство, позволяющее своевременно обнаруживать и устранять несанкционированное изменение ресурсов системы (объектов файловой системы). Механизм контроля целостности позволяет обеспечивать правильное функционирование системы защиты и целостность обрабатываемой информации. Неизменность файлов механизма контроля целостности СЗИ проверяется каждый раз при загрузке операционной системы. Целостность поставленных на контроль файлов обеспечивается путем периодической проверки вычисленных при постановке файлов на контроль контрольных сумм. Период проверки контрольных сумм задается администратором безопасности на основе требований политики безопасности. При несоответствии полученных контрольных сумм эталонным значениям производится автоматическое восстановление исходных файлов из резервной папки.

6.2.2.1. Настройка механизма контроля целостности

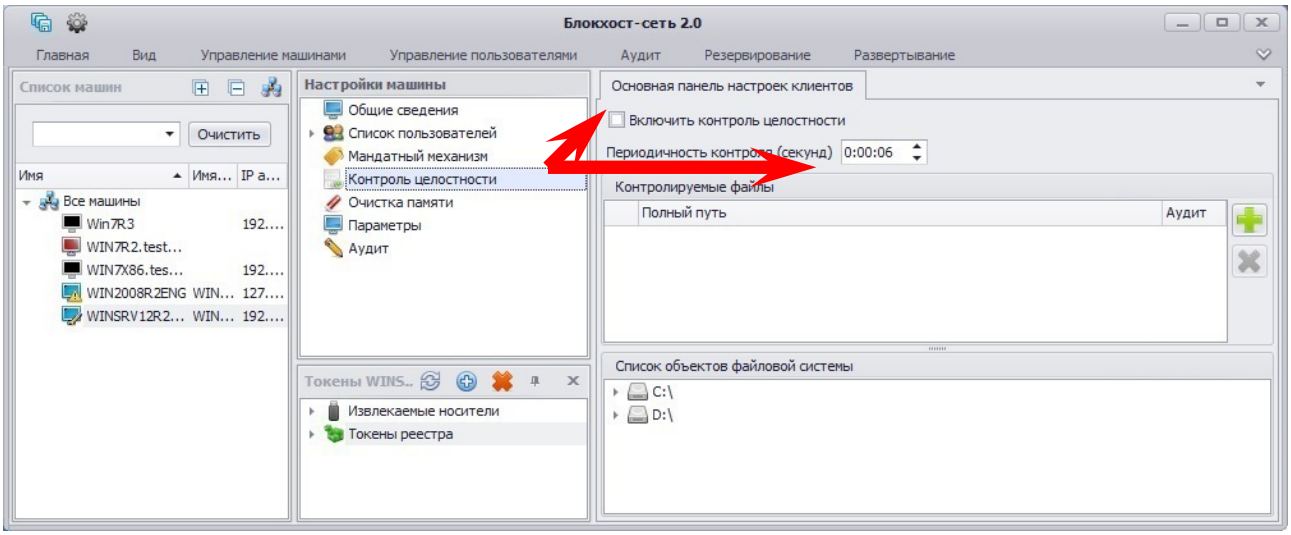
Для настройки механизма контроля целостности администратор безопасности должен:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля целостности.
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Контроль целостности*** (рис. 6.62, а) или в окне **«Настройки машины»** выбрать пункт ***Контроль целостности***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.62, б).
3. В **Основной панели настроек клиентов** включить (отключить) механизм контроля целостности, выбрав пункт ***Включить контроль целостности***.
4. В **Основной панели настроек клиентов** задать значение периода проверки контрольных сумм, указав в поле ввода ***Периодичность контроля***

соответствующее значение в формате *ЧЧ:ММ:СС*, минимальное значение периода контроля целостности 1 секунда, максимальное – 23:59:59.



а)



б)

Рисунок 6.62. Настройка механизма контроля целостности

5. В **Основной панели настроек клиентов** добавить файлы на контроль, для чего выделить необходимый объект в списке ресурсов файловой системы (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько файлов) и при помощи мыши перетащить его в область *Контролируемые файлы*.

   Для постановки файлов на контроль целостности можно также воспользоваться кнопкой ***Добавить***  , после нажатия на которую откроется окно **«Выбор»** (см. пример на рис. 6.50). В окне **«Выбор»** необходимо раскрыть структуру каталогов контролируемого компьютера, выбрать необходимый файл и нажать кнопку ***Добавить***.
6. При необходимости администратор безопасности может разрешить фиксацию событий, связанных с безопасностью информации, содержащейся в данном объекте, в журнал СЗИ «Блокхост-сеть 2.0». Для этого в области *Контролируемые*

файлы необходимо оставить отмеченным переключатель параметра ***Аудит***, расположенный справа от выбранного объекта:

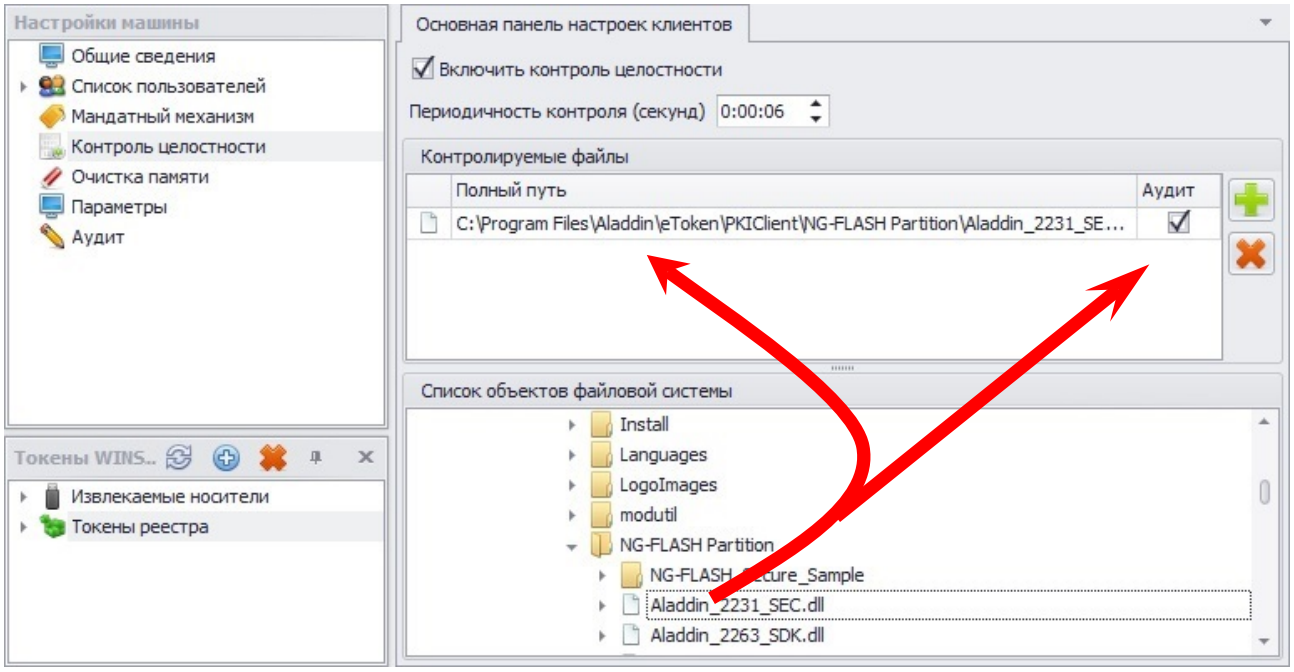


Рисунок 6.63. Добавление ресурсов на контроль целостности

7. Для удаления файлов из списка контролируемых достаточно выделить в области *Контролируемые файлы* требуемый файл (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько файлов) и нажать клавишу **<Del>** (либо воспользоваться кнопкой ***Удалить*** , которая находится справа от списка файлов, поставленных на контроль).
8. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

Следует иметь в виду, что в СЗИ «Блокхост-сеть 2.0» невозможно поставить на контроль целостности файлы нулевой длины (т.е. файлы, имеющие размер 0 байт). При попытке добавления такого файла в область *Контролируемые файлы*, перетаскиванием мыши или с использованием окна **«Выбор»**, он автоматически удалится из нее, а в окне **«Лог»** появится сообщение: `Ошибка получения контрольной суммы для файла <имя_файла>`.

6.2.3. Механизм очистки памяти

В СЗИ «Блокхост-сеть 2.0» механизм очистки памяти производит запись маскирующей информации в участки памяти, освобождаемые контролируемыми процессами. Список контролируемых процессов определяется политикой безопасности и задается администратором безопасности в консоли администрирования СЗИ «Блокхост-сеть 2.0».

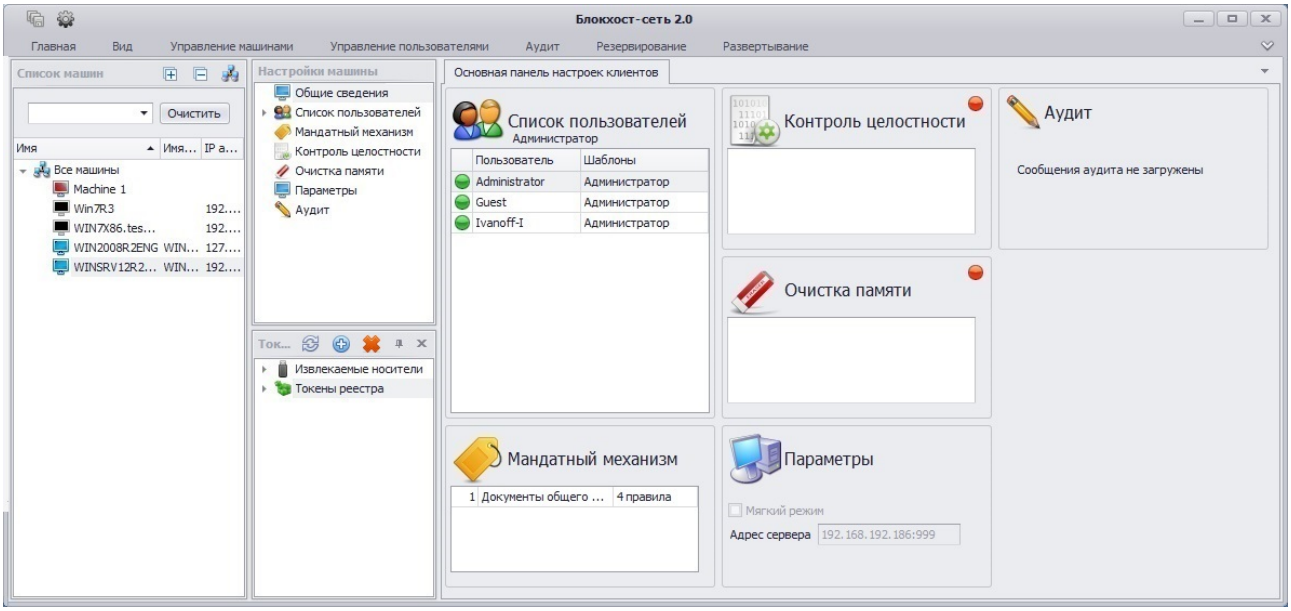
Процесс перезаписи оперативной памяти происходит по следующей схеме: по окончании работы контролируемого процесса механизм очистки памяти производит захват всей свободной оперативной памяти, включая и область, освобожденную контролируемым процессом. Захваченные области оперативной памяти перезаписываются маскирующими данными. По мере перезаписи механизм очистки высвобождает перезаписанную область. В начальный момент перезаписи оперативной памяти возможно замедление

производительности системы вплоть до некоторого “зависания”. Однако по мере высвобождения перезаписанных областей оперативной памяти работа системы возвращается в нормальное состояние.

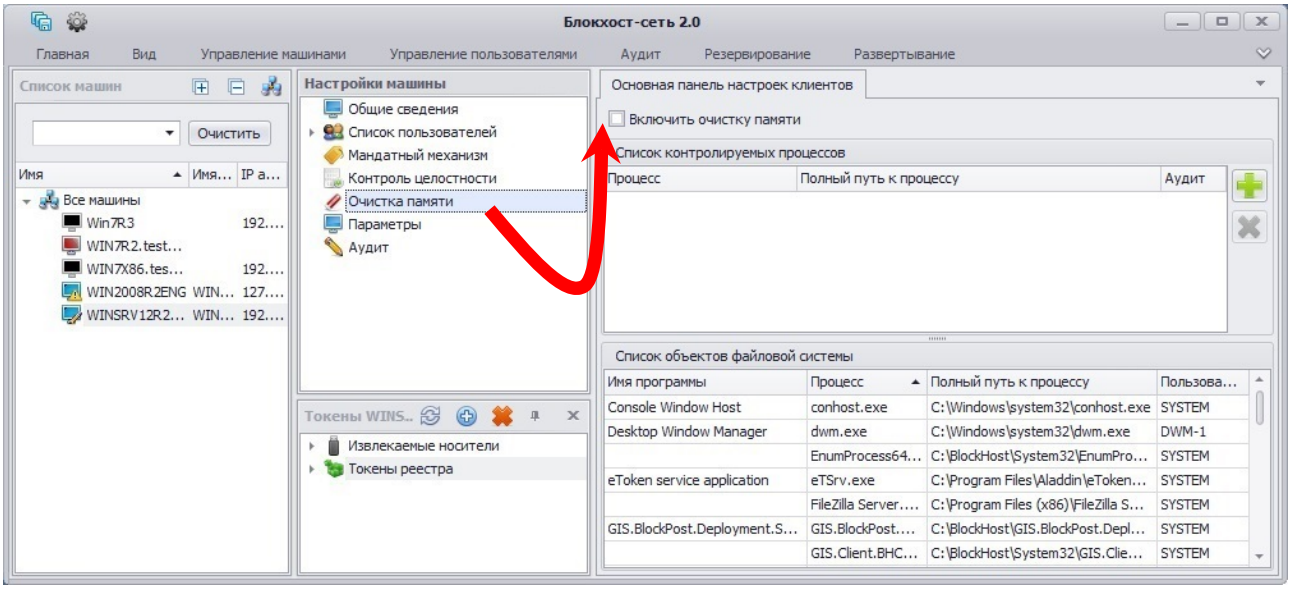
6.2.3.1. Настройка механизма очистки памяти

Для настройки механизма очистки памяти администратору безопасности необходимо осуществить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля целостности.
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Контроль целостности*** (рис. 6.64, а) или в окне **«Настройки машины»** выбрать пункт ***Контроль целостности***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.64, б).
3. В **Основной панели настроек клиентов** включить (отключить) механизм очистки памяти, выбрав пункт **«Включить очистку памяти»** (рис. 6.64, б).



а)



б)

Рисунок 6.64. Активизация механизма очистки памяти

4. В **Основной панели настроек клиентов** добавить процессы на контроль, для чего выделить необходимый объект в списке объектов файловой системы (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько объектов), и при помощи мыши перетащить его в область *Список контролируемых процессов* (рис. 6.65). Для добавления процесса, если он не запущен в настоящее время, можно также воспользоваться кнопкой добавления процесса ***Добавить***, после нажатия на которую откроется окно **«Выбор»** (см. пример на рис. 6.51). В окне **«Выбор»** следует раскрыть структуру каталогов удаленного компьютера, выбрать необходимый исполняемый файл и нажать кнопку ***Добавить***.

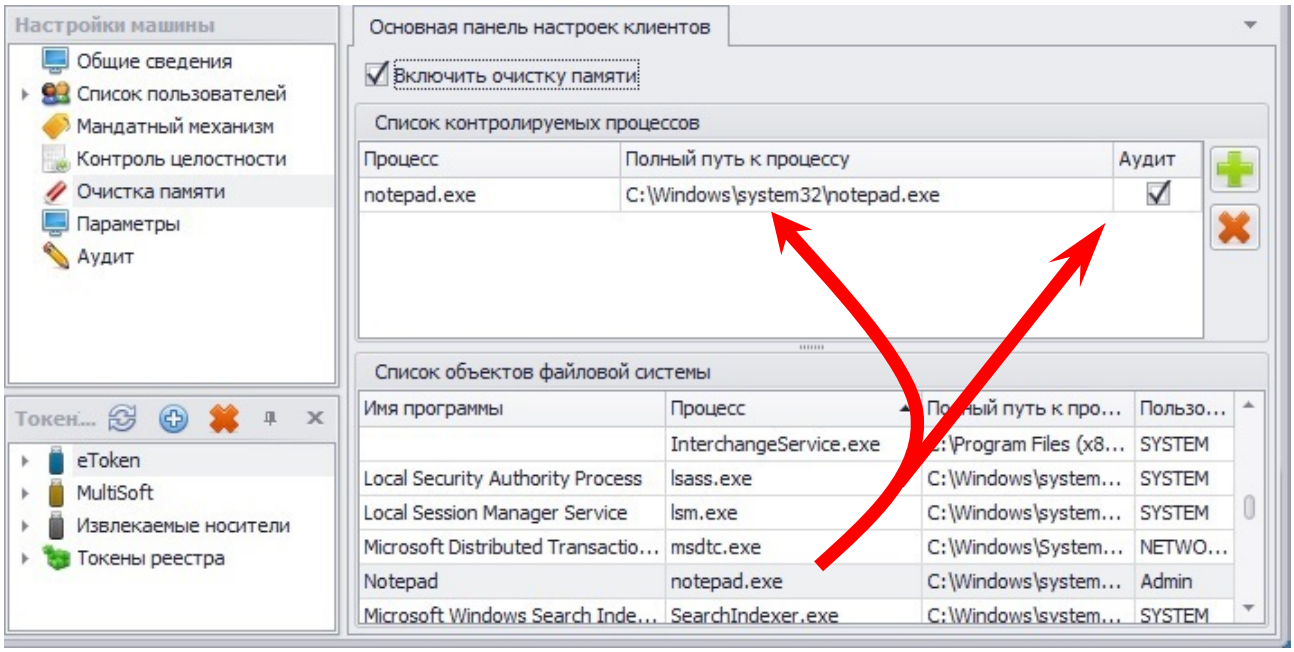


Рисунок 6.65. Добавление ресурсов для механизма очистки памяти

5. При необходимости администратор безопасности может разрешить фиксацию событий, связанных с безопасностью информации, содержащейся в контролируемом объекте, в журнал СЗИ «Блокхост-сеть 2.0». Для этого в области *Список контролируемых процессов* необходимо оставить отмеченным переключатель параметра ***Аудит***, расположенный справа от выбранного объекта.
6. Для удаления процесса из списка контролируемых достаточно выделить в области *Список контролируемых процессов* требуемый процесс (при помощи клавиш **<Ctrl>** или **<Shift>** можно выделить несколько объектов) и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Удалить***, которая находится справа от списка контролируемых процессов).
7. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***, расположенной в левом верхнем углу консоли администрирования СЗИ.

6.2.4. Механизм мягкого режима

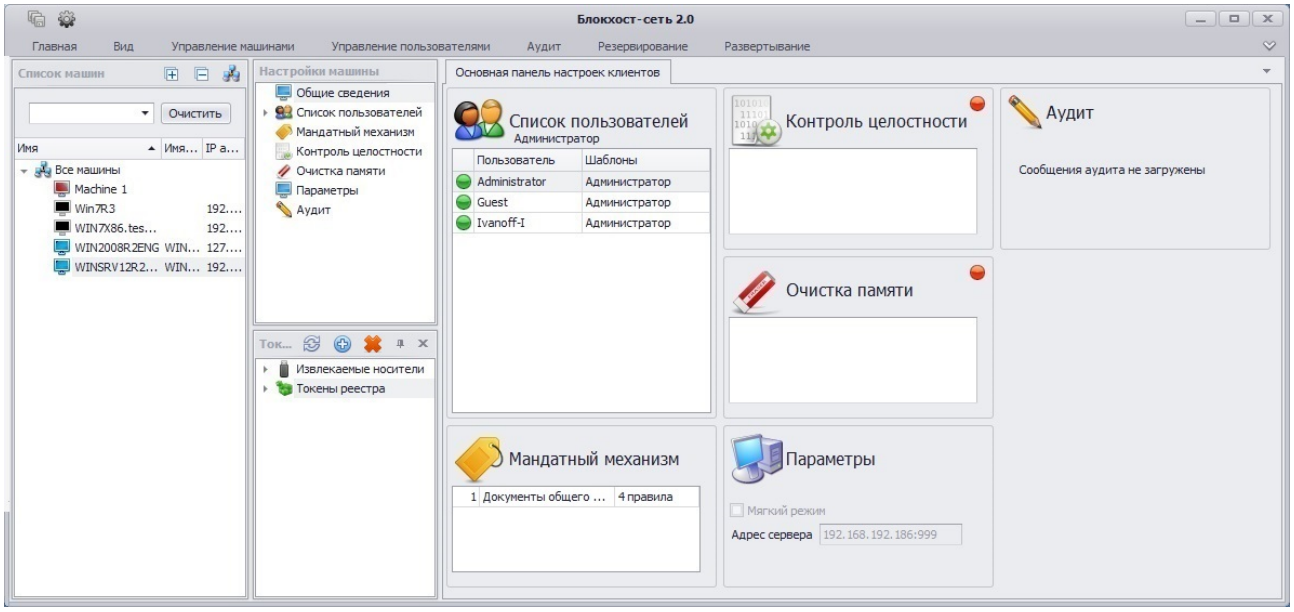
Механизм мягкого режима предназначен для полного и точного определения списка ресурсов, используемых пользователями при выполнении своих повседневных обязанностей. Данный механизм позволяет получить сведения для выявления ошибок в настройках СЗИ и корректировки правил разграничения доступа.

Механизм мягкого режима функционирует при настройках СЗИ, планируемых к использованию в рамках сформированной политики безопасности. Работа данного механизма заключается в разрешении доступа пользователей к ресурсам, запрещенным настройками СЗИ с фиксацией всех запрещенных попыток доступа. Фиксация осуществляется механизмом регистрации событий, связанных с безопасностью защищаемой информации. Администратор безопасности должен выявить ресурсы, которые необходимо добавить в список разрешенных для данного пользователя и на основе полученных данных выполнить корректировку настроек СЗИ.

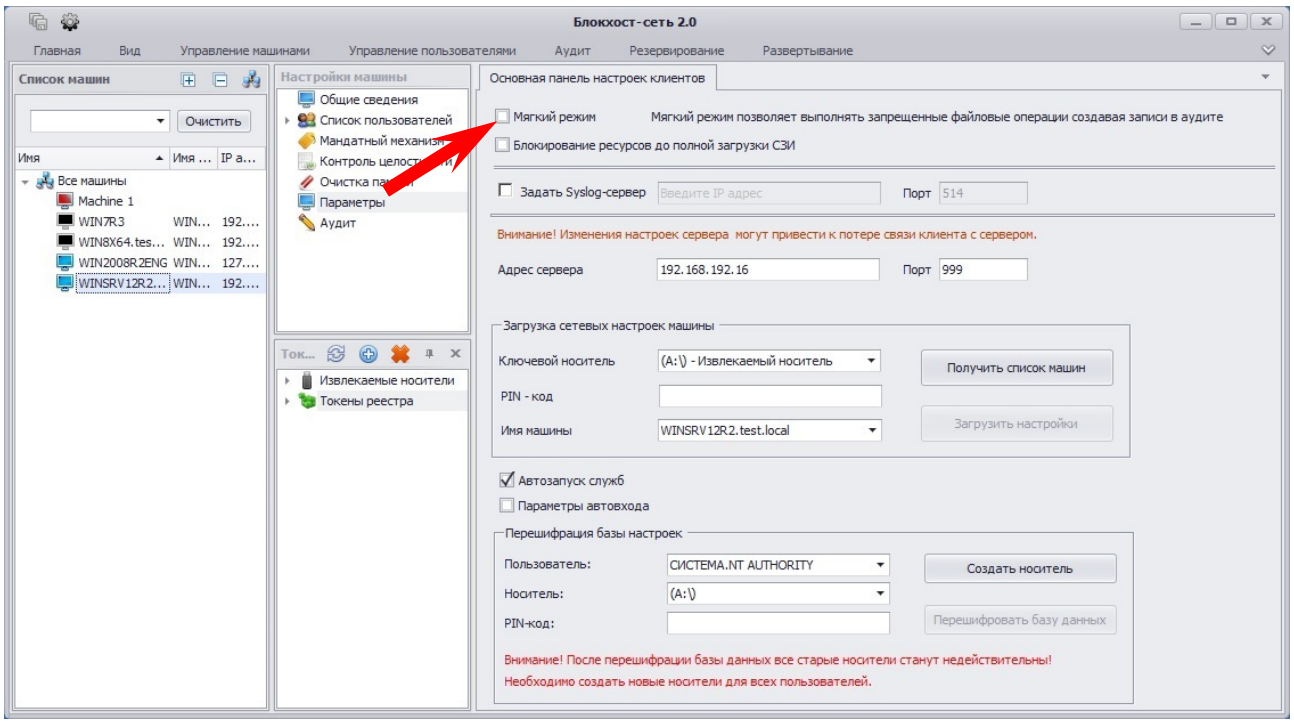
6.2.4.1. Порядок использования механизма мягкого режима

Для включения (отключения) механизма мягкого режима администратор безопасности должен выполнить следующие действия:

1. В окне **«Список машин»** серверной консоли администрирования, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма мягкого режима.
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Параметры*** (рис. 6.66, а) или в окне **«Настройки машины»** выбрать пункт ***Параметры***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.66, б).
3. В **Основной панели настроек клиентов** включить (отключить) механизм мягкого режима, выбрав пункт ***Мягкий режим*** (рис. 6.66, б).



а)



б)

Рисунок 6.66. Включение «Мягкого режима»

4. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Работоспособность компонентов СЗИ «Блокхост-сеть 2.0» при включенном механизме мягкого режима после входа пользователя в ОС приведена в таблице 6.2.4.

Таблица 6.2.4. – Работоспособность компонентов СЗИ «Блокхост-сеть 2.0» при включенном механизме мягкого режима

Наименование компонента	**Мягкий режим (обычный пользователь)**
Дискреционный доступ	не активен
Контроль портов	не активен
Контроль процессов	не активен
Временные ограничения	не активен
Персональный экран	не активен
Контроль печати	не активен
Мандатный доступ	не активен
Контроль целостности	не активен
Очистка памяти	не активен
Регистрация событий (аудит)	активен

Необходимо обратить внимание, что при неактивных в мягком режиме компонентах СЗИ субъекты смогут получать доступ к защищаемым ресурсам, а при нарушении субъектами заданных правил разграничения доступа защищаемая информация может быть утрачена.

6.2.5. Механизм идентификаторов входа

Задача встроенного в серверную часть СЗИ механизма управления идентификаторами заключается в возможности администрирования всех ключевых

носителей (eToken, SafeNet eToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, Avest Token, ruToken, ESmart Token, USB-накопитель, дискета или персональный идентификатор в реестре), которые используются в системе СЗИ «Блокхост-сеть 2.0».

Каждому пользователю может быть сопоставлен один или более ключевых носителей, идентификация пользователя будет осуществляться по SID (данные о привязке пользователя, носителя и рабочей станции хранится на носителе и в базе настроек СЗИ рабочей станции). Данные о привязке носителя к пользователю хранятся в БД СЗИ каждой локальной станции.

Администратор имеет возможность редактировать любой носитель, даже если он не присвоен пользователям на данной машине, в специальном разделе, где будут отображаться пользователи, ассоциированные с данным идентификатором, и машины, с которыми ассоциируется носитель.

Отображение доступных идентификаторов входа осуществляется в окне **«Токены сервера»** или **«Токены <имя_рабочей_станции>»** консоли администрирования СЗИ. (рис. 6.67). В окне **«Токены сервера»** отображаются персональные идентификаторы, подключенные к серверу СЗИ. Данное окно отображается, если в окне **«Список машин»** выделена какая-либо группа (в примере на рис. 6.67 – выделена группа по умолчанию ***Все машины***).

Окно **«Токены <имя_рабочей_станции>»** отображается, если в окне **«Список машин»** выделена контролируемая рабочая станция. В окне **«Токены <имя_рабочей_станции>»** отображены токены, которые подключены к контролируемой рабочей станции.

Механизм идентификаторов входа позволяет:

- Получать информацию по носителю;
- Менять PIN-код доступа к ключевому носителю;
- Отвязывать пользователей от носителя;
- Отвязать носитель от рабочей станции;
- Задать время жизни носителя;
- Сохранить настройки носителя в файл;
- Загрузить настройки носителя из файла на носитель;
- Создать персональный идентификатор в реестре ОС Windows;
- Удалить идентификатор в реестре ОС Windows.

Для получения доступа к настройкам ключевого носителя необходимо пройти процедуру авторизации. Для этого в окне **«Токены сервера»** (**«Токены <имя_рабочей_станции>»**) серверной консоли администрирования СЗИ следует раскрыть ветку типа ключевого носителя, щелкнуть по имени носителя, в появившемся окне ввести PIN-код доступа к нему и нажать кнопку ***Вход***:

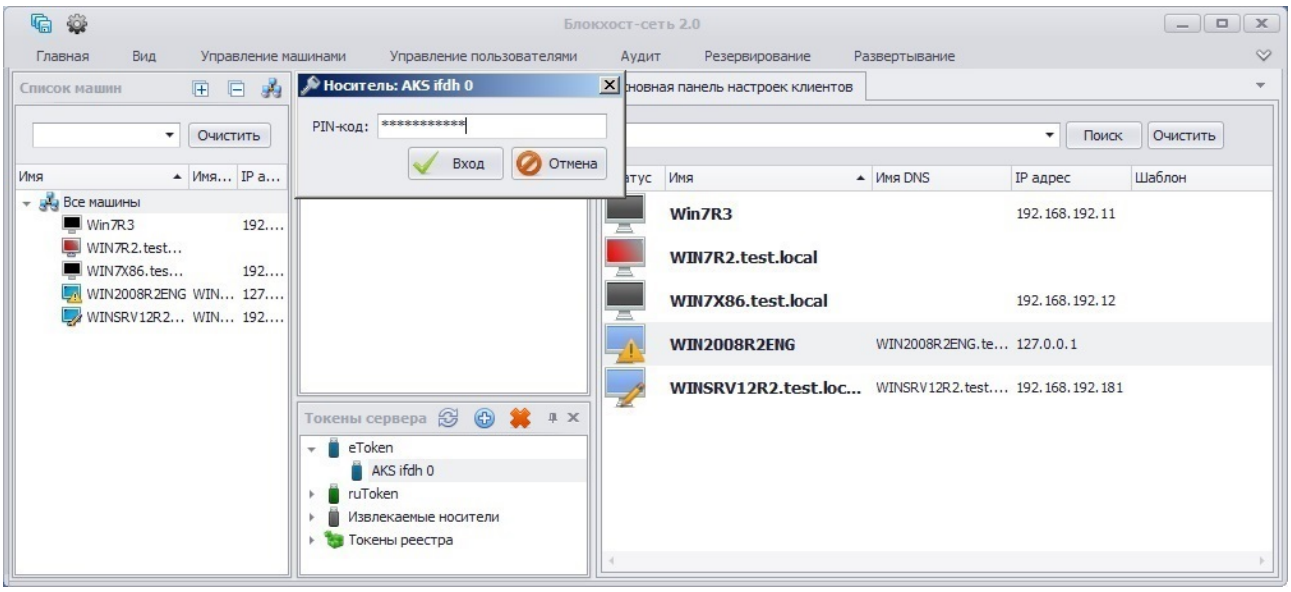


Рисунок 6.67. Авторизация для доступа к настройкам ключевого носителя

Если введен корректный PIN-код, то откроется вкладка **Настройки токена** (рис. 6.68). Во вкладке **Настройки токена** расположена вся информация о носителе (тип носителя, его идентификатор, оставшееся свободное место, размер настроек, период действия). В нижней части вкладки находится список рабочих станций и пользователей, привязанных к выбранному носителю. Переключатель ***Машины с пользователями ↔ Пользователи с машинами*** позволяет настроить сортировку списка, привязанных к носителю субъектов, по рабочим станциям или пользователям соответственно. В списке привязанных к носителю субъектов рабочие станции и пользователи могут отображаться как неизвестные (см. рис. 6.68). Это может быть связано с тем, что настройки рабочей станции, субъекты которой привязаны к выбранному носителю, не были загружены во время текущего сеанса работы администратора безопасности в консоли администрирования СЗИ, или привязка указанных объектов/субъектов к выбранному носителю производилась на другом сервере СЗИ.

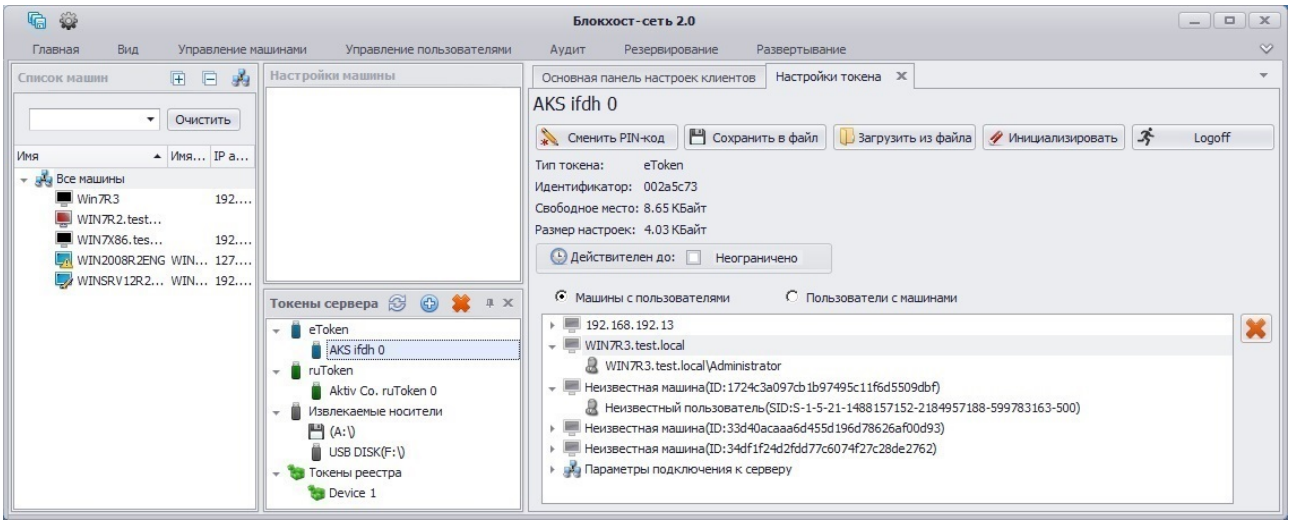


Рисунок 6.68. Окно настроек идентификатора входа

Смена PIN-кода доступа к ключевому носителю

Для смены PIN-кода доступа к ключевому носителю необходимо нажать кнопку ***Сменить PIN-код*** во вкладке **Настройки токена**. В открывшемся окне (рис. 6.69) ввести

новое значение PIN-кода доступа к ключевому носителю и его подтверждение в соответствующие поля и нажать кнопку ***Изменить***. В результате PIN-код доступа к носителю будет изменен.

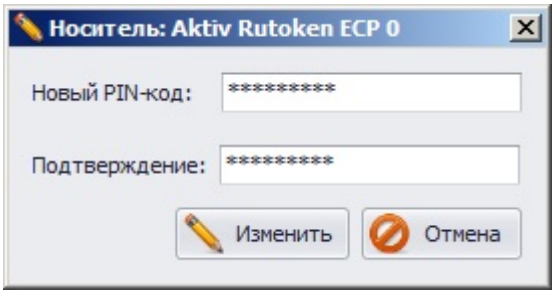


Рисунок 6.69. Изменение PIN-кода ключевого носителя

При изменении PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] `{ } ( ) < >. При изменении PIN-кода пользователем самостоятельно, с применением драйверов персонального идентификатора, использование символов русского алфавита и спецсимволов не запрещается.

Сохранение настроек ключевого носителя в файл

Для сохранения настроек ключевого носителя в файл администратору безопасности необходимо:

1. Во вкладке **Настройки токена** (см. рис. 6.68) нажать кнопку ***Сохранить в файл***;
2. В открывшемся окне **«Сохранение настроек токена»** (рис. 6.70):
   - ввести пароль, с применением которого будет зашифрован файл настроек токена;
   - указать имя сохраняемого файла и выбрать каталог его размещения. Для этого нажать кнопку ***Выбор пути***, в открывшемся стандартном окне Windows **«Сохранить как»** выбрать каталог размещения и ввести имя файла настроек;
   - нажать кнопку ***Сохранить***.

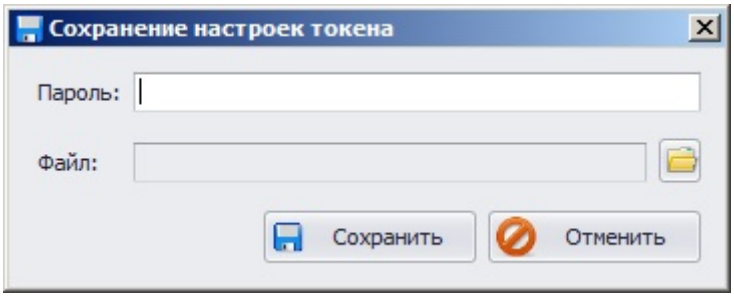


Рисунок 6.70. Окно сохранения настроек ключевого носителя

В результате в выбранном каталоге будет сохранен файл с указанным именем, в котором в зашифрованном виде содержится информация о настройках ключевого носителя.

Процедура сохранения настроек ключевого носителя в файл может понадобиться, например, для резервирования настроек ключевого носителя администратора безопасности сервера СЗИ. В случае неисправности действующего носителя администратора безопасности для его восстановления необходимо будет загрузить сохраненный файл настроек этого ключевого носителя на новый носитель.

Загрузка настроек на ключевой носитель из файла

Для восстановления настроек ключевого носителя администратору безопасности необходимо:

Во вкладке **Настройки токена** (см. рис. 6.68) нажать кнопку ***Загрузить из файла***;

В открывшемся окне **«Восстановление настроек токена»**:

- ввести пароль, с применением которого был зашифрован файл настроек;
- указать каталог размещения и имя файла, в котором были зарезервированы настройки ключевого носителя. Полный путь к файлу настроек ключевого носителя можно ввести вручную в поле ***Файл*** или, воспользовавшись кнопкой ***Выбор пути***, указать необходимые данные в стандартном окне Windows **«Открыть»**;
- нажать кнопку ***Восстановить***.

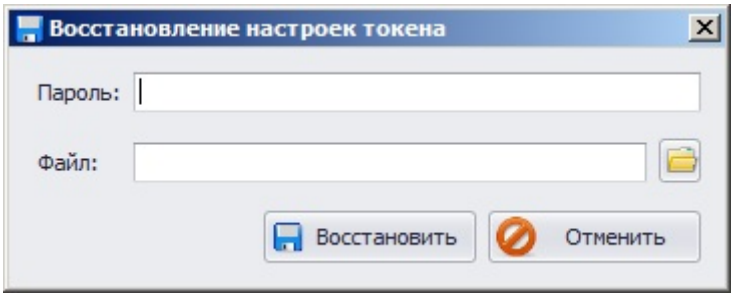


Рисунок 6.71. Окно восстановления настроек ключевого носителя

В результате на ключевой носитель будут загружены настройки, содержавшиеся на ключевом носителе, с которого они были скопированы в файл.

Возможность загрузки настроек из файла существует только для ключевых носителей одного типа.

Инициализация ключевого носителя

Кнопка ***Инициализировать***, расположенная во вкладке **Настройки токена**, служит для очистки области памяти персонального идентификатора, в которой расположены настройки СЗИ «Блокхост-сеть 2.0». При этом с носителя удаляется только информация, связанная с привязкой к носителю пользователей и сгенерированные рабочие станции. Никакая другая информация (например, файлы пользователя с отчуждаемых носителей или закрытые ключи сертификатов) не удаляется. Также при операции инициализации из вкладки **Настройки токена** не изменяется PIN-код и имя ключевого носителя.

Срок действия ключевого носителя

Параметр ***Действителен до*** вкладки **Настройка токена** (см. рис. 6.68) позволяет указать дату, после которой пользователь не сможет войти в систему с данным носителем. Для установки даты окончания действия ключевого носителя необходимо отметить параметр ***Действителен до*** и ввести в появившееся поле дату. Возможно два варианта ввода даты окончания срока действия ключевого носителя:

- вручную в формате *ДД.ММ.ГГГГ*;
- выбрать необходимую дату в окне календаря (рис 6.72), который появляется после нажатия на кнопку раскрытия списка поля даты.

По умолчанию срок действия персонального идентификатора пользователя не ограничен.

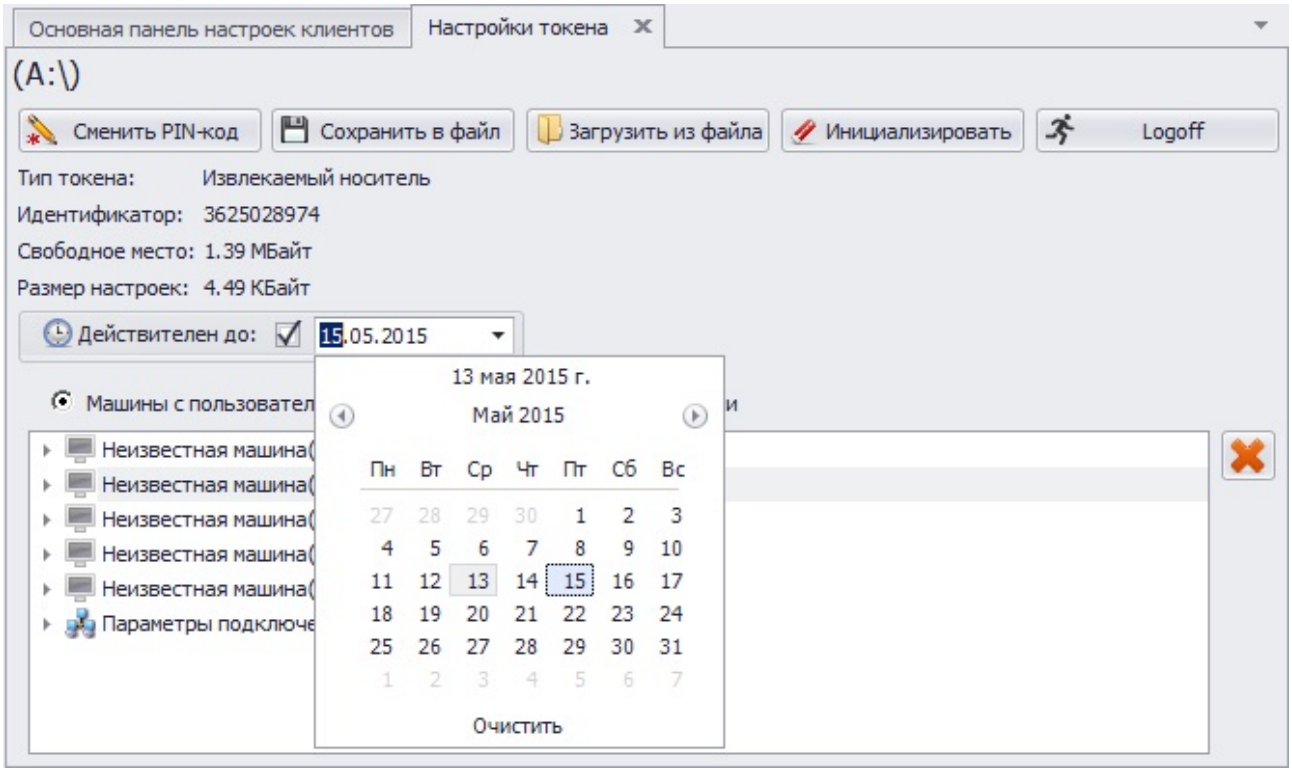


Рисунок 6.72. Время жизни носителя

Редактирование списка субъектов, привязанных к ключевому носителю

Для удаления пользователя из списка привязанных к выбранному ключевому носителю необходимо во вкладке **Настройки токена** (см. рис. 6.68) выбрать параметр ***Пользователи с машинами***. В результате отобразится список пользователей, привязанных к носителю. Затем необходимо выделить удаляемого пользователя и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Отвязать*** , находящейся справа от списка пользователей). В результате с носителя будут удалены сведения о привязке пользователя к выбранному носителю. При этом рабочая станция (или несколько рабочих станций), на которую имел право входа, с использованием редактируемого носителя, удаленный пользователь, останется на носителе.

Для удаления рабочей станции из списка привязанных к ключевому носителю необходимо во вкладке **Настройки токена** (см. рис. 6.68) выбрать параметр ***Машины с пользователями***. В результате отобразится список рабочих станций, пользователи которых привязаны к носителю. Затем необходимо выделить удаляемую рабочую станцию и нажать клавишу **<Del>** (или воспользоваться кнопкой ***Отвязать*** , находящейся справа от списка машин). При удалении рабочей станции из списка привязанных к ключевому носителю, все пользователи, имевшие право входа на эту рабочую станцию с редактируемым ключевым носителем, также будут удалены с этого носителя.

Если ключевой носитель использовался для генерации рабочих станций на сервере СЗИ, то сведения о сгенерированных рабочих станциях также отображаются во вкладке **Настройки токена** – в этом случае в списке привязанных к носителю пользователей появляется раскрываемый список ***Параметры подключения к серверу***. Данный список доступен при любом положении переключателя отображения списка привязанных к носителю субъектов – ***Машины с пользователями*** или ***Пользователи с машинами***.

Для удаления сгенерированных на редактируемый носитель, но не подключенных к серверу СЗИ, рабочих станций необходимо во вкладке **Настройки токена** раскрыть дерево ***Параметры подключения к серверу*** (рис. 6.73). Затем необходимо выбрать удаляемую рабочую станцию и нажать кнопку кнопку ***Отвязать***  , находящуюся справа от списка машин или воспользоваться клавишей **<DEL>**.

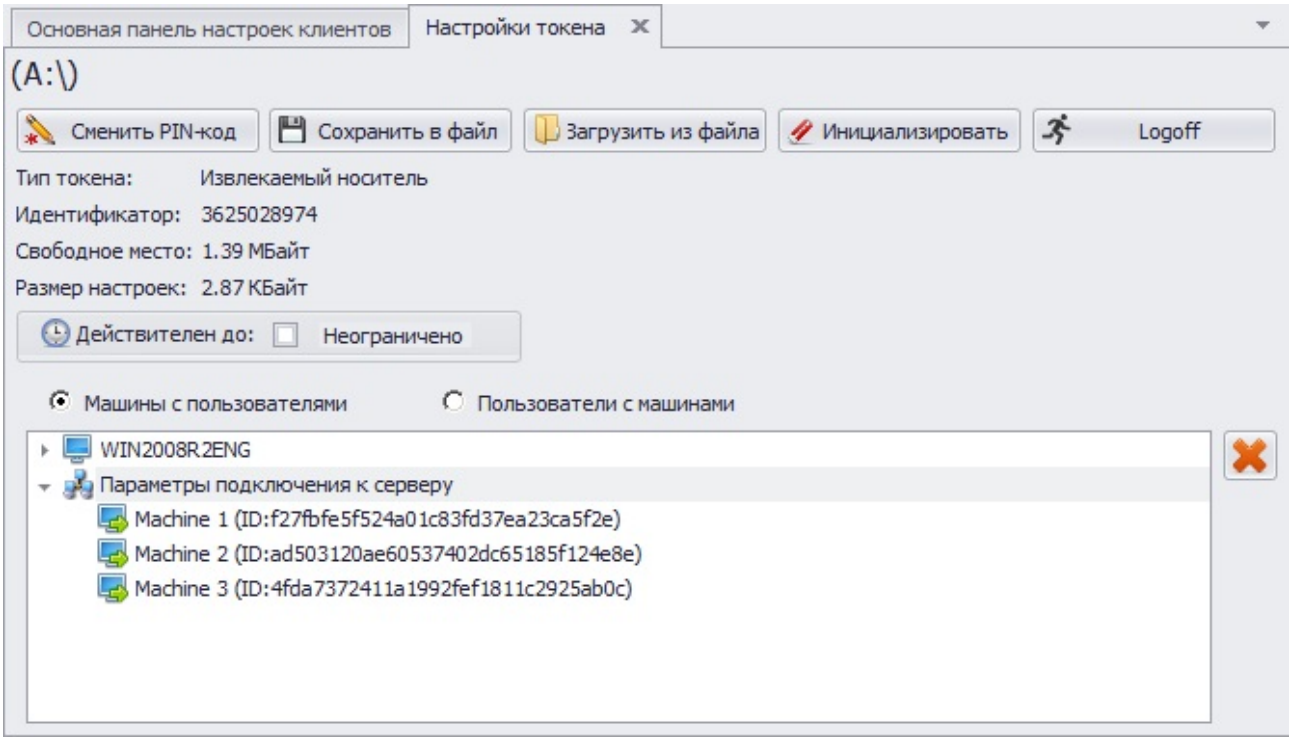


Рисунок 6.73. Список сгенерированных на сервере СЗИ рабочих станций

Создание персонального идентификатора в реестре ОС Windows

Для создания персонального идентификатора в реестре ОС Windows администратору безопасности необходимо:

1. В окне **«Список машин»** выбрать рабочую станцию, в реестре которой будет создан персональный идентификатор;

2. В окне **«Токены <имя рабочей станции>»** нажать кнопку ***Создать токен в реестре***  ;

3. В открывшемся окне **«Создание нового токена в реестре»** ввести PIN-код доступа к создаваемому идентификатору в реестре и нажать кнопку ***Создать***:

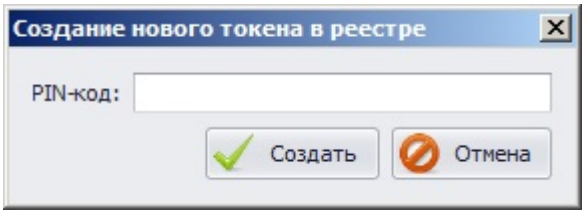


Рисунок 6.74. Окно создания персонального идентификатора в реестре

При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] ` { } ( ) < >.

4. В результате в реестре редактируемой рабочей станции будет создан персональный идентификатор с именем по умолчанию *Device 1*:

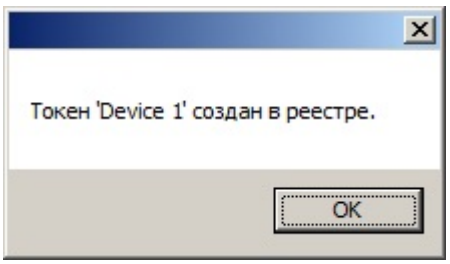


Рисунок 6.75. Информационное окно об успешном создании идентификатора в реестре

Если в реестре рабочей станции уже существует персональный идентификатор с именем *Device 1*, то будет создан идентификатор, содержащий в своем имени следующий порядковый номер – 2 и т.д.

После создания персонального идентификатора в реестре, щелкнув по его имени в окне **«Токены <имя рабочей станции>»**, можно без ввода PIN-кода перейти во вкладку **Токены**, где сразу же отредактировать его свойства: изменить PIN-код доступа к нему, загрузить на него сохраненные в файле настройки ключевого носителя, ограничить время использования идентификатора.

Удаление персонального идентификатора из реестра ОС Windows

Для удаления персонального идентификатора из реестра ОС Windows администратору безопасности необходимо:

1. В окне **«Список машин»** выбрать рабочую станцию, персональный идентификатор в реестре которой будет удаляться;

2. В окне **«Токены <имя рабочей станции>»** нажать кнопку ***Удалить токен из реестра***  ;

3. Из раскрывающегося списка поля ***Токен реестра*** открывшегося окна **«Удаление токена из реестра»** выбрать имя удаляемого идентификатора и нажать кнопку ***Удалить***:

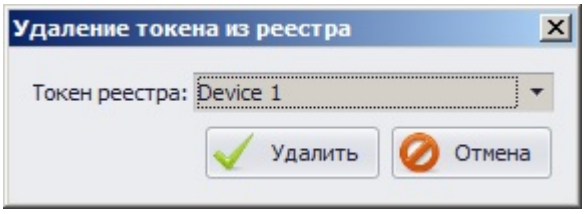


Рисунок 6.76. Окно удаления персонального идентификатора в реестре ОС Windows

4. В результате из реестра редактируемой рабочей станции будет удален выбранный персональный идентификатор в реестре ОС Windows:

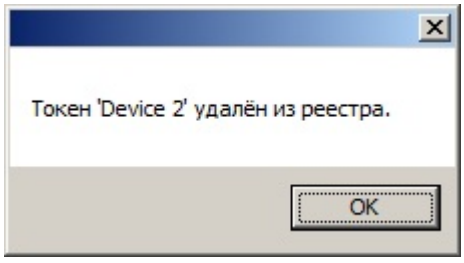


Рисунок 6.77. Информационное окно об успешном удалении идентификатора из реестра

6.2.6. Редактирование БД СЗИ «Блокхост-сеть 2.0»

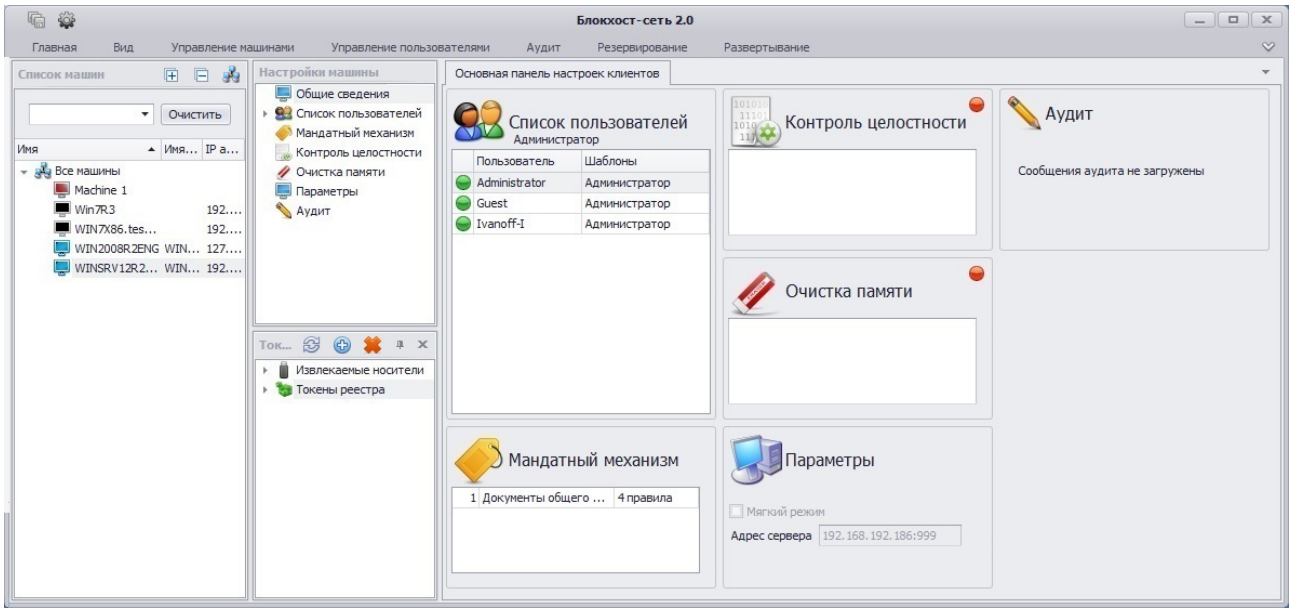
При установке клиентской части СЗИ «Блокхост-сеть 2.0» на контролируемую рабочую станцию, с указанием параметров подключения к серверу СЗИ, с использованием

групповых политик или из вкладки **Развертывание MSI пакетов** серверной консоли в список пользователей БД СЗИ добавляются все локальные пользователи рабочей станции, а также учетные записи доменных пользователей, профили которых существуют на рабочей станции. Также в процессе такой установки происходит создание персонального идентификатора в реестре ОС Windows, задается PIN-код доступа к нему, и этот идентификатор присваивается всем пользователям, созданным в процессе установки СЗИ на контролируемую рабочую станцию.

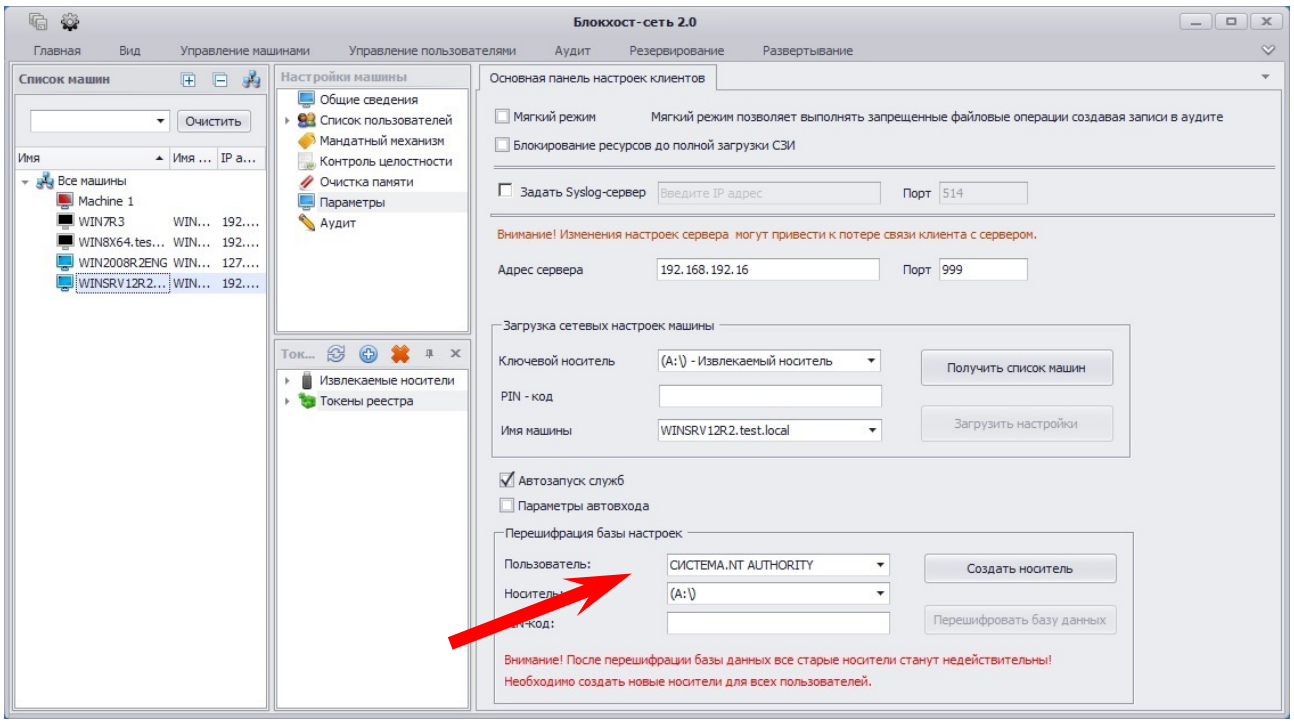
Ситуация, при которой все пользователи используют один персональный идентификатор в качестве средства аутентификации для доступа к рабочей станции, является не правильной с точки зрения обеспечения защиты информации, обрабатываемой на этой рабочей станции. Для возможности единовременной и полной очистки базы данных пользователей в СЗИ на контролируемой рабочей станции служит механизм ***Перешифрации базы настроек СЗИ***.

Для того чтобы очистить сведения о присвоенных на контролируемой рабочей станции пользователям ключевых носителях администратору безопасности в серверной консоли администрирования СЗИ необходимо выполнить следующие действия:

1. В окне **«Список машин»**, раскрыв пункт ***Все машины***, выбрать рабочую станцию, база настроек СЗИ которой будет перешифровываться;
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Параметры*** (рис. 6.78, а) или в окне **«Настройки машины»** выбрать пункт ***Параметры***. В обоих случаях в **Основной панели настроек клиентов** откроются параметры редактируемой рабочей станции (рис. 6.78, б);
3. В **Основной панели настроек клиентов** в области *Перешифрация базы настроек* (рис. 6.78, б) из выпадающего списка поля ***Пользователь*** выбрать учетную запись администратора безопасности, из выпадающего списка ***Носитель*** выбрать персональный идентификатор АБ, заранее подключенный к серверу СЗИ, и ввести PIN-код доступа к выбранному персональному идентификатору в поле ***PIN-код***;



а)



б)

Рисунок 6.78. Отображение вкладки «Параметры» контролируемой рабочей станции

4. Затем нажать кнопку ***Создать носитель***. В случае успешного добавления персонального идентификатора появится окно с соответствующим сообщением:

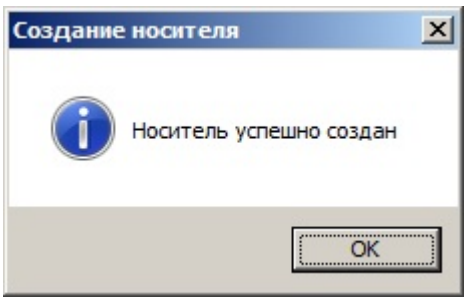


Рисунок 6.79. Информационное окно «Создание носителя»

5. При необходимости следует повторить операцию добавления персонального идентификатора для каждого пользователя, зарегистрированного в СЗИ «Блокхост-сеть 2.0», на контролируемом АРМ;
6. Затем для очистки базы настроек СЗИ нажать кнопку ***Перешифровать базу данных***. В случае успешной операции очистки БД СЗИ появится окно с соответствующим сообщением:

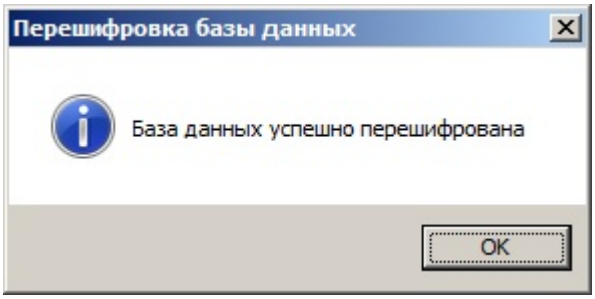


Рисунок 6.80. Информационное окно «Перешифровка базы данных»

7. Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

После сохранения настроек администратор безопасности сможет войти на удаленную рабочую станцию, используя новый идентификатор.

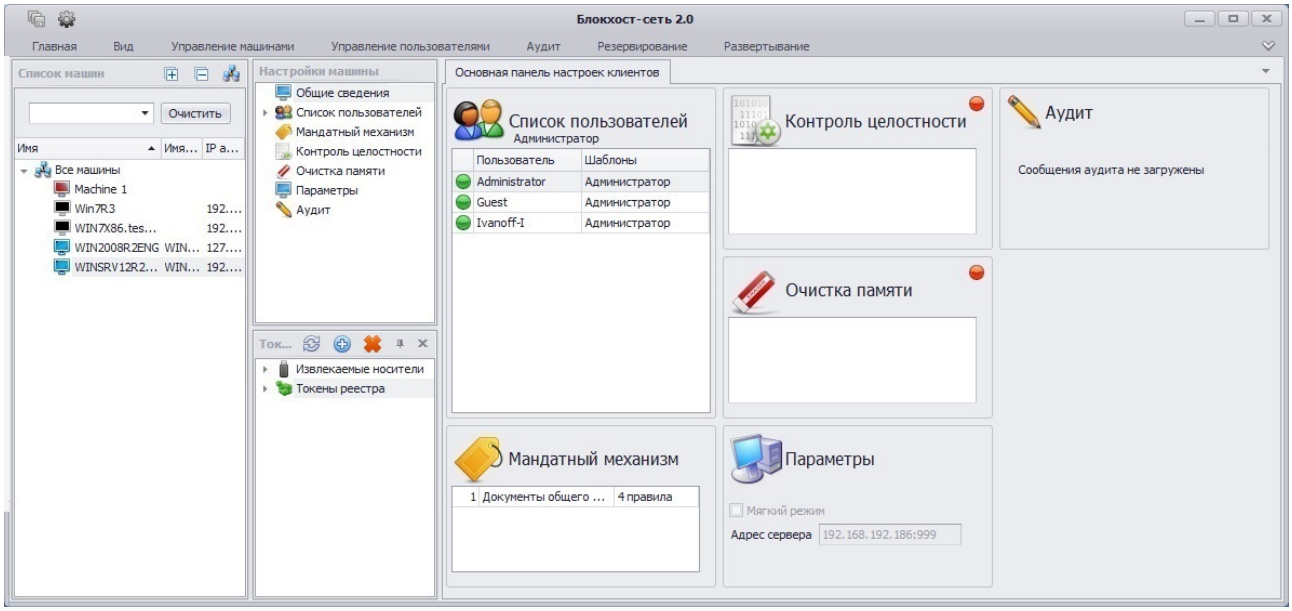
Операция очистки базы данных СЗИ влечет за собой уничтожение всей информации о ранее присвоенных носителях пользователей удаленной рабочей станции. Поэтому необходимо заново присвоить персональные идентификаторы всем пользователям контролируемой РС.

6.2.7. Автоматический запуск служб СЗИ «Блокхост-сеть 2.0»

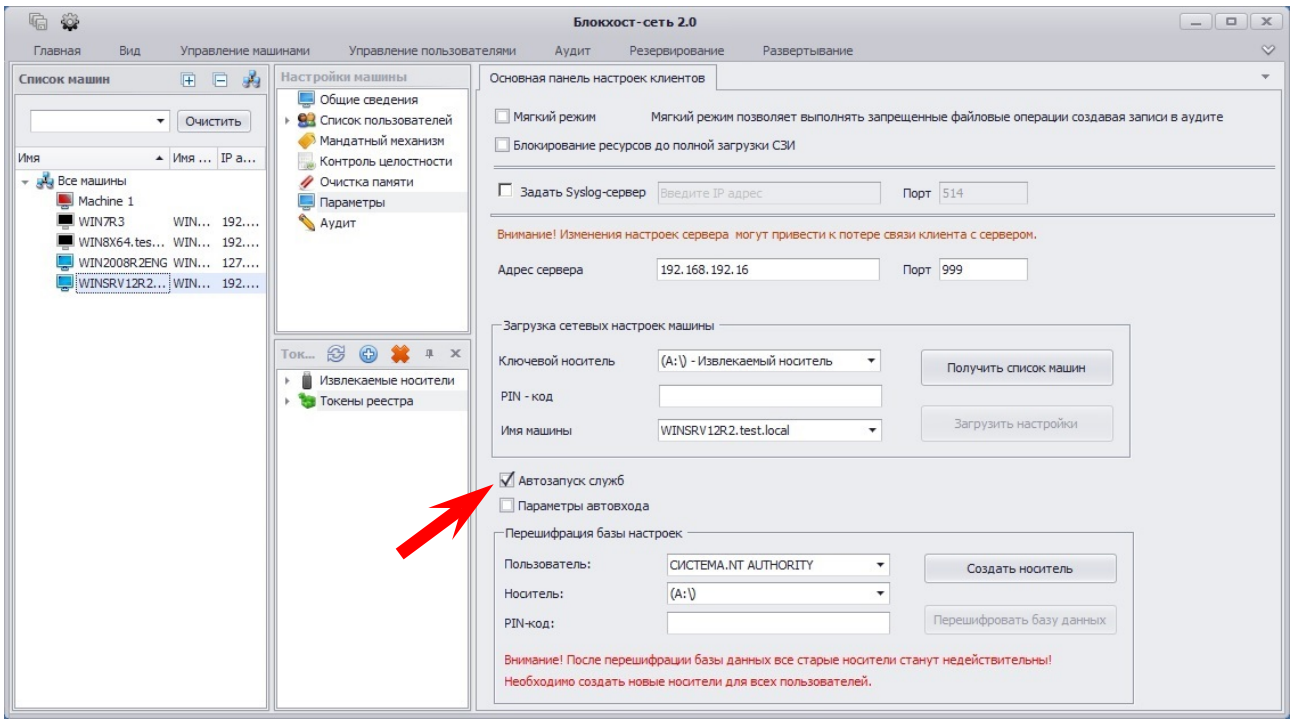
В СЗИ «Блокхост-сеть 2.0» существует возможность автоматического запуска служб СЗИ при старте ОС Windows до момента входа в нее пользователя. Параметр, отвечающий за автоматический запуск служб СЗИ на контролируемой рабочей станции, можно установить в серверной консоли администрирования СЗИ.

Для того, чтобы включить возможность автоматического запуска служб СЗИ на контролируемой рабочей станции администратору безопасности необходимо выполнить следующие действия в серверной консоли администрирования СЗИ:

1. В окне **«Список машин»**, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет настраиваться автоматический запуск служб СЗИ;
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Параметры*** (рис. 6.81, а) или в окне **«Настройки машины»** выбрать пункт ***Параметры***. В обоих случаях в **Основной панели настроек клиентов** откроются параметры редактируемой рабочей станции (рис. 6.81, б);



а)



б)

Рисунок 6.81. Отображение вкладки «Параметры» контролируемой рабочей станции

3. В **Основной панели настроек клиентов** (рис. 6.81, б) отметить параметр ***Автозапуск служб***.

При установке параметра ***Автозапуск служб*** в серверной консоли администрирования СЗИ, на редактируемой рабочей станции в защищенной области реестра создается параметр *BHStorage*, в котором содержится ключ, с использованием которого происходит запуск служб СЗИ. В этом случае сохранять произведенные на контролируемой рабочей станции изменения нет необходимости.

В результате этих действий основные службы СЗИ на рабочей станции будут запущены до входа в ОС Windows пользователя. При работе служб СЗИ становится возможным управление настройками СЗИ на контролируемой рабочей станции из серверной консоли администрирования, а также доступ ресурсам к рабочей станции по сети, зарегистрированных в СЗИ пользователей.

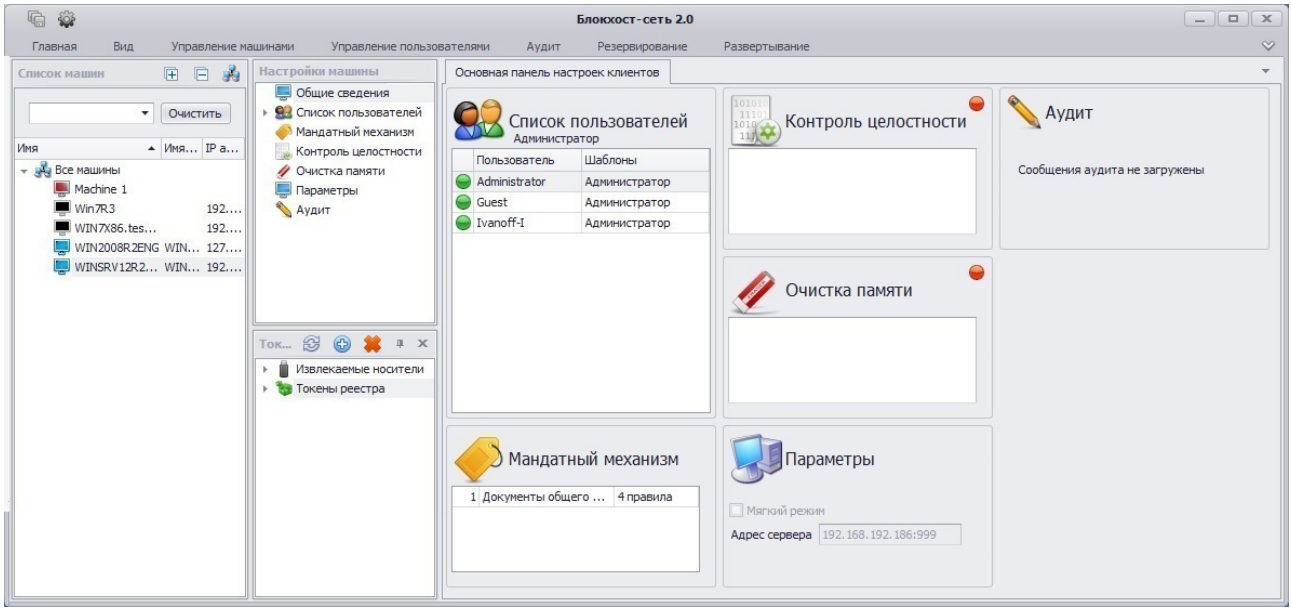
6.2.8. Блокировка сетевых ресурсов рабочей станции

В СЗИ «Блокхост-сеть 2.0» реализована возможность блокировки сетевых ресурсов контролируемой рабочей станции до входа в ее систему пользователей. Такая блокировка может понадобиться для запрета доступа к ресурсам рабочей станции при ее возможной аварийной перезагрузке в момент отсутствия рядом с ней пользователя. Для запрета доступа пользователей к ресурсам рабочей станции до входа в ее систему авторизованного пользователя, администратору безопасности необходимо в серверной консоли администрирования СЗИ выполнить следующие действия:

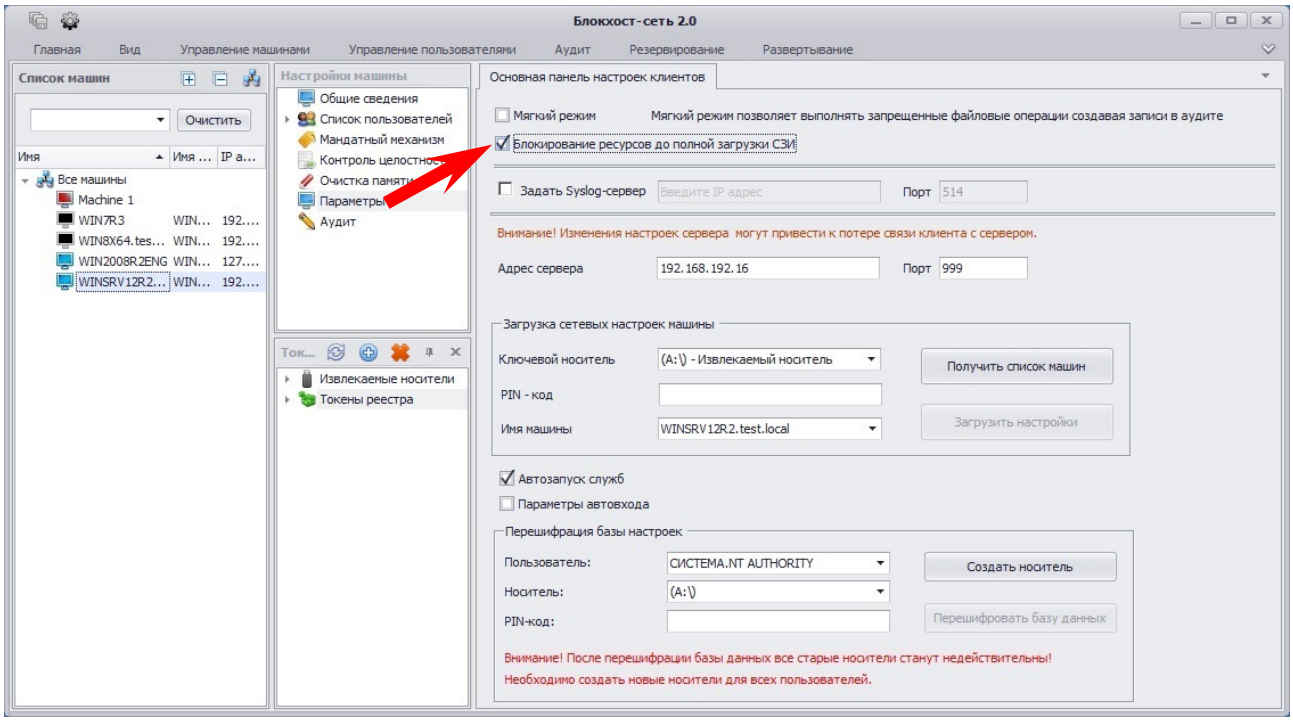
1. В окне **«Список машин»**, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет настраиваться автоматический запуск служб СЗИ;
2. В **Основной панели настроек клиентов** щелкнуть по названию ***Параметры*** (рис. 6.82, а) или в окне **«Настройки машины»** выбрать пункт ***Параметры***. В

обоих случаях в **Основной панели настроек клиентов** откроются параметры редактируемой рабочей станции (рис. 6.82, б);

3. В **Основной панели настроек клиентов** (рис. 6.82, б) отметить параметр ***Блокирование ресурсов до полной загрузки СЗИ***.



а)



б)

Рисунок 6.82. Отображение вкладки «Параметры» контролируемой рабочей станции

В результате этих действий доступ к сетевым ресурсам контролируемой рабочей станции до входа в ее систему авторизованного пользователя будет запрещен всем, в том числе и пользователям, входящим в список пользователей рабочей станции. После входа в ОС рабочей станции авторизованного в СЗИ пользователя доступ к ее ресурсам будет осуществляться в соответствии с установленными настройками механизмов СЗИ.

Блокировка ресурсов рабочей станции до входа в ее ОС пользователя возможна только в случае установленного параметра ***Автозапуск служб***.
Также не блокируется доступ пользователей к ресурсам рабочей станции, если был осуществлен выход пользователя из ОС без ее перезагрузки.

6.2.9. Репликация системных механизмов защиты информации

В СЗИ «Блокхост-сеть 2.0» существует возможность репликации (копирования путем замещения) мандатного механизма СЗИ и механизма очистки памяти настроенного на одной рабочей станции на другие, контролируемые на текущем сервере СЗИ. Использование репликации системных настроек защиты информации позволит администратору безопасности существенно упростить процесс назначения однотипных политик на рабочие станции в сети.

Для того, чтобы реплицировать настройки мандатного механизма СЗИ или механизма очистки памяти администратору безопасности необходимо:

1. В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все машины***, выбрать рабочую станцию, настройки системных механизмов которой будут копироваться;
2. В окне **«Настройки машины»** выделить копируемый механизм (пункт Мандатный механизм или Очистка памяти);
3. Выбрать пункт меню ***Главная →Копировать***. В результате в буфер обмена будут скопированы настройки выбранного механизма СЗИ указанной рабочей станции;
4. Затем в окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все машины***, выбрать рабочую станцию, на которую будут установлены скопированные настройки механизма СЗИ;
5. В окне **«Настройки машины»** выделить пункт ***Общие сведения***;
6. Выбрать пункт меню ***Главная →Вставить***. В результате на обеих рабочих станциях настройки скопированного механизма СЗИ будут идентичны:
7. При необходимости повторить операцию репликации выбранного механизма СЗИ и для других рабочих станций.

Для репликации следующего механизма СЗИ рабочей станции следует заново пройти шаги, описанные в п.п. 1 – 6.

7. Группирование объектов

В серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» существует возможность группировки рабочих станций, подключенных к серверу СЗИ, по логическим группам (например, дирекция, бухгалтерия, группа проектирования и т.п.).

Для активации меню создания групп администратору безопасности необходимо в серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» нажать кнопку ***Показывать группы*** , расположенную в заголовке окна **«Список машин»** (рис. 7.1). В результате станут активными пункты меню ***Управление машинами*** в разделе *Группы*: ***Добавить группу*** и ***Удалить группу***, а также в контекстном меню окна **«Список машин»** появятся пункты по работе с группами:

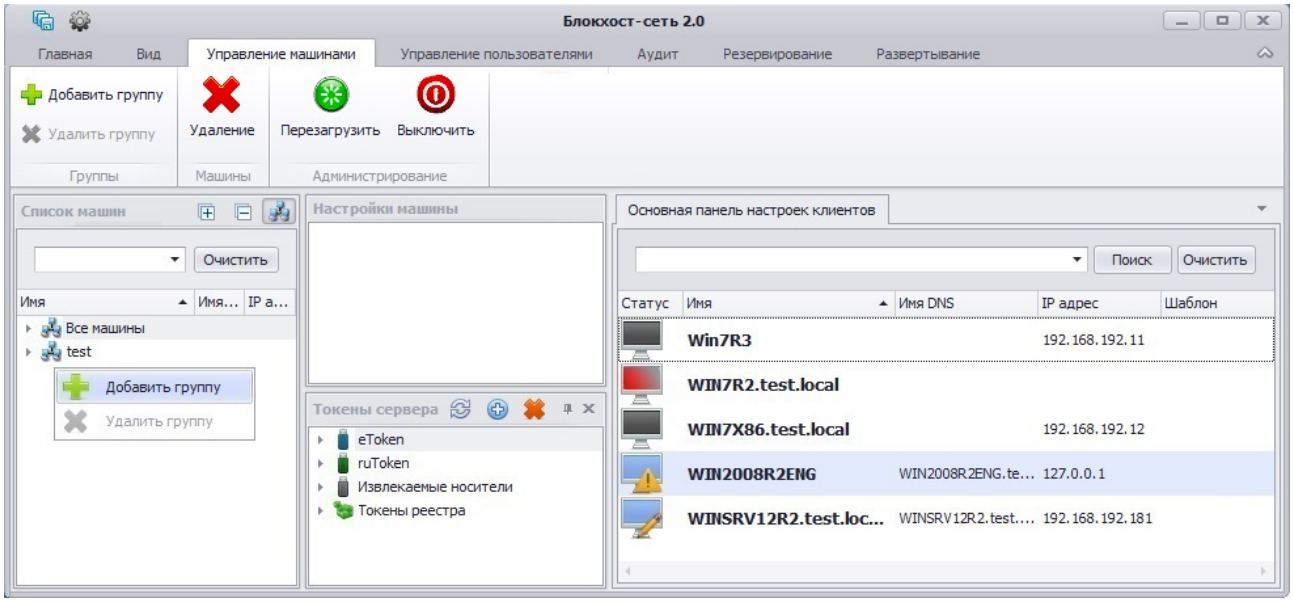


Рисунок 7.1. Меню создания группы объектов

Для создания группы необходимо выбрать пункт меню ***Управление машинами →Добавить группу***, или воспользоваться пунктом контекстного меню ***Добавить группу***, появляющегося при щелчке правой кнопкой мыши в окне **«Список машин»** (см. рис. 7.1) – в окне **«Список машин»** появится группа с именем ***Новая_группа***. Для изменения имени группы необходимо щелкнуть левой кнопкой мыши по ее названию, ввести новое имя и нажать клавишу **<Enter>**.

При определении имени группы необходимо учитывать следующие ограничения:

- имя группы не должно содержать пробелы и символы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] `{ } ( ) < >;
- имя группы не может начинаться с цифры и состоять только из цифр;
- в имени группы запрещено использовать символы русского алфавита.

Для добавления рабочей станции в группу необходимо захватить ее левой кнопкой мыши и, не отпуская кнопку, перетащить рабочую станцию на имя группы (рис. 7.2). Одну и ту же рабочую станцию можно добавить только в одну из созданных групп, при этом она пропадет из группы по умолчанию (***Все машины***). Перетащить рабочую станцию из созданной группы, в группу по умолчанию (***Все машины***) нельзя. Настройки СЗИ, ранее

произведенные на контролируемых рабочих станциях, сохраняются и после перемещения рабочих станций в группы.

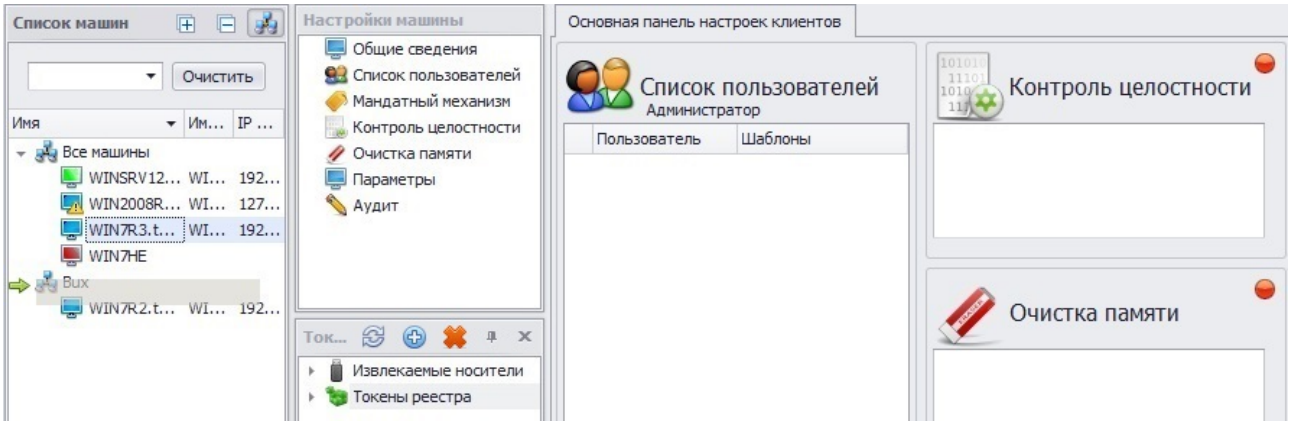


Рисунок 7.2. Перемещение рабочей станции в группу

Для удаления рабочей станции из группы необходимо в окне **«Список машин»** выделить группу, из которой будет удаляться рабочая станция, затем в **Основной панели настроек клиентов** выделить необходимую рабочую станцию и нажать клавишу **<Del>** или воспользоваться пунктом меню ***Управление машинами →Удалить*** , или воспользоваться пунктом контекстного меню ***Удалить из группы*** (рис. 7.3). В результате рабочая станция будет перемещена в группу по умолчанию (***Все машины***). Из группы по умолчанию (***Все машины***) удалить рабочую станцию нельзя – в этом случае пункт контекстного меню ***Удалить из группы*** будет неактивен. Выбор пункта контекстного меню ***Удалить из настроек*** приведет к удалению рабочей станции из списка контролируемых текущим сервером СЗИ.

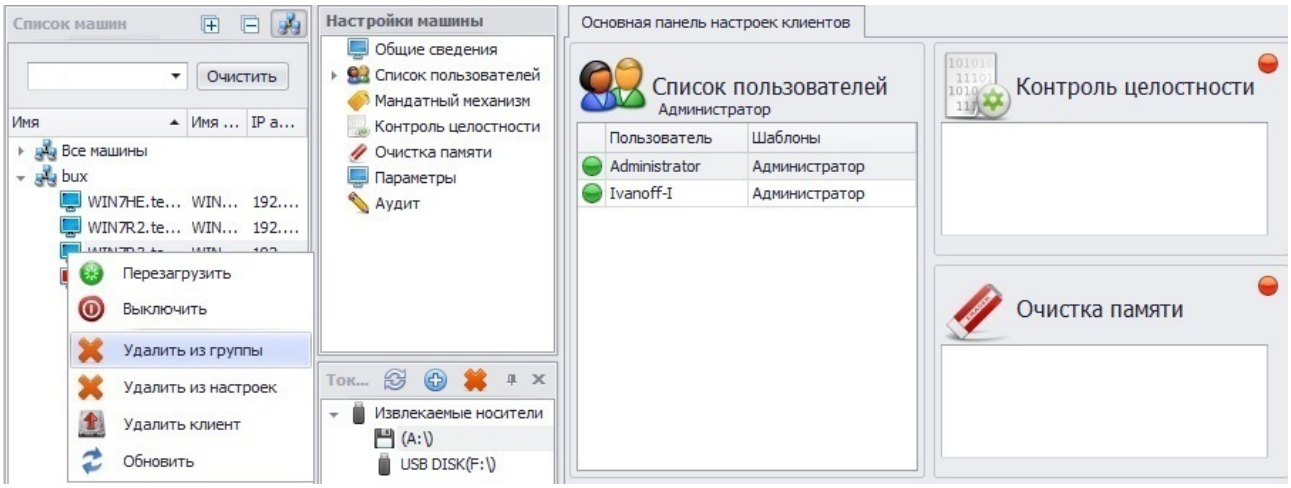


Рисунок 7.3. Удаление рабочей станции из группы

Созданную группу можно удалить. Для этого необходимо выделить ее и нажать клавишу **<Del>** или воспользоваться пунктом меню ***Управление машинами →Удалить группу*** (или выбрать этот же пункт в контекстном меню). При этом находившиеся в удаленной группе рабочие станции останутся на сервере СЗИ и будут перемещены в группу ***Все машины***. Группу ***Все машины*** удалить нельзя.

Для всех групп, за исключением группы по умолчанию ***Все машины***, можно создать вложенные группы. Для этого необходимо выделить группу, в которую будет добавлена новая группа, выбрать пункт меню ***Управление машинами →Добавить группу*** и скорректировать в окне **«Список машин»** имя новой группы.

Удаление родительской группы влечет за собой удаление всех вложенных в нее групп, при этом рабочие станции, находившиеся в этих группах, будут перемещены в группу по умолчанию ***Все машины***.

8. Регистрация событий, связанных с безопасностью защищаемой информации

Механизм регистрации событий СЗИ «Блокхост-сеть 2.0» дополняет механизм аудита операционной системы и осуществляет прием сообщений аудита от компонентов СЗИ «Блокхост-сеть 2.0». Сообщения поступают как при обращении субъектов доступа к защищаемым ресурсам, так и при срабатывании механизмов защиты, встроенных в операционную систему. Из этих сообщений формируются следующие журналы событий:

- Журналы, формируемые средствами операционной системы.
- Журнал СЗИ «Блокхост-сеть 2.0».

Журналы, формируемые средствами операционной системы, содержат сообщения, полученные при срабатывании стандартных механизмов защиты, встроенных в операционную систему. В отличие от этих журналов, журнал СЗИ «Блокхост-сеть 2.0» содержит сообщения о тех событиях, которые могут влиять на безопасность защищаемой информации, но были пропущены механизмом регистрации событий операционной системы. Сообщения журнала аудита СЗИ «Блокхост-сеть 2.0» содержат следующую информацию:

- тип события (успешное или неуспешное);
- дата и время;
- источник записи;
- категория доступа;
- код (ID);
- имя компьютера;
- пользователь;
- метка пользователя;
- имя объекта;
- метка объекта;
- тип доступа;
- привилегии.

Кроме того, в сообщении может содержаться и дополнительная информация, характерная для каждого модуля СЗИ «Блокхост-сеть 2.0».

Настройка параметров аудита и просмотр журнала аудита СЗИ «Блокхост-сеть» на контролируемых рабочих станциях возможны удаленно с серверной консоли СЗИ «Блокхост-сеть 2.0».

Также возможна отправка сообщений аудита СЗИ «Блокхост-сеть 2.0» на внешний Syslog-сервер.

8.1. Настройки аудита

СЗИ «Блокхост-сеть 2.0» регистрирует события, влияющие на безопасность того набора объектов информации, который определил администратор безопасности. Необходимость регистрации событий, связанных с работой СЗИ «Блокхост-сеть 2.0», указывается при настройке правил контроля каждого из механизмов входящих в состав СЗИ. Для включения (отключения) механизма регистрации событий, связанных с безопасностью информации объектов поставленных на контроль, администратор безопасности должен при

настройке механизмов СЗИ установить параметр ***Аудит*** для соответствующего объекта. По умолчанию в серверной консоли администрирования СЗИ включен аудит работы всех механизмов СЗИ.

8.2. Просмотр сообщений аудита

Для просмотра сообщений аудита, содержащихся в журнале СЗИ «Блокхост-сеть 2.0», администратор безопасности может воспользоваться:

- программой просмотра событий операционной системы – через консоль MMC.
- средством просмотра событий серверной консоли администрирования СЗИ «Блокхост-сеть 2.0».

Просмотр событий с помощью средств консоли MMC позволяет осуществлять просмотр всех событий системы. Просмотр событий с помощью средств консоли администрирования СЗИ «Блокхост-сеть 2.0» позволяет осуществлять только просмотр событий, зафиксированных СЗИ «Блокхост-сеть 2.0».

Для просмотра сообщений аудита с помощью консоли MMC администратору безопасности необходимо запустить оснастку ***Просмотр событий*** (в меню ***Пуск*** выбрать пункт ***Панель управления →Администрирование →Просмотр событий***) в открывшемся окне **«Просмотр событий»** перейти к пункту ***Журналы приложений и служб →Блокхост-сеть*** (на рис. 8.1 представлен пример просмотра сообщений СЗИ «Блокхост-сеть 2.0» в англоязычной версии ОС).

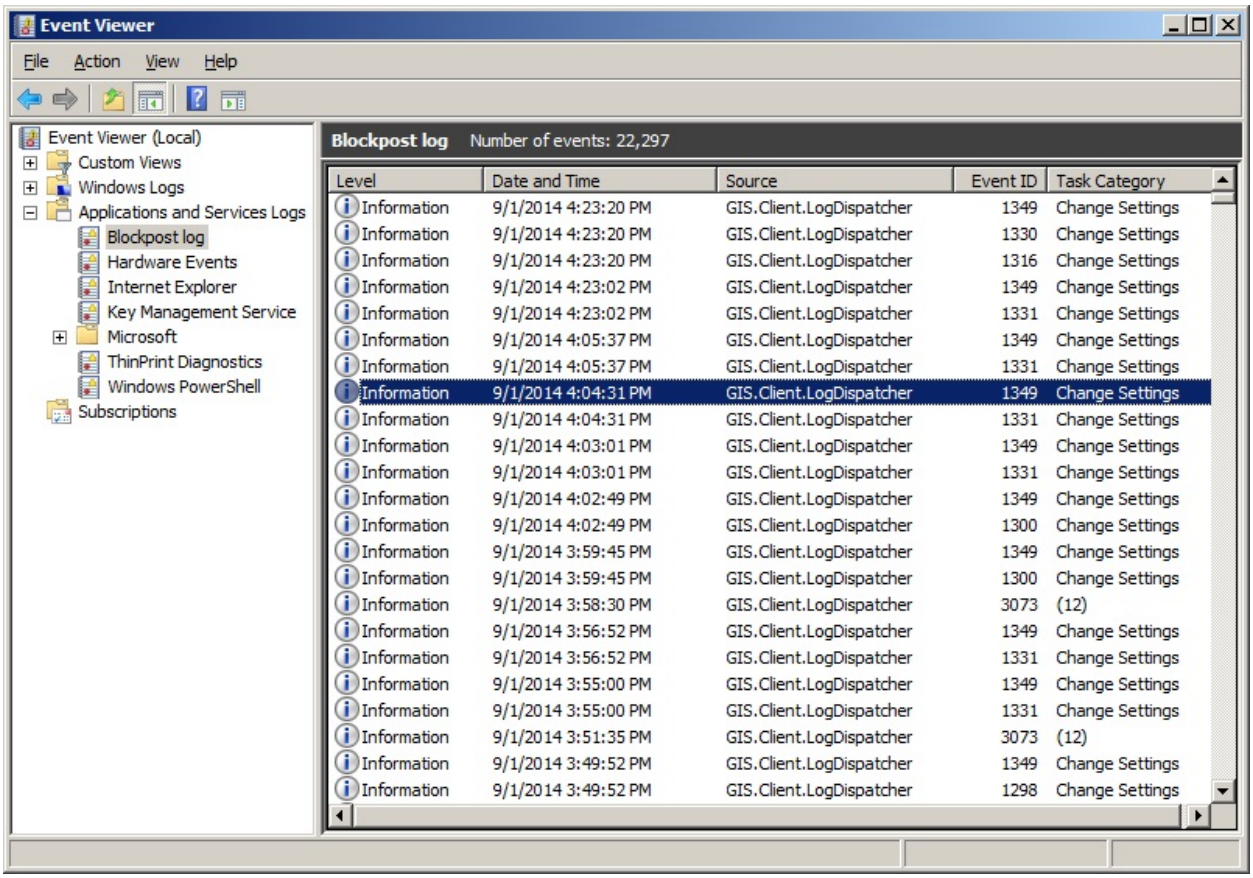


Рисунок 8.1. Окно просмотра аудита с помощью консоли MMC

После двойного щелчка на выбранном событии станет доступным его описание (рис. 8.2).

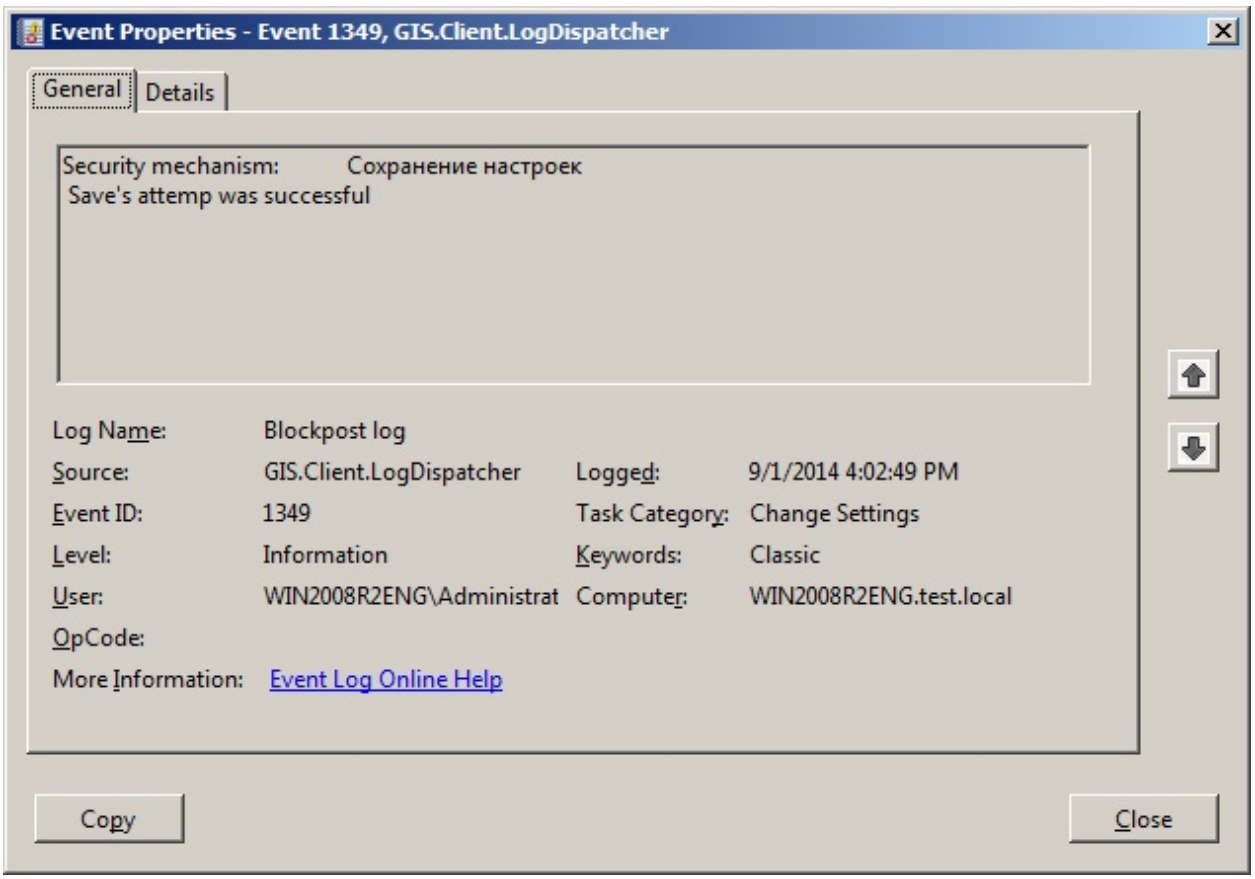
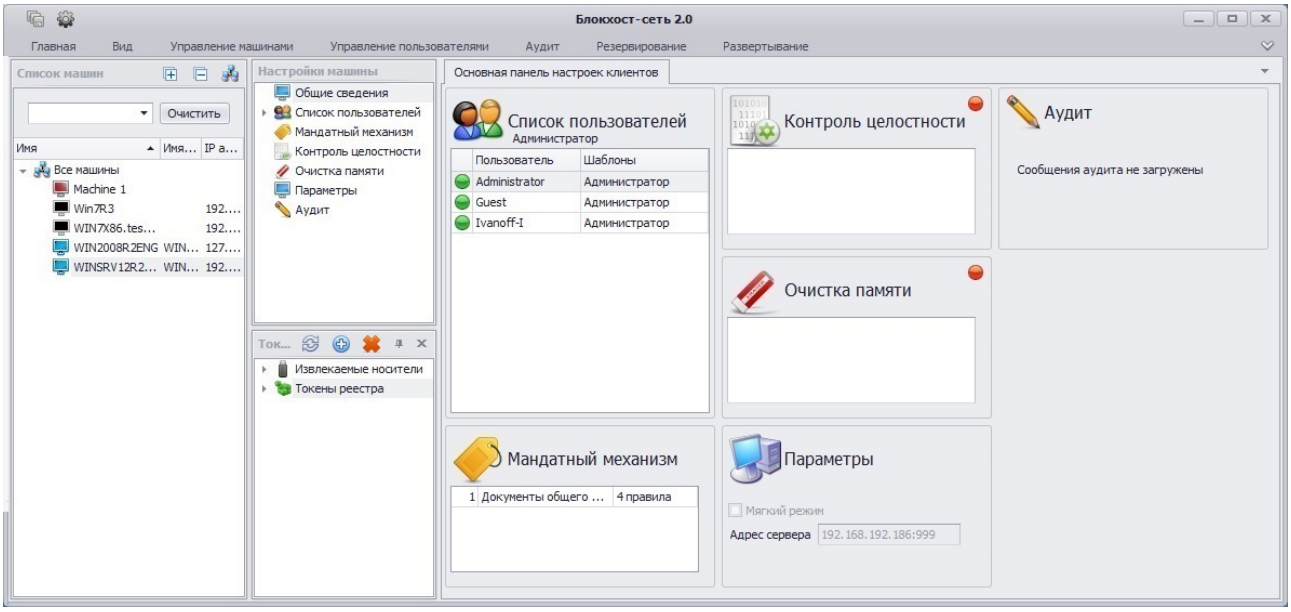


Рисунок 8.2. Окно описания события

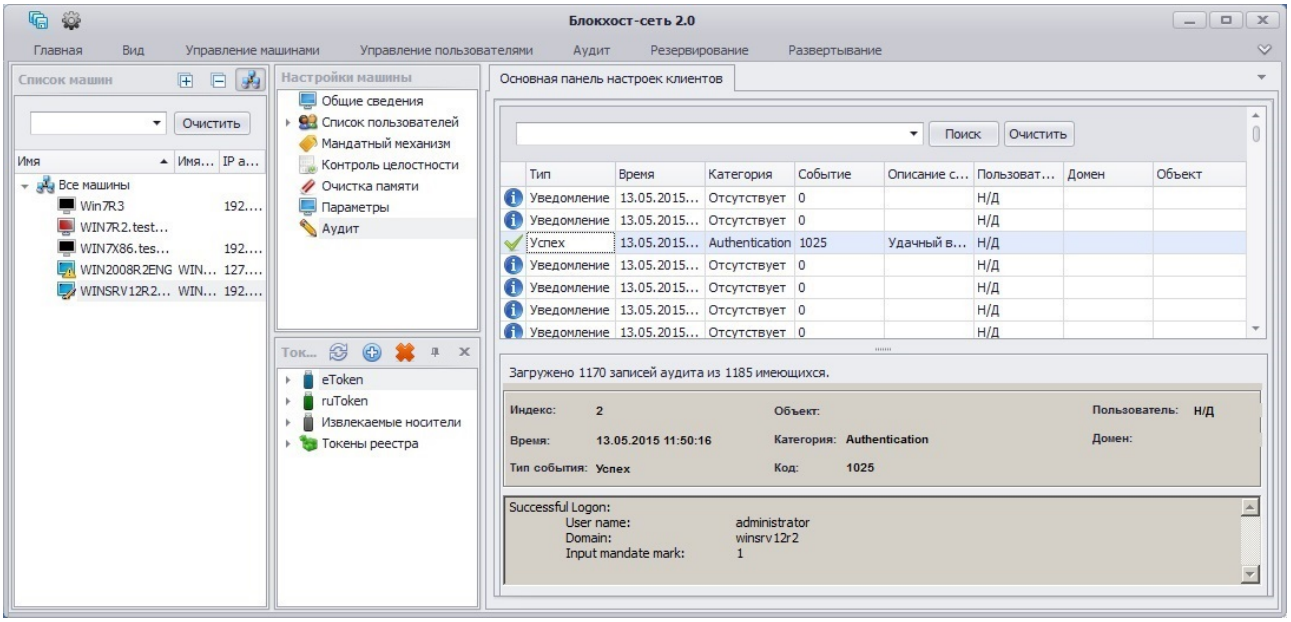
Для пользователя, не имеющего соответствующих полномочий, можно ограничить просмотр событий аудита. Для этого необходимо запретить соответствующему пользователю запуск процесса *Event Viewer* в ОС Windows (т.е. запретить запуск MMC-консоли). Запретить запуск *Event Viewer* можно, воспользовавшись механизмом замкнутой программной среды СЗИ, который позволяет создать перечень разрешенных к запуску процессов для пользователя. Процессы, не включенные в этот список (в том числе *Event Viewer*) будут запрещены для запуска. Подробное описание данного механизма приведено в пункте 6.1.3 «Разграничение доступа к запуску процессов» настоящего руководства.

Для просмотра сообщений аудита из серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» администратору безопасности необходимо:

1. В окне **«Список машин»** выбрать рабочую станцию, события которой необходимо просмотреть, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции;
2. В окне **«Настройки машины»** выбрать пункт ***Аудит*** или щелкнуть в **Основной панели настроек клиентов** по названию ***Аудит*** (рис. 8.3, а). В обоих случаях в **Основной панели настроек клиентов** откроется журнал событий СЗИ (рис. 8.3, б);



а)



б)

Рисунок 8.3. Просмотр аудита в серверной консоли администрирования СЗИ «Блокхост-сеть 2.0»

3. В **Основной панели настроек клиентов** двойным щелчком на интересующем событии можно вызвать окно с его описанием (рис. 8.4) или просмотреть эту же информацию в нижней части вкладки;

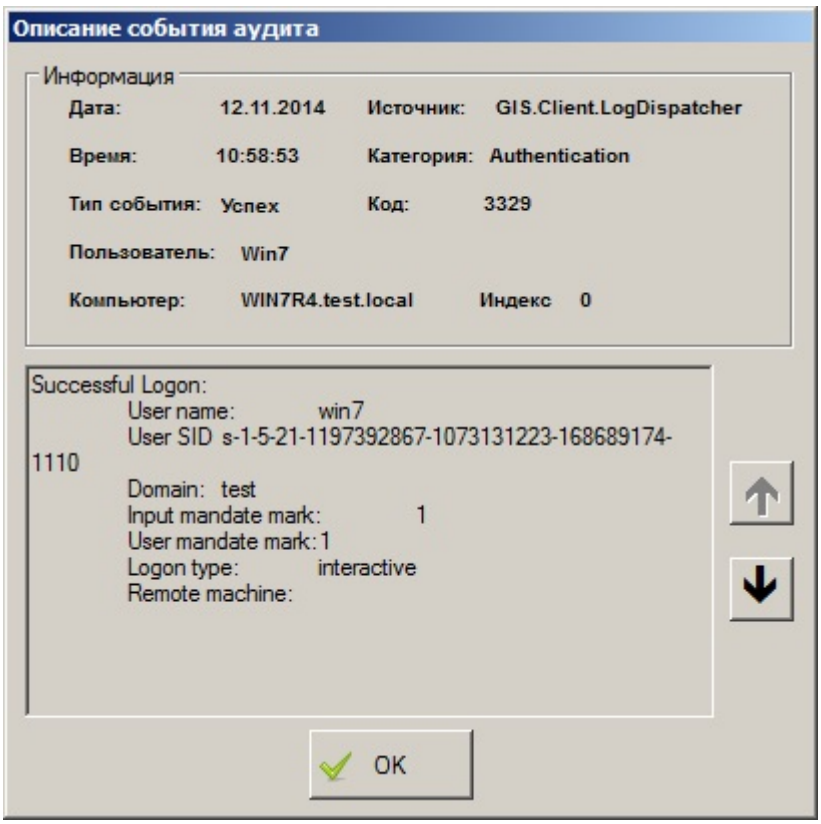


Рисунок 8.4. Подробное описание событий аудита

Для удобства просмотра журнала событий СЗИ администратор безопасности может сортировать записи по категориям (типу, дате, времени, источнику, категории, событию и т.п.). Существует возможность выборки событий размещенных на текущей странице, установив значение фильтра по любому из полей журнала. Устанавливать значения фильтра можно сразу по нескольким полям, при этом в нижней части области списка событий отобразится строка с критериями отбора событий по полям:

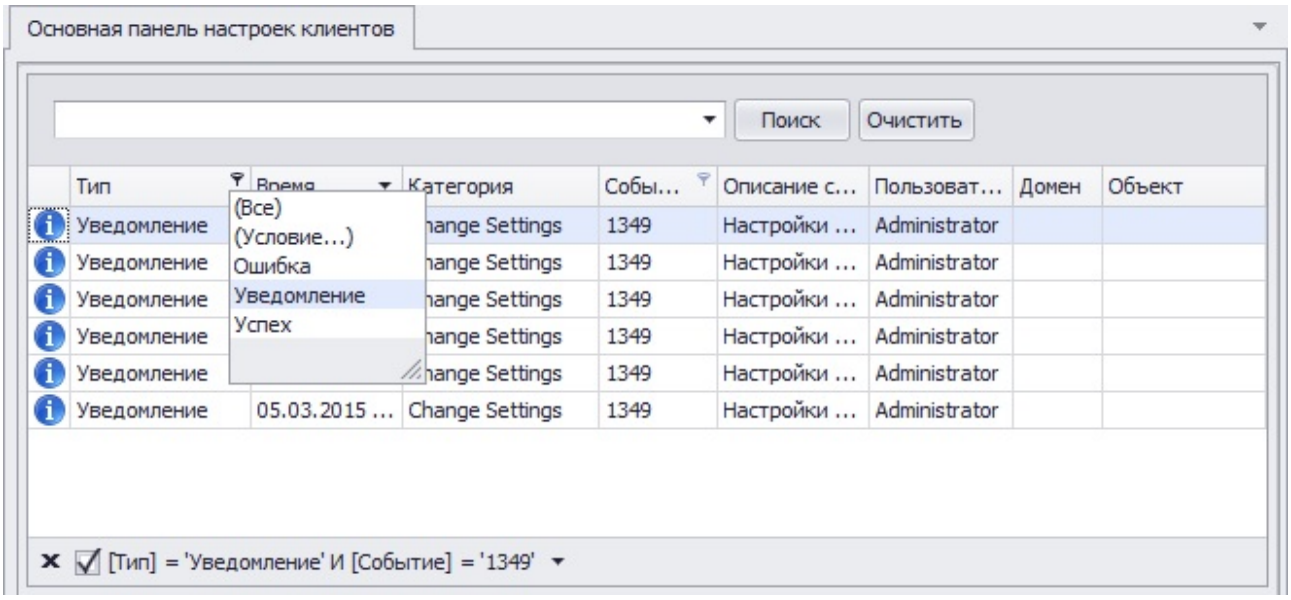


Рисунок 8.5 Установка фильтрации событий на текущей странице

Следует учесть, что загрузка событий в **Основную панель настроек клиента** консоли администрирования СЗИ осуществляется блоками по 300 записей – при достижении последней записи блока происходит загрузка следующего блока списка зарегистрированных событий. Поэтому установка параметров фильтрации по полям журнала событий позволяет осуществить выборку событий только из загруженных в консоль записей аудита.

8.3. Фильтрация событий

Фильтрация событий предназначена для выбора событий аудита по параметрам, которые задаются в диалоговом окне **«Настройки фильтра»** (рис. 8.6). Вызвать окно **«Настройки фильтра»** можно, щелкнув правой кнопкой мыши в **Основной панели настроек клиентов** и выбрав пункт контекстного меню ***Фильтр*** или выбрать пункт главного меню ***Аудит →Фильтр***:

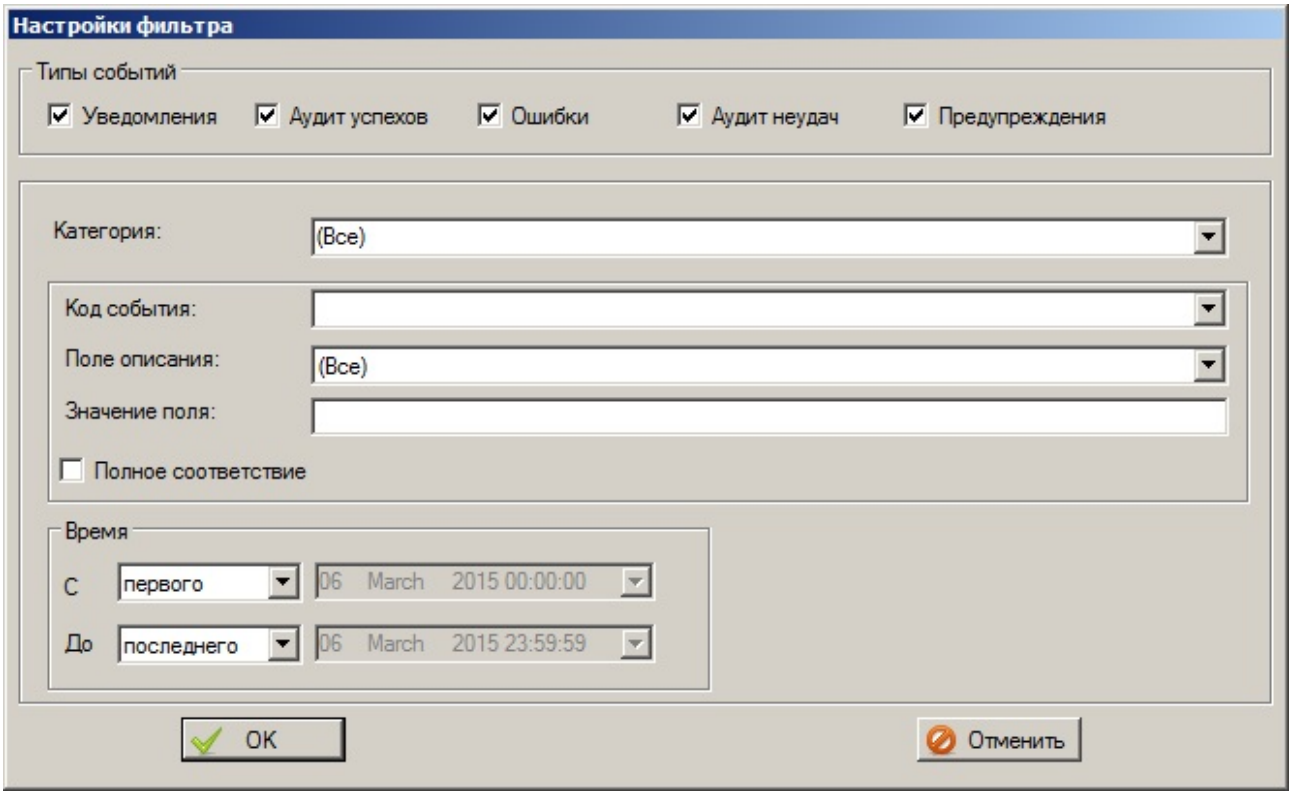


Рисунок 8.6. Окно фильтра журнала

В окне **«Настройки фильтра»** можно настроить вывод сообщений о произошедших событиях аудита в консоли администрирования СЗИ по типу, категории, коду, описанию, времени совершения события.

8.4. Свойства журнала событий СЗИ

Окно свойств журнала (рис. 8.8) позволяет увидеть основные характеристики файла журнала аудита СЗИ «Блокхост-сеть 2.0», а при необходимости – изменить его размер и длительность хранения зарегистрированных в нем событий. Вызвать окно свойств журнала можно выбором соответствующего пункта контекстного меню, вызываемого нажатием правой кнопкой мыши в **Основной панели настроек клиента** или выбрав пункт главного меню ***Аудит →Свойства*** (рис. 8.7).

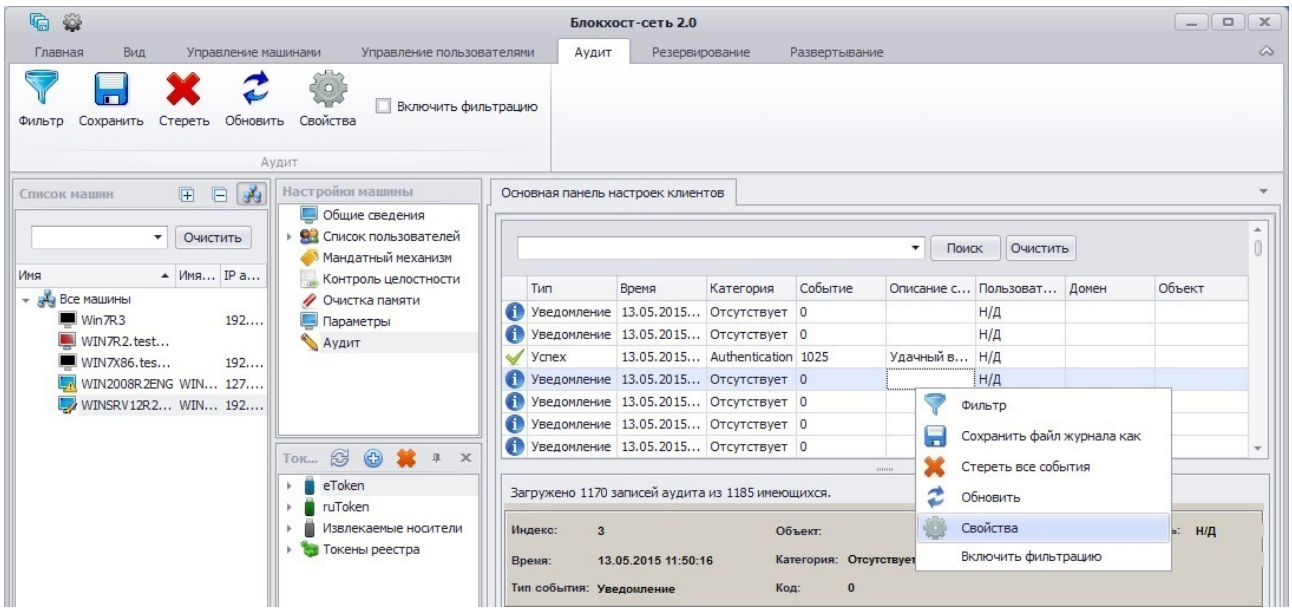


Рисунок 8.7. Вызов окна свойств журнала СЗИ «Блокхост-сеть 2.0»

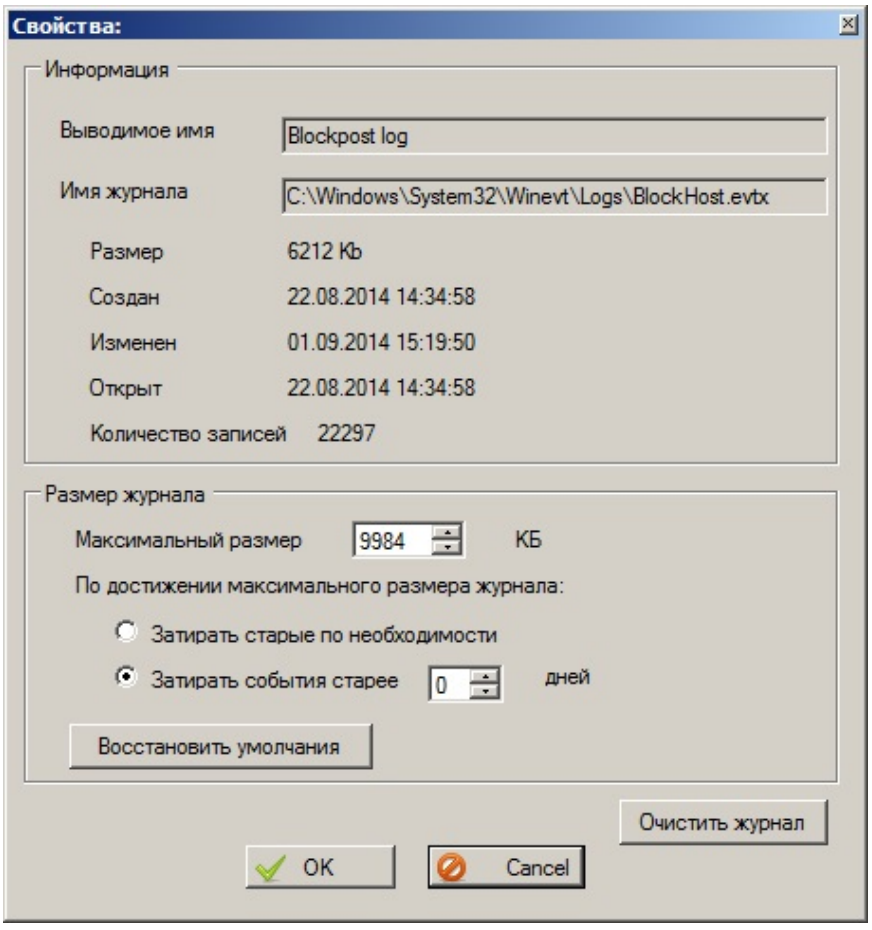


Рисунок 8.8. Окно свойств журнала СЗИ «Блокхост-сеть 2.0»

При большом количестве записей в журнале, загрузка данных аудита в консоли администрирования может занимать продолжительное время. Все события из журнала можно удалить, воспользовавшись пунктом контекстного меню ***Стереть все события*** или пунктом главного меню ***Аудит →Стереть***.

8.5. Другие действия с журналом аудита

Дополнительно серверная консоль администрирования СЗИ позволяет выполнять следующие действия с журналом аудита:

- *сохранение журнала аудита в файл*. Для этого нужно щелкнуть правой кнопкой мыши в **Основной панели настроек клиентов** и выбрать пункт контекстного меню ***Сохранить файл журнала как*** или выбрать пункт главного меню ***Аудит →Сохранить*** (см. рис. 8.7);
- *очистить журнал аудита*. Для этого нужно щелкнуть правой кнопкой мыши в **Основной панели настроек клиентов** и выбрать пункт контекстного меню ***Стереть все события*** или выбрать пункт главного меню ***Аудит →Стереть*** (см. рис. 8.7);
- *обновить журнал аудита.* Для этого нужно щелкнуть правой кнопкой мыши в **Основной панели настроек клиентов** и выбрать пункт контекстного меню ***Обновить*** или выбрать пункт главного меню ***Аудит →Обновить*** (см. рис. 8.7).

8.6. Типы сообщений оперативного контроля

СЗИ «Блокхост-сеть 2.0» в журнале аудита фиксирует сообщения четырех типов:

Уведомление	Информационные сообщения, уведомляющие администратора безопасности о событии, которое может оказать влияние на безопасность защищаемой информации.
Успех	Аудит успехов – сообщения, фиксирующие удачные, разрешенные события в системе, например, успешный вход в систему.
Неудача	Аудит неудач – сообщения, фиксирующие запрещенные события в системе, например, несанкционированная попытку входа в систему.
Ошибка	Ошибки – сообщения, фиксирующие нарушения правил разграничения доступа и целостности контролируемых объектов, например, нарушение целостности файла, поставленного на контроль целостности.

8.7. Отправка сообщений на внешний Syslog-сервер

СЗИ «Блокхост-сеть 2.0» позволяет отправлять события аудита на внешний Syslog-сервер. Для включения данной функции необходимо:

1. В консоли администрирования в окне **«Список машин»** выбрать АРМ, сообщения о событиях которого необходимо отправлять на внешний Syslog-сервер, для чего раскрыть пункт ***Все машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции.
2. В окне **«Настройки машины»** выбрать пункт ***Параметры*** (рис. 8.9).

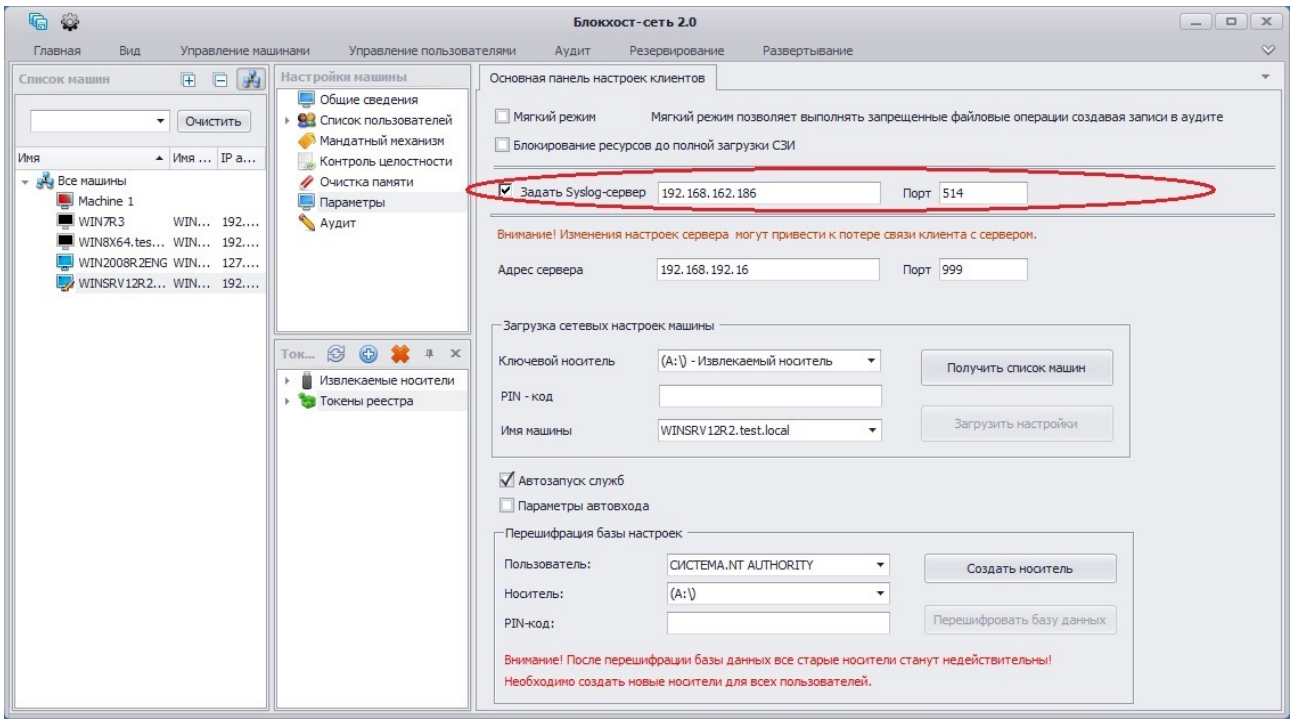


Рисунок 8.9. Установка параметров Syslog-сервера

3. В **Основной панели настроек клиента** установить параметр ***Задать Syslog-сервер*** и ввести IP-адрес Syslog-сервера и номер порта взаимодействия с ним в соответствующие поля.
4. Сохранить произведенные настройки с помощью кнопки ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ, или воспользоваться пунктом меню ***Главная→ Сохранить***.

После этого, события аудита СЗИ начнут поступать на внешний Syslog-сервер. При этом в консоли администрирования СЗИ «Блокхост-сеть 2.0» для контролируемых объектов должна быть включена опция ***Аудит***.

Параметры внешнего syslog-сервера для сообщений СЗИ «Блокхост-сеть 2.0» также можно указать внеся изменения в реестр на удаленной рабочей станции:

1) на всех рабочих станциях с установленным СЗИ (в т.ч. – на сервере безопасности) создать ключ реестра `HKLM\Software\Blockhost\Syslog` (для 32-bit ОС), ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlockHost\Syslog` (для 64-bit ОС);
2) внутри данного ключа реестра создать два параметра типа ***string*** (***REG_SZ***): `ServerAddress`, `ServerPort`;
3) в качестве значений параметров `ServerAddress`, `ServerPort` указать адрес и порт Syslog-сервера соответственно;
4) перезагрузить рабочие станции (либо перезапустить на них службу *GIS.Client.LogDispatcher.exe*).

В качестве внешнего Syslog-сервера может быть использована, например, «Система мониторинга событий», которая входит в состав системы управления модулями «Блокхост-МДЗ» и представляет собой Web-сервер. «Система мониторинга событий» позволяет осуществлять сбор и анализ событий, происходящих в системе (рис. 8.10). Подробное описание работы «Системы мониторинга событий» приведено в документе «Система

удаленного управления модулем «Блокхост-МДЗ». Система мониторинга событий (сервер мониторинга). Описание применения».

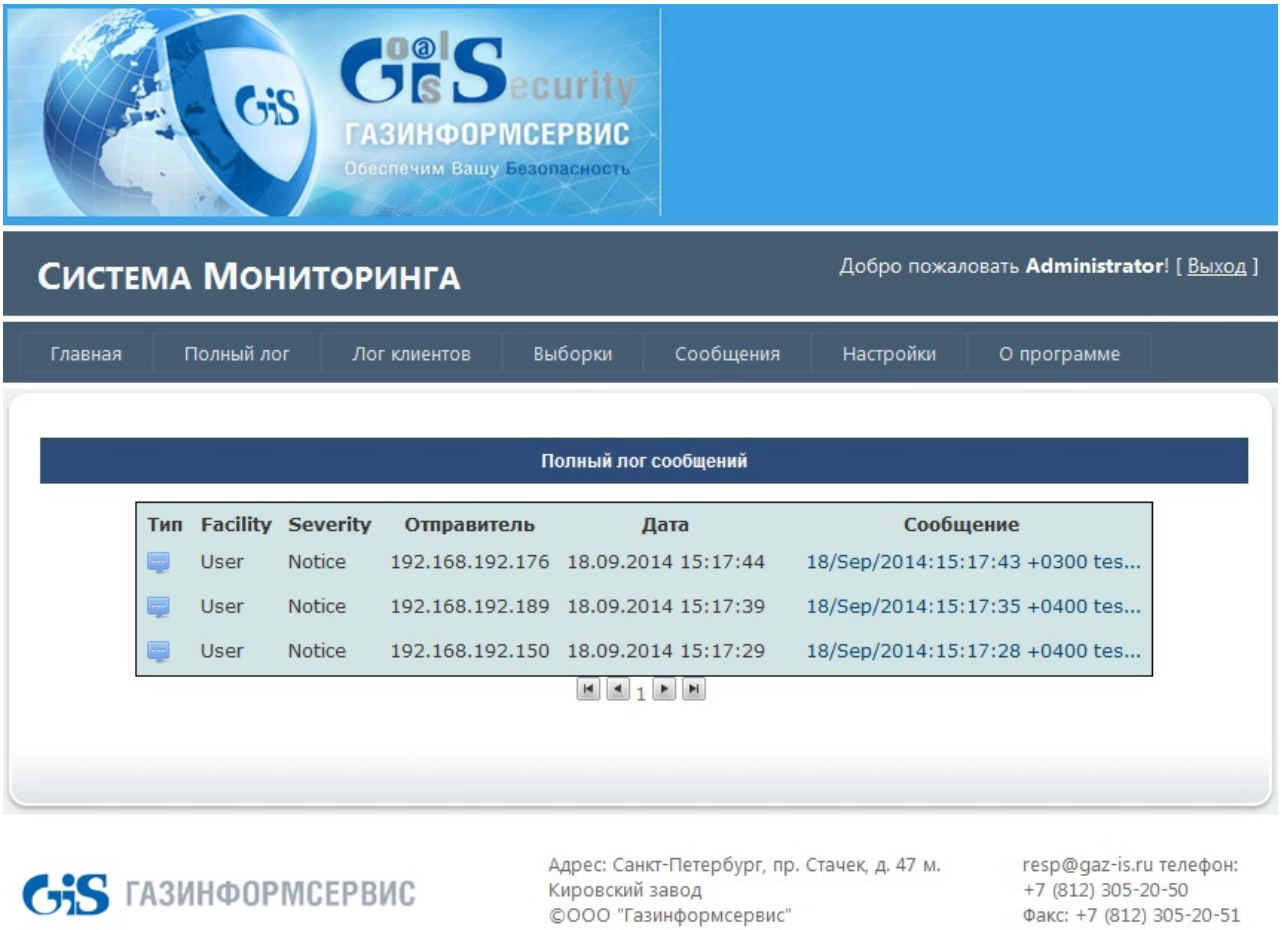


Рисунок 8.10. Окно «Системы мониторинга событий»

8.8. Фиксация событий клиентов СЗИ «Блокхост-сеть 2.0»

В состав СЗИ «Блокхост-сеть 2.0» входит также приложение ServerTrayMonitor, которое устанавливается вместе с серверной частью СЗИ и предназначено для интерактивного отслеживания отдельных событий клиентов СЗИ «Блокхост-сеть 2.0». К таким событиям относятся:

- подключение клиентов СЗИ,
- события контроля целостности,
- события контроля печати;
- вход пользователя на рабочую станцию/выход пользователя с рабочей станции.

Приложение ServerTrayMonitor запускается автоматически при входе пользователя в ОС, с установленной серверной частью СЗИ. После автоматического запуска приложение находится в свернутом виде, а его значок  отображается в области уведомлений.

Открыть окно приложения можно дважды щелкнув левой кнопкой мыши по его значку в области уведомлений. Окно приложения **ServerTrayMonitor** имеет вид, приведенный на рисунке 8.11.

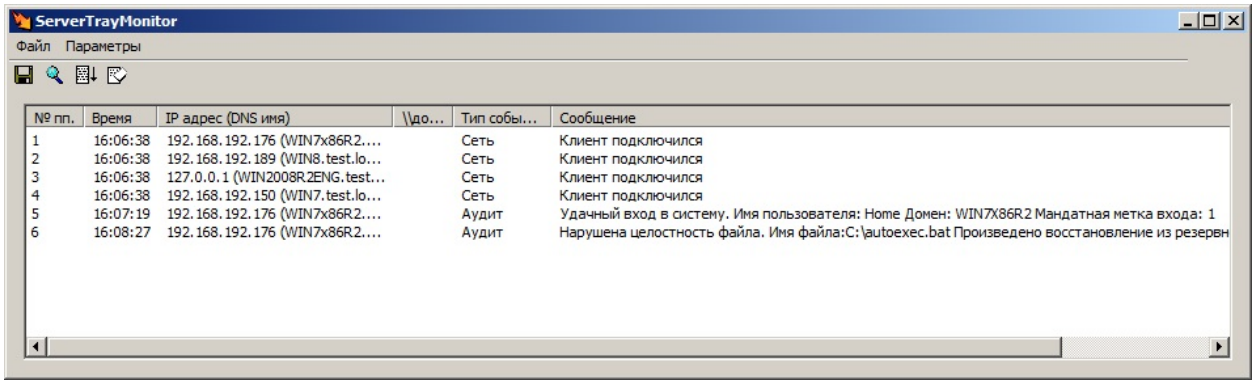


Рисунок 8.11. Окно ServerTrayMonitor

После закрытия окна программы приложение продолжает работать. Для окончания работы приложения ServerTrayMonitor необходимо в окне программы выбрать пункт меню ***Файл→Выход***.

После окончания работы приложения заново запустить его можно из меню ***Пуск →Программы →BlockHost-Net 2.0 →Monitor*** – его запуск также будет осуществлен в свернутом виде.

Приложение 1

(рекомендуемое)

Сбор диагностической информации

В СЗИ «Блокхост-сеть 2.0» реализована возможность вывода, сбора и сохранения информационных сообщений по выявлению проблем функционирования механизмов СЗИ. В большинстве случаев необходимость сбора такой информации требуется для рассмотрения проблемы функционирования СЗИ и запрашивается специалистами технической поддержки.

Запуск консоли администрирования в режиме отображения информационных сообщений.

В серверной консоли имеется возможность контролировать информационные сообщения СЗИ. Для этого необходимо на ярлыке приложения вызвать его свойства (правая кнопка мыши→**Свойства**) и в текстовом поле «**Объект**» добавить к команде вызова приложения параметр ***-trace*** таким образом, чтобы получилась команда: *C:\BlockHost\ServerBPShell.New\GIS.BlockPost.Server.exe -trace*.

После включения этой опции в окне **«Лог»** будут отображаться все события, связанные с работой серверной консоли. А в каталоге размещения СЗИ «Блокхост-сеть 2.0» *C:\BlockHost\ServerBPShell.New\Log* будет создан файл *full_log.log*, в который также будут записываться все события связанные с работой консоли администрирования. По умолчанию в окне **«Лог»** консоли администрирования отображаются только сообщения связанные с работой администратора безопасности, которые также записываются в файл short_log.log, находящийся в каталоге размещения СЗИ *C:\BlockHost\ServerBPShell.New\Log*.

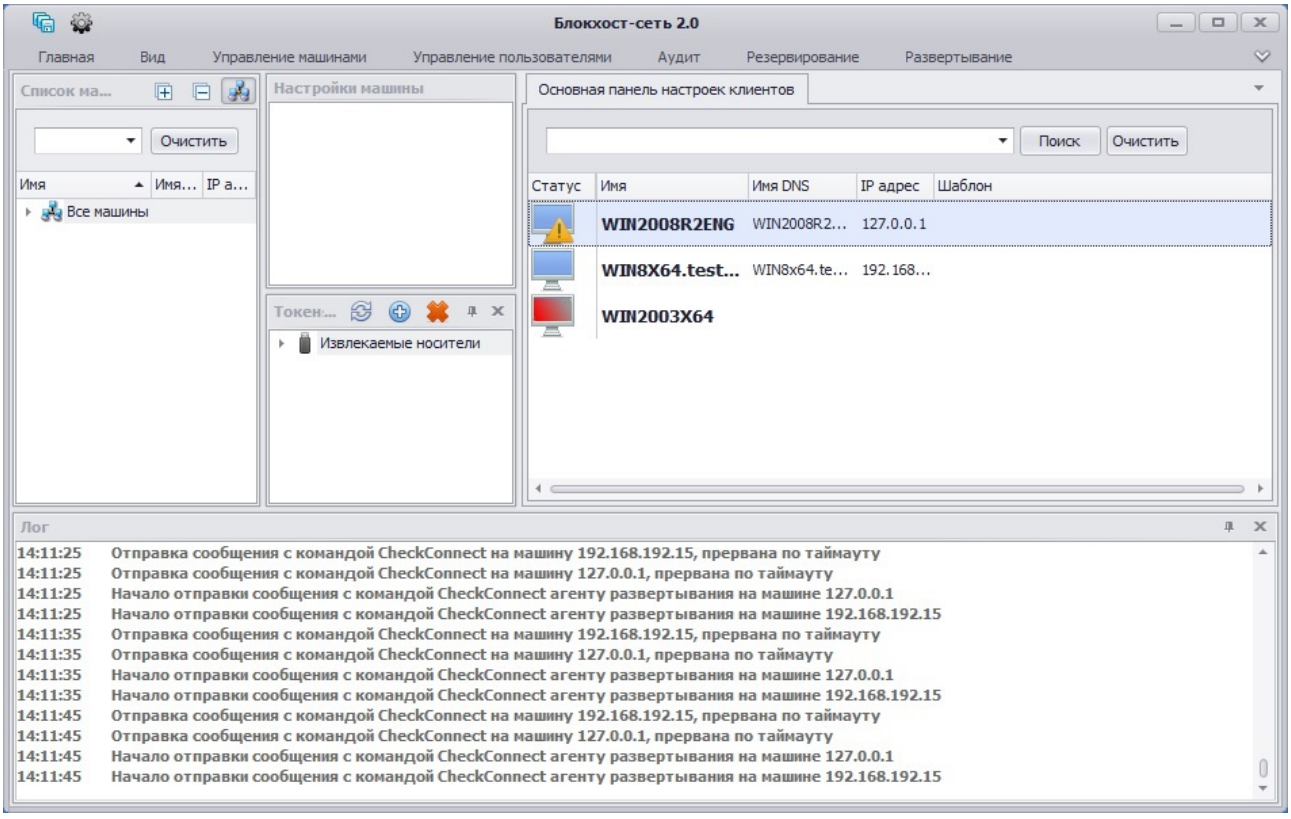


Рисунок П.1. Отображение информационных сообщений СЗИ в окне «Лог» серверной консоли

Включение логирования работы механизма контроля печати

При необходимости сбора технической информации о работе механизма контроля печати следует провести ряд настроек на рабочей станции:

1. Создать в корне диска ***C:*** каталог ***Temp*** для размещения в нем лог-файлов работы механизма контроля печати. Предоставить доступ к этому каталогу с правами «Чтение» и «Запись» группе «Пользователи» рабочей станции;

2. В ключе реестра *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GIS.Client.PrintControl* следует добавить параметр ***DebugFlag*** (тип REG_DWORD) и присвоить ему значение «1»;

3. Перезагрузить рабочую станцию.

В результате выполненных настроек, в процессе работы механизма контроля печати СЗИ, в зависимости от выполняемых действий в каталоге *C:\Temp* будут вестись текстовые лог-файлы:

- fpc.txt – информационные сообщения о работе сервиса GIS.Client.PrintControl;
- fpp.txt – информационные сообщения о работе принт-процессора pp_ctrl.dll:
- ff.txt, fc.txt – информационные сообщения о работе библиотеки инжекта PCInjDLL.dll;
- fe.txt – информационные сообщения о работе помощника для 64-битного окружения EnumProcess64.exe.

Включение логирования работы подсистемы аутентификации СЗИ

При необходимости сбора технической информации о работе подсистемы аутентификации СЗИ следует провести ряд настроек на рабочей станции:

1. Создать в корне диска ***C:*** каталог ***Temp*** для размещения в нем лог-файлов работы механизма контроля печати. Предоставить доступ к этому каталогу с правами «Чтение» и «Запись» группе «Пользователи» рабочей станции;

2. В ключе реестра *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon* следует добавить параметр ***DebugFlag*** (тип REG_DWORD) и присвоить ему значение:

- «1» - будет вестись минимальный лог работы подсистемы аутентификации;
- «2» - будет вестись полный лог работы подсистемы аутентификации с записью сообщений о пошаговом выполнении команд программы;

3. Перезагрузить рабочую станцию.

В результате выполненных настроек в процессе работы подсистемы аутентификации СЗИ в каталоге *C:\Temp* будет вестись текстовый лог-файл LogonUI.exe.txt.