ГАЗИНФОРМ СЕРВИС

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

Руководство администратора безопасности

Санкт-Петербург, 2019

Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 3» (далее по тексту – СЗИ «Блокхост-Сеть 3» или СЗИ).

В документе приведено назначение и состав СЗИ, описаны реализованные функции (механизмы) защиты. В нем содержатся сведения об аппаратных и программных требованиях для установки клиентской и серверной части СЗИ на серверах и клиентских компьютерах, где предполагается использование средства.

Руководство содержит описание интерфейса СЗИ, предоставленного локальной и серверной консолями, и основных приемов работы с ним,

Важнейшей частью документа являются разделы, в которых где изложено как производить настройку системы: организовать иерархию серверов (если используется иерархия), настраивать параметры сервера/серверов, формировать список контролируемых рабочих станций, создавать группы рабочих станций для упрощения настройки и т.д.

В документе описано управление учетными записями пользователей и ключевыми носителями информации, а также настройка механизмов защиты информации, реализованных в СЗИ.

Содержание

Введение

Структурно СЗИ «Блокхост-Сеть 3» состоит из клиентской части СЗИ «Блокхост-Сеть 3», в рамках которой реализованы базовые механизмы защиты, и серверной части (сервера безопасности), к которой обращается администратор безопасности (АБ) для централизованного управления серверной и клиентской частями СЗИ «Блокхост-Сеть 3».

Клиентская часть устанавливается на защищаемые рабочие станции (в составе локальной вычислительной сети (ЛВС) или работающие автономно) и серверы ЛВС, в том числе на автоматизированное рабочее место (АРМ) администратора безопасности, и обеспечивает защиту рабочей станции от несанкционированного доступа (НСД) к информации.

Настройка клиентской части может быть выполнена через локальную или серверную консоль администрирования СЗИ «Блокхост-Сеть 3», настройка серверной части выполняется через серверную консоль.

Локальная консоль администрирования позволяет выполнять настройку СЗИ «Блокхост-Сеть 3» непосредственно на рабочей станции. Серверная консоль предназначена для настройки тех же механизмов СЗИ на контролируемых рабочих станциях с АРМ АБ.

В состав СЗИ «Блокхост-Сеть 3» также входит дополнительный компонент, реализованный в виде отдельного программного приложения:

- *система развертывания и аудита СЗИ «Блокхост-Сеть 3»* (вариант с удаленным управлением) – позволяет удаленно, с сервера безопасности, устанавливать клиентские части СЗИ на рабочие станции в сети и централизованного сбора аудита со всех рабочих станций. Консоль системы развертывания и аудита (СРиА) устанавливается на сервер безопасности одновременно с установкой серверной части СЗИ, агент системы развертывания и аудита устанавливается на рабочие станции в составе ЛВС. Подробное описание СРиА приведено в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

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 3»

1.1 Назначение СЗИ «Блокхост-Сеть 3»

Средство защиты информации «Блокхост-Сеть 3» является программным средством защиты информации от несанкционированного доступа к информации, предназначенным для комплексной и многофункциональной защиты информационно-программных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС) на базе персональных компьютеров (ПК) под управлением операционных систем (ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

Реализованные в СЗИ «Блокхост-Сеть 3» 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;
- 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 3». Настройка осуществляется в соответствии с данным руководством и заключается в определении пользователей, которым надлежит обеспечить доступ к защищаемому средству вычислительной техники (СВТ), и формировании для них политик безопасности на основе реализованных в СЗИ механизмов разграничения доступа и защиты информации;
- выполнять аудит информационной безопасности компьютера. Ведение оперативного контроля событий необходимо для выявления ошибок в настройках СЗИ и корректировки правил разграничения доступа, а также для своевременного реагирования на осуществление НСД к защищаемой информации.

1.2 Локальная и централизованная защита информации

СЗИ «Блокхост-Сеть 3» обеспечивает защиту от НСД 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 3», так и без таковой.

СЗИ «Блокхост-Сеть 3» дополняет функциональные возможности ОС по защите информации. Таким образом, информация защищается от НСД следующими компонентами (рисунок 1.1):

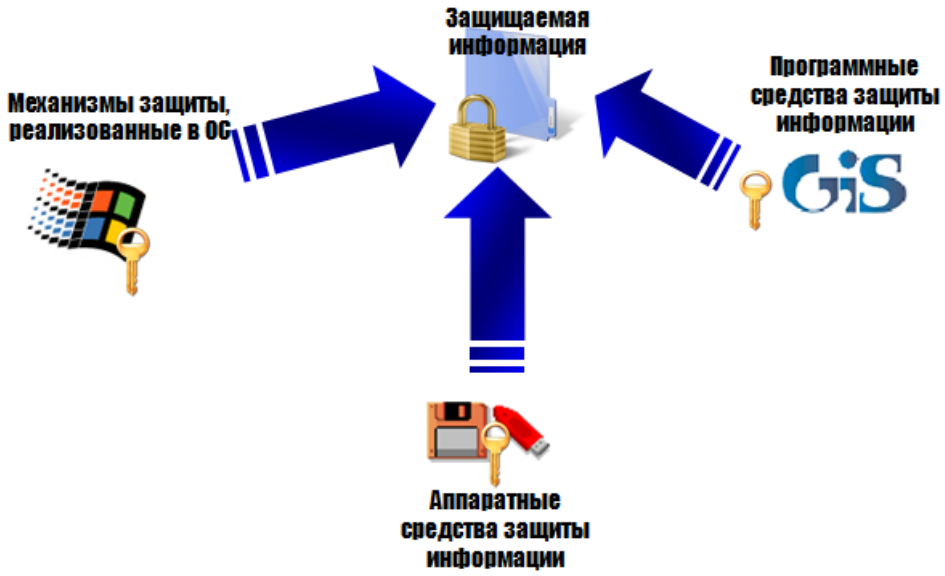


Рисунок 1.1 – Компоненты защиты от НСД

1.3 Состав СЗИ «Блокхост-Сеть 3»

СЗИ «Блокхост-Сеть 3» включает в себя **специализированный программный комплекс**, состоящий из клиентской и серверной частей СЗИ.

Клиентская часть СЗИ «Блокхост-Сеть 3» обеспечивает локальную защиту рабочей станции от НСД к информации. После установки СЗИ «Блокхост-Сеть 3» администратору безопасности доступны следующие механизмы защиты:

- идентификация и аутентификация АБ и пользователей, работающих на ПК с СЗИ «Блокхост-Сеть 3», в том числе с применением персональных электронных идентификаторов;
- возможность двухфакторной аутентификации пользователей средствами СЗИ при входе в ОС Windows с использованием цифровых сертификатов пользователей. Сертификаты могут храниться на вышеуказанных персональных электронных идентификаторах eToken, SafeNet eToken, ruToken, JaCarta, ESMART Token и Avest

Token;

- дискреционный и мандатный механизмы контроля доступа к информационным ресурсам рабочей станции в соответствии с заданными параметрами безопасности;
- контроль целостности файловой системы;
- гарантированное восстановление функций безопасности СЗИ;
- 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;
- управление идентификаторами входа;
- временное разграничение доступа пользователей к рабочей станции;
- администрирование СЗИ с использованием интерфейса администратора;
- контроль целостности программно-аппаратной среды.

Серверная часть СЗИ «Блокхост-Сеть 3» выполняет функции централизованного управления удаленными рабочими станциями:

- присоединение клиентских частей к сети СЗИ от несанкционированного доступа (НСД) «Блокхост-Сеть 3»;
- выполнение удаленной установки клиентских частей СЗИ «Блокхост-Сеть 3» на рабочие станции из серверной консоли администрирования СЗИ;
- выполнение удаленной установки программного обеспечения на рабочие станции в сети из консоли системы развертывания и аудита Блокхост-Сеть;
- удаленное управление настройками клиентов СЗИ от НСД «Блокхост-Сеть 3»;
- управление групповыми политиками безопасности;
- взаимная аутентификация клиентов при сетевом взаимодействии;
- сетевое мандатное разграничение;
- централизованный сбор и просмотр данных аудита;
- присоединение и управление параметрами подчинённых серверов.

1.4 Персональные идентификаторы

Реализованный в СЗИ «Блокхост-Сеть 3» механизм двухфакторной аутентификации позволяет усилить защищенность входа рабочей станции за счет использования, помимо персональных идентификационных данных пользователя, ключевых носителей.

Под ключевым носителем подразумевается: eToken, SafeNet eToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, JaCarta-2, JaCarta LT, AvBign, ESMART Token и ruToken, USB-накопитель, дискета, а также возможно использование персонального идентификатора

пользователя, хранящегося в области недоступной для непривилегированного пользователя (персональный идентификатор пользователя в реестре Windows).

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 3».

Механизм управления идентификаторами позволяет выполнять следующие действия:

- менять PIN-код ключевого носителя;
- получать информацию по носителю;
- менять имя зарегистрированного носителя (для ruToken);
- отвязывать пользователей от носителя;
- отвязать носитель от рабочей станции;
- редактировать сгенерированные станции;
- задать время жизни носителя.

Данные по каждому носителю отображаются в консоли на одном уровне с настройками пользователя (дополнительный узел в дереве «идентификаторы входа»).

Каждому пользователю соответствует один или более носитель, идентификация пользователя будет осуществляться по SID (данные о привязке пользователя, носителя и рабочей станции хранится на носителе и в базе настроек рабочей 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.

1.5 Механизмы, предназначенные для решения задач защиты информации

Подробнее о настройках механизмов в п. 6 «Формирование политики безопасности» данного документа.

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 его доступе на ПК в составе СЗИ предназначена для защиты от несанкционированного доступа к защищаемой информации на ПК незарегистрированных пользователей или пользователей не имеющих установленных прав доступа к защищаемой информации.

В СЗИ ведется список разрешенных пользователей для входа в систему, который может быть изменен только АБ. Идентификация и аутентификация пользователей осуществляются после инициализации механизмов защиты СЗИ. При этом в СЗИ отключена возможность загрузки ОС в защищенном режиме для всех пользователей, за исключением АБ.

В системе реализованы следующие способы идентификации и аутентификации пользователя:

- вход в систему по паролю, вводимому пользователем с клавиатуры;
- вход в систему по ключевому носителю с паролем (пароль в зашифрованном виде хранится на ключевом носителе);
- вход в систему с предъявлением цифрового сертификата, записанного на ключевом носителе.

В СЗИ «Блокхост-Сеть 3» ограничение на минимальную длину пароля определяется настройками политик безопасности.

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.

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

Механизм аутентификации СЗИ «Блокхост-Сеть 3» можно полностью отключить, активировав ***Мягкий режим работы*** СЗИ (подробнее п. 6.2.5 «Механизм мягкого режима»). При включенном мягком режиме вход в операционную систему может выполнить любой доменный или локальный пользователь рабочей станции, если это не противоречит установленным в домене политикам.

Мягкий режим работы, а также режим аутентификации ***Доверять аутентификации Windows*** (данный режим автоматически устанавливается при добавлении новых учетных записей в СЗИ) используются для первичной настройки средства защиты, до начала эксплуатации. В данных режимах средство защиты не обеспечивает выполнение заявленных функций безопасности. Эксплуатировать СЗИ в описанных режимах для защиты станции **запрещено**.

1.5.2 Дискреционный механизм контроля доступа к ресурсам

В качестве субъектов доступа в СЗИ рассматриваются поименованные пользователи, в т.ч. и администратор безопасности. Объектами доступа выступают объекты файловой системы (логические диски, каталоги и файлы).

Дискреционный механизм контроля доступа к ресурсам включает:

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

СЗИ предоставляет право АБ после его авторизации изменять правила разграничения доступа. При этом может изменяться как список пользователей и контролируемых объектов защиты, так и права доступа к объектам защиты.

1.5.3 Мандатное разграничение контроля доступа к ресурсам

Мандатное разграничение контроля доступа обеспечивает разграничение доступа субъектов (пользователей, процессов) к объектам (дискам, папкам, файлам) путем сочетания назначенных субъектам и объектам допуска квалификационных меток (числовых значений уровня допуска субъекта или конфиденциальности объекта) и неиерархических категорий, к которым принадлежат объекты и субъекты доступа. Степень конфиденциальности информации зависит от иерархической метки, чем метка больше, тем выше конфиденциальность объекта и уровень допуска субъекта.

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 ОС Windows 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).

1.5.5 Механизм очистки остаточной информации

Механизм очистки остаточной информации объединяет в себе механизм очистки памяти и механизм гарантированного удаления.

Очистка памяти выполняется с целью удаления остаточной информации после работы контролируемого процесса.

Модуль очистки памяти СЗИ контролирует завершение поставленных на контроль процессов и после их завершения производит очистку всей свободной физической памяти путем записи в нее маскирующей информации.

Гарантированное удаление выполняется модулем диспетчера доступа СЗИ. При попытке удаления поставленного на контроль файла диспетчер доступа запрещает удаление средствами ОС и запускает модуль гарантированного удаления. Поставленные на контроль файлы удаляются путем трехкратного затирания их содержимого по специальному алгоритму, который исключает считывание остаточной информации на диске после удаления.

1.5.6 Механизм контроля целостности и гарантированного восстановления

Механизм контроля целостности выполняет проверку установленных на контроль целостности файлов. Расчет контрольных сумм осуществляется по алгоритму CRC-32 и при обнаружении нарушений контрольных сумм (КС) СЗИ обеспечивает их надежное

восстановление без привлечения АБ.

Этот же механизм используется для контроля целостности и надежного восстановления программных модулей СЗИ после сбоев. При инсталляции СЗИ автоматически создаются резервные копии всех программных модулей СЗИ и рассчитываются контрольные суммы файлов резервных копий программных модулей СЗИ по указанному выше алгоритму. Проверка целостности осуществляется по заданному АБ временному интервалу в процессе работы СЗИ. При обнаружении нарушений выполняется перезагрузка ОС с восстановлением модулей из резервных копий.

1.5.7 Механизм регистрации событий и аудита

Механизм регистрации событий и аудита предназначен для отслеживания событий и регистрации обращения к защищаемым ресурсам. а также при срабатывании всех механизмов защиты. Централизованный сбор и просмотр данных аудита, из настроенного АБ перечня, осуществляется в консоли системы развертывания и аудита Блокхост-Сеть.

В консоли системы развертывания и аудита Блокхост-Сеть АБ доступен следующий функционал для работы с событиями аудита:

- формирование сводного отчета с информацией о состоянии клиентов, подключенных к серверам иерархии;
- сбор событий аудита с клиентов на сервер СЗИ;
- просмотр и фильтрация событий аудита, собранных с клиентских компьютеров на сервер;
- просмотр и фильтрация событий аудита напрямую из журнала клиентского компьютера;
- передача событий аудита вверх по иерархии серверов вплоть до головного сервера с последующей передачей в SIEM-систему.

Информация анализируется и события, входящие в перечень, определенный администратором безопасности, отправляются сетевому монитору безопасности на сервер безопасности.

1.5.8 Механизм контроля целостности среды

Механизм контроля целостности среды предназначен для слежения за неизменностью контролируемых объектов с целью обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

Механизм контроль целостности среды включает в себя:

- отслеживание изменений списка установленных программ;
- отслеживание изменений списка установленных служб/драйверов;

- отслеживание изменений перечня каталогов общего доступа;
- контроль аппаратной среды (отслеживает изменения конфигурации следующих устройств компьютера: процессор, жесткий диск, CDROM, сетевой адаптер. материнская плата, видеокарта).

Контроль параметров устройства осуществляется в момент запуска соответствующей службы. Получение информации о перечисленных устройствах осуществляется через интерфейс WMI. Соответствие контролируемых устройств классам WMI и поля, по которым осуществляется контроль изменения конфигурации, описаны в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Описание применения».

1.5.9 Механизм администрирования СЗИ

Механизм администрирования обеспечивает настройку параметров работы СЗИ. Параметры СЗИ делятся на механизмы станции, которые задают правила разграничения доступа для всех пользователей рабочей станции, и пользовательские, которые задают правила разграничения доступа для конкретных пользователей. Для удобства работы предусмотрен режим репликации настроек механизмов СЗИ.

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, разрешенных и запрещенных для запуска;
- формирование списка файлов, целостность которых требуется контролировать;
- формирование списка процессов, по завершению работы которых требуется очистка памяти;
- делегирование прав доступа по администрированию СЗИ пользователям (такие пользователи должны быть включены в группу администраторов текущей рабочей станции);
- управление аппаратными идентификаторами входа (изменение PIN-кода, задание времени жизни носителя, редактирование параметров станций и др.);
- управление групповыми политиками безопасности;
- формирование списка процессов для контроля печати и настройка колонтитулов для выводимой информации;

- формирование списка объектов контроля целостности среды;
- просмотр и анализ данных аудита в консоли системы развертывания и аудита Блокхост-Сеть, настройка перечня регистрируемых событий;
- выполнение удаленной установки клиентских частей СЗИ «Блокхост-Сеть 3» на рабочие станции, а также программного обеспечения на рабочие станции в сети из консоли системы развертывания и аудита Блокхост-Сеть.

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

2 Условия применения СЗИ «Блокхост-Сеть 3»

2.1 Требования к аппаратной конфигурации

СЗИ «Блокхост-Сеть 3» устанавливается на компьютеры с процессорами, имеющими архитектуру x86 и AMD64.

Минимальные требования к производительности ПК обусловлены требованиями используемых ОС.

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 3» 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 7 Professional SP1 (32-разрядная/64-разрядная);
- Windows 7 Enterprise SP1 (32-разрядная/64-разрядная);
- Windows 7 Ultimate SP1 (32-разрядная/64-разрядная);
- Windows 8.1 Core (32-разрядная/64-разрядная);
- Windows 8.1 Professional (32-разрядная/64-разрядная);
- Windows 8.1 Enterprise (32-разрядная/64-разрядная);
- Windows Server 2012/2012R2 Foundation (64-разрядная);
- Windows Server 2012/2012R2 Essentials (64-разрядная);
- Windows Server 2012/2012R2 Standard (64-разрядная);
- Windows Server 2012/2012R2 Datacenter (64-разрядная);
- Windows 10 Home (32-разрядная/64-разрядная);

- Windows 10 Pro (32-разрядная/64-разрядная);
- Windows 10 Enterprise (32-разрядная/64-разрядная);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (64-разрядная).
- Windows Server 2019 (64-разрядная).

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);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (64-разрядная);
- Windows Server 2019 (64-разрядная).

Рекомендуется наличие дисковода 3,5"; COM-, USB- и LPT-портов; необходимо наличие сетевой карты (при использовании варианта с удаленным управлением СЗИ «Блокхост-Сеть 3»).

Дополнительно на ПК должно быть установлено следующее программное обеспечение (ПО):

- .NET Framework 4.5.2;
- распространяемый пакет Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015;
- обновление системы безопасности KB3033929 (для ОС Windows 7 и Windows Server 2008/2008R2);

При использовании персональных идентификаторов на ПК должно быть установлено следующее ПО:

- драйверы для устройств eToken и SafeNet eToken, ruToken, JaCarta, ESMART Token, AvBign.

При входе в ОС Windows с использованием цифровых сертификатов пользователей

необходимо:

- установить СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2;
- при использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

Перед началом установки СЗИ на ОС Windows 8.1/2012/2012R2/10/2016/2019 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 корректной работы консолей администрирования СЗИ необходимо отключить параметр безопасности локальной политики ОС Windows **Системная криптография: использовать FIPS совместимые алгоритмы для шифрования, хеширования и подписывания.**

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности должен быть открыт 999 TCP-порт.

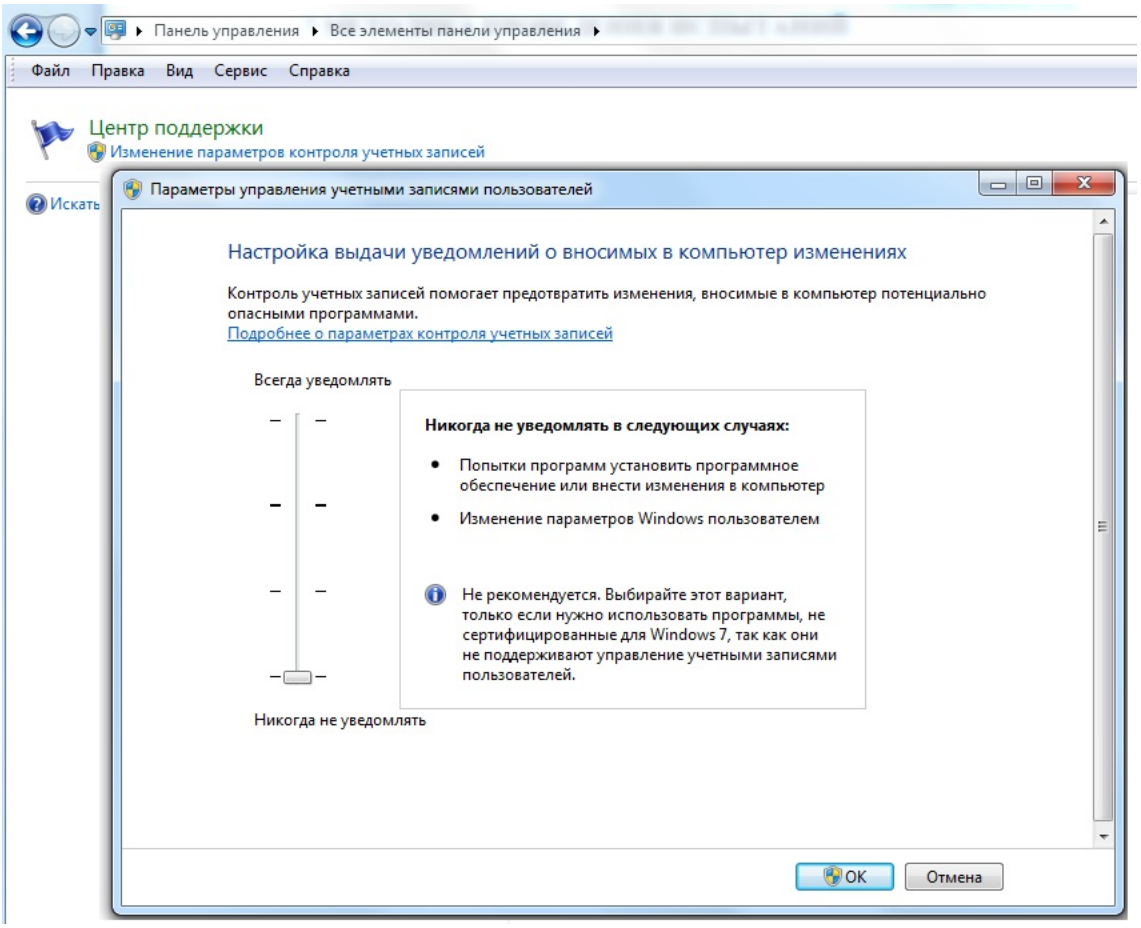


Рисунок 2.1 – Изменение уровня контроля UAC

2.3 Настройки безопасности среды функционирования СЗИ

При настройке мандатного разграничения доступа и эксплуатации СЗИ «Блокхост-Сеть 3» (порядок настройки мандатного разграничения СЗИ см. п. 6.2.2 «Мандатное разграничение доступа» настоящего руководства) **запрещено** создание вложенных объектов, для которых в объекте с низкой классификационной меткой может быть размещен объект с более высокой классификационной меткой.

С целью противостояния потенциальным уязвимостям среды функционирования СЗИ «Блокхост-Сеть 3» (в случае отсутствия модулей доверенной загрузки, контролирующих целостность директорий СЗИ и ОС Windows) администратор безопасности должен:

1) средствами BIOS ПК установить запрет загрузки ПК с внешних носителей информации и установить пароль администратора BIOS во избежание его модификации неавторизованными пользователями;

2) отключить возможность автоматического запуска консоли восстановления ОС, для чего последовательно выполнить в окне эмулятора командной строки (**cmd.exe**) следующие команды:

- для ОС Windows 7:
  - *bcdedit /set {default} bootstatuspolicy ignoreallfailures* – игнорирует ошибки неудачных загрузок, сбоев отключения, или неудачных точек восстановления;
  - *bcdedit /set {default} recoveryenabled No* – отключает функцию автоматического восстановления;
  - *reagentc /disable* – отключает образ восстановления системы, удаляет из BCD разделы, касающиеся загрузки образа winrm, устанавливает параметр *recoveryenabled* в *No* (равносильно команде *bcdedit /set {default} recoveryenabled No*).
- для ОС Windows 10:
  - *REAGENTC.EXE /disable* – отключение использования среды восстановления Windows;
- отключение запуска консоли восстановления ОС для группы рабочих станций приведено в подразделе 2.4. документа.

Для поддержания необходимого уровня защищенности ПК (АС) и информационных ресурсов, эксплуатации и эффективного применения системы защиты дополнительно требуется выполнение следующих организационно-технических мероприятий:

- обеспечение физической сохранности (целостности) ПК (АС), наличие физической охраны помещения, в котором эксплуатируется ПК (АС) и исключение возможности несанкционированного доступа к ПК (АС) посторонних лиц;
- наличие администратора безопасности, отвечающего за ее установку и правильную эксплуатацию;
- соблюдение принципа минимизации привилегий пользователей ПК, при котором

пользователям предоставляются только те права доступа, которые необходимы им для выполнения служебных обязанностей. Привилегии локальных администраторов ПК допускается предоставлять только пользователям, выполняющим функции администратора безопасности СЗИ;

- хранение в секрете паролей (кодов), а также – PIN-кодов персональных электронных идентификаторов администратора и пользователей системы;
- периодической смены паролей и PIN-кодов пользователей и администратора безопасности;
- учет носителей информации (отчуждаемых физических носителей, персональных идентификаторов и т.п. устройств);
- периодическое тестирование функций СЗИ «Блокхост-Сеть 3» в соответствии с Приложением 4 к настоящему руководству;
- использование в ПК (АС) сертифицированных технических и программных средств;
- проверка носителей информации на наличии вирусов.

Администратору безопасности СЗИ необходимо обеспечить контроль наличия и создания дополнительных ссылок на объекты, поддерживаемых файловой системой (подробнее в Приложении 2 «Особенности работы с жесткими и символьными ссылками объектов».

Должны быть установлены все актуальные обновления безопасности среды функционирования СЗИ «Блокхост-Сеть 3».

2.4 Отключение запуска консоли восстановления ОС с использованием консоли СРиА

Отключение среды восстановления ОС Windows для группы рабочих станций осуществляется с использованием консоли СРиА. При этом на рабочих станциях, где предполагается процедура группового отключения среды восстановления ОС Windows, предварительно должны быть установлены агенты развертывания.

Для группового отключения среды восстановления ОС Windows на рабочих станциях администратору необходимо выполнить следующие действия:

1) На сервере СЗИ «Блокхост-Сеть 3» с помощью текстового редактора создать bat-файл с названием ***reagent.bat***, в котором необходимо указать команду отключения среды восстановления и сохранить изменения в файле:

REAGENTC.EXE /disable.

2) Запустить консоль СРиА и перейти в раздел **Развертывание** во вкладку **Задачи** и, нажав кнопку ***Создать задачу***, выбрать пункт ***Создать задачу на удаление программы*** (рисунок 2.2).

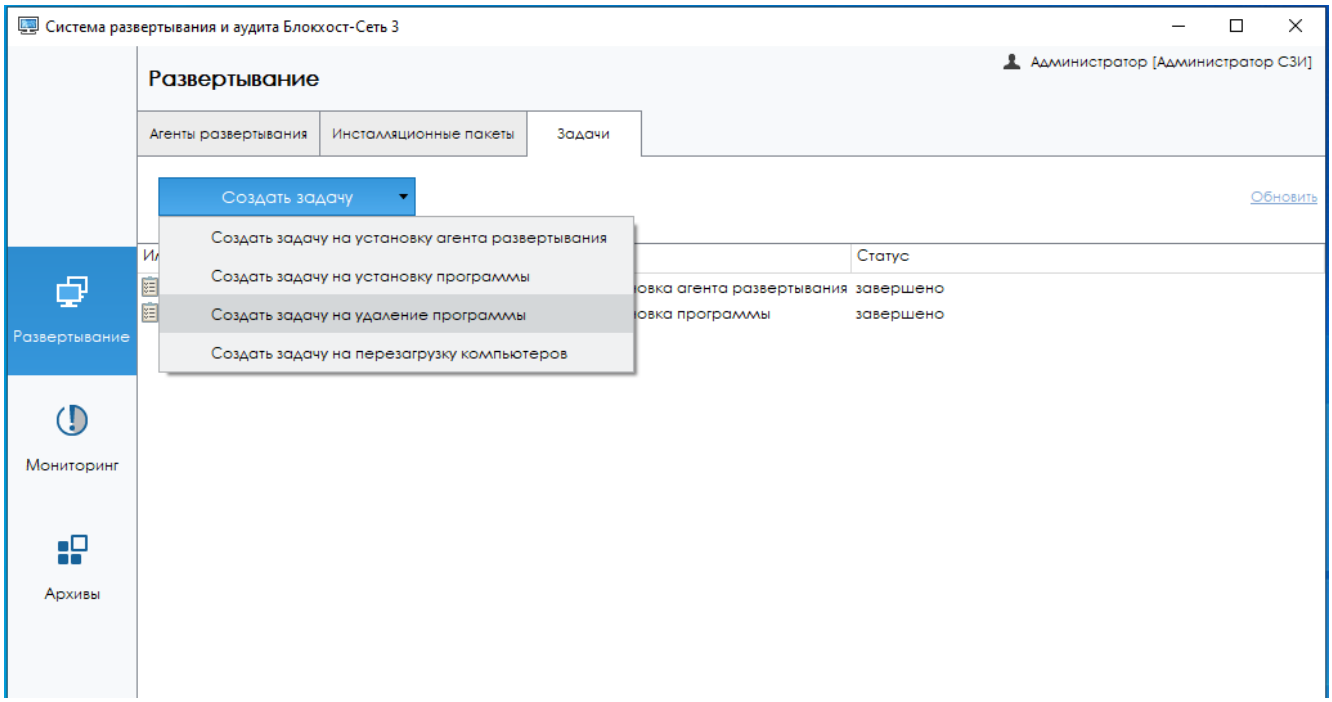


Рисунок 2.2 – Создание задачи на удаление программы

3) В открывшемся окне мастера создания задачи на удаление программы выбрать подзадачу ***Выполнение скрипта для удаления программы*** (рисунок 2.3) и нажать кнопку ***Далее***.

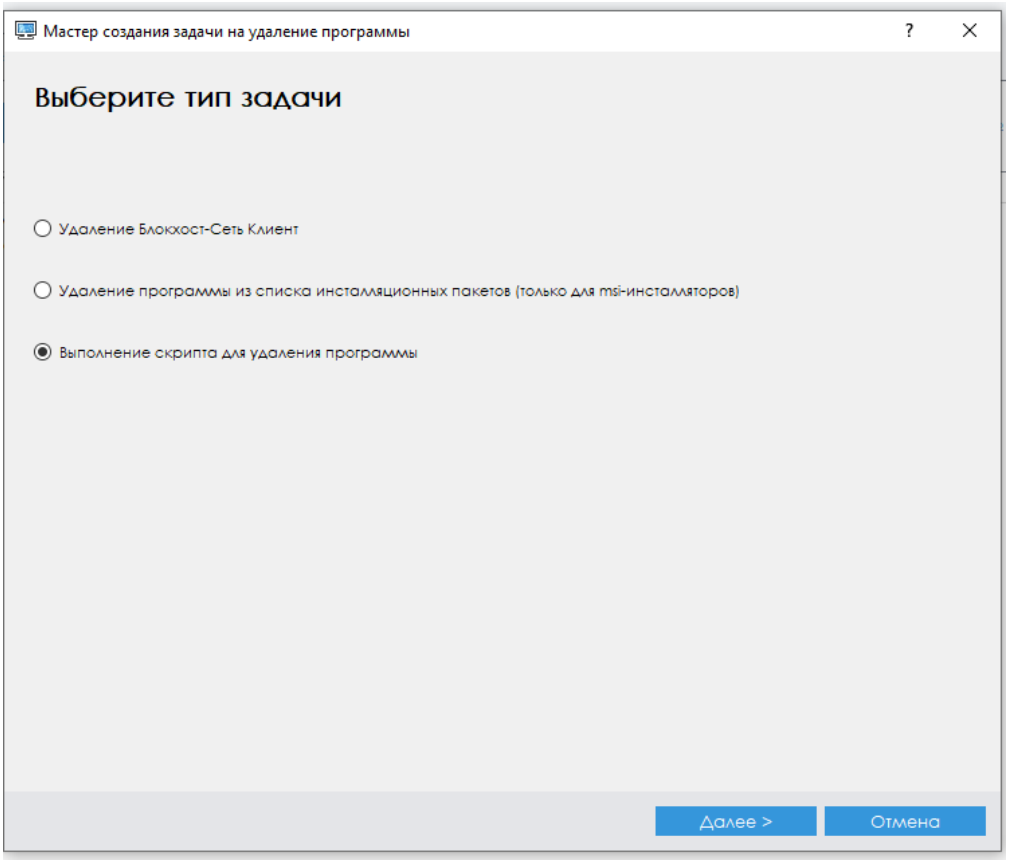


Рисунок 2.3 – Выбор типа задачи

4) В открывшемся окне выбрать созданный файл ***reagent.bat***, нажать ***Далее.***

5) В следующем окне (рисунок 2.4) выбрать из списка все рабочие станции на которых предполагается запуск скрипта для отключения среды восстановления ОС Windows и нажать ***Далее***.

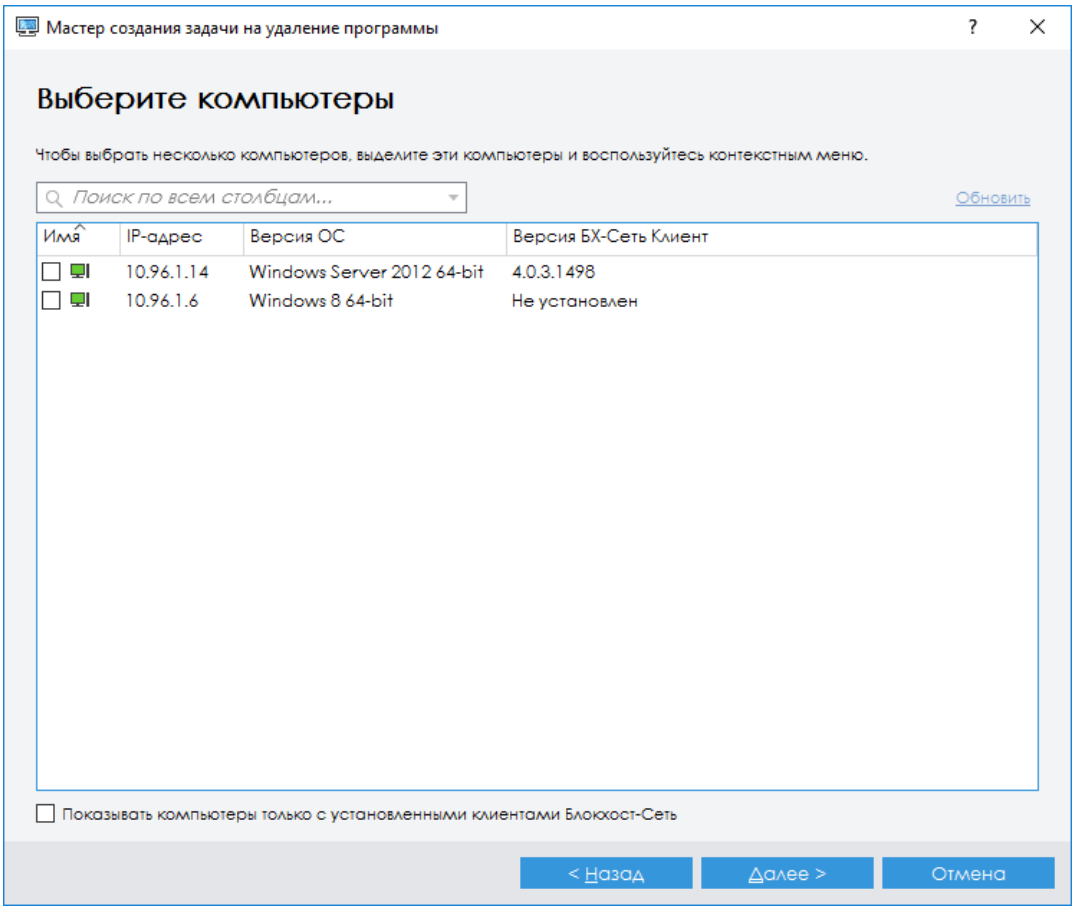


Рисунок 2.4 – Выбор рабочих станций

6) На следующих шагах мастера создания задачи на удаление программы необходимо отредактировать:

- параметры планировщика запуска задачи и определить интервалы времени выполнения задачи;
- параметры перезагрузки рабочей станции.

Более подробно процесс создания задачи на удаление программы описан в пункте 3.3.4 документа «СЗИ «Блокхост-Сеть 3». Руководство администратора безопасности. Система развертывания и аудита».

7) После успешного редактирования всех необходимых параметров, необходимо ввести имя создаваемой задачи и нажать кнопку ***Создать***.

В результате работы мастера создания задачи на удаление программы в список задач будет добавлена новая задача, с указанными в диалоговых окнах мастера параметрами.

В зависимости от установленных параметров планировщика запуск задачи на удаление программ с рабочих станций осуществляется автоматически или вручную. Для запуска созданной задачи вручную необходимо выделить созданную задачу в списке, и в открывшейся панели нажать кнопку ***Запустить***.

3 Подготовка СЗИ «Блокхост-Сеть 3» к работе

3.1 Запуск консоли администрирования СЗИ «Блокхост-Сеть 3»

СЗИ «Блокхост-Сеть 3» включает в себя локальную и серверную консоли администрирования. Локальная консоль администрирования позволяет выполнять настройку СЗИ «Блокхост-Сеть 3» непосредственно на рабочей станции. Серверная консоль администрирования позволяет выполнять удаленное администрирование СЗИ с рабочего места администратора безопасности.

Первый запуск локальной или серверной консолей администрирования СЗИ «Блокхост-Сеть 3» должен осуществляться от имени учетной записи пользователя с правами администратора, и может быть произведен сразу после установки СЗИ или после перезагрузки ОС. Последующие запуски локальной или серверной консолей СЗИ должны осуществлять зарегистрированные в СЗИ пользователи, входящие в группу администраторов ОС Windows рабочей станции (сервера СЗИ) и которые имеют право запуска консоли администрирования СЗИ. Обязательным условием для работы в локальной или серверной консолях СЗИ является вход в систему администраторов СЗИ со значением мандатной метки равным **1**, без ввода категорий.

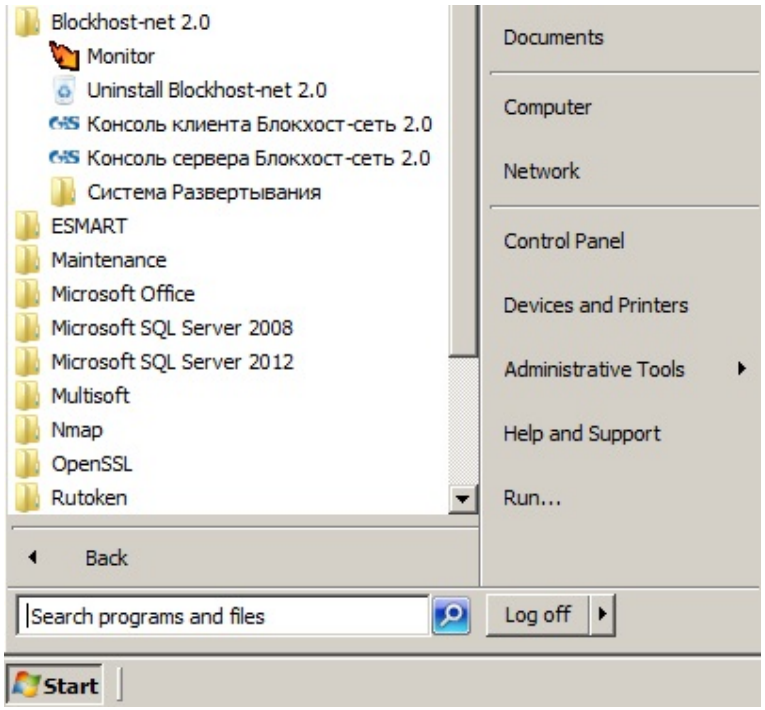


Рисунок 3.1 – Меню вызова консолей администрирования СЗИ в ОС Windows Server 2008R2

Запуск серверной консоли администрирования СЗИ «Блокхост-Сеть 3» осуществляется из меню ***Пуск →Все программы →Блокхост-Сеть 3 →Консоль сервера Блокхост-Сеть 3*** (на рис. 3.1 показано меню для англоязычных ОС). Запуск локальной консоли

администрирования СЗИ «Блокхост-Сеть 3» осуществляется из меню ***Пуск →Все программы →Блокхост-Сеть 3 Клиент →Консоль клиента Блокхост-Сеть 3*** (***Start →All Programms →BlockHost-net 3 Client →Консоль клиента Блокхост-Сеть 3***).

Ярлыки для вызова локальной и серверной консолей администрирования СЗИ «Блокхост-Сеть 3» при использовании ОС Windows 8.1/Server 2012/2012R2 приведены на рисунке 3.2, меню вызова локальной и серверной консолей администрирования СЗИ «Блокхост-Сеть 3» при использовании ОС Windows 10/Server 2016 – на рисунке 3.3.

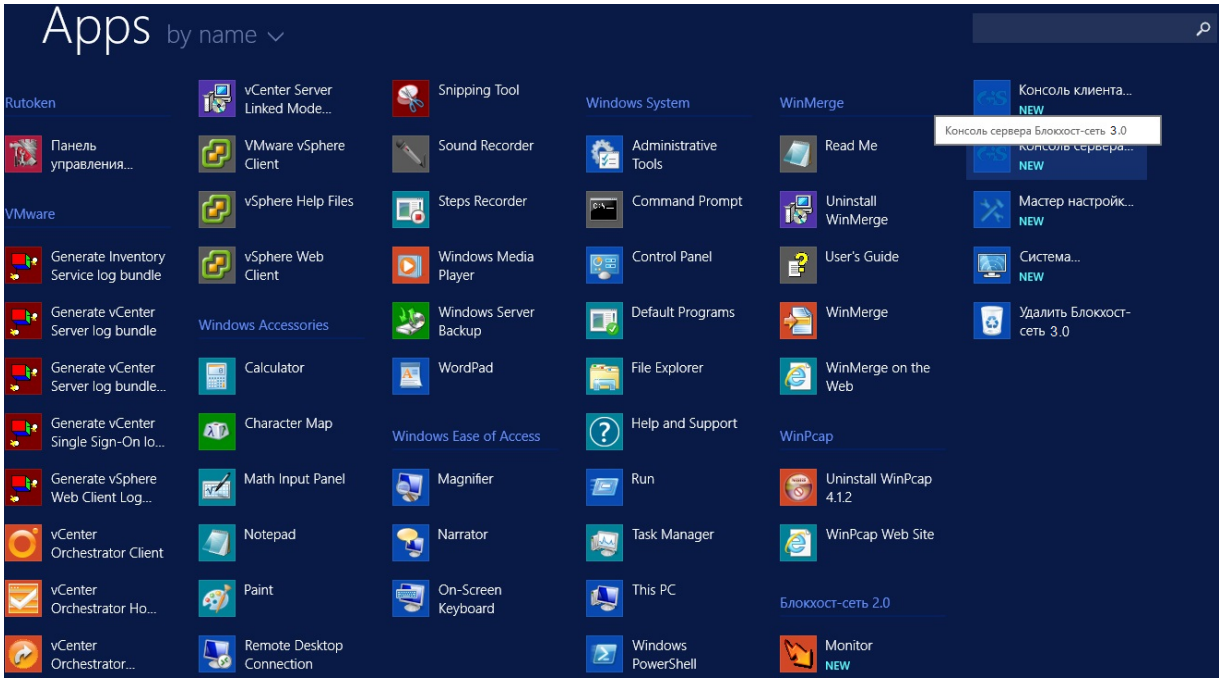


Рисунок 3.2 – Ярлыки вызова консолей администрирования СЗИ в ОС Windows Server 2012

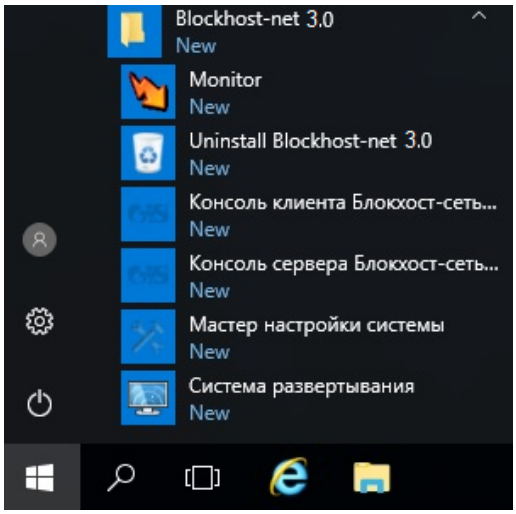


Рисунок 3.3 – Меню вызова консолей администрирования СЗИ в ОС Windows Server 2016

3.2 Консоль администрирования СЗИ «Блокхост-Сеть 3»

Локальная консоль администрирования предназначена для:

- осуществления настроек механизмов разграничения доступа и защиты информации на рабочей станции;
- отображения информации о ресурсах рабочей станции, пользователях, объектах, стоящих на контроле, настройках механизмов защиты информации.

Серверная консоль позволяет выполнять централизованное управление удаленными рабочими станциями с рабочего места администратора безопасности и предназначена для:

- осуществления настроек механизмов разграничения доступа и защиты информации на контролируемых рабочих станциях;
- осуществления настроек серверной части СЗИ;
- отображения информации о ресурсах контролируемых рабочих станций, пользователях, объектах, стоящих на контроле, настройках механизмов защиты информации.

Локальная и серверная консоли администрирования решены в виде единого графического интерфейса администратора безопасности (на рис. 3.4 приведена серверная консоль администрирования СЗИ) и содержат следующие элементы:

- главное меню;
- элементы управления – кнопки;
- дочерние окна: «Список машин», «Лог», «Токены», «Настройки машины» («Настройки группы»);

В серверной консоли администрирования СЗИ содержимое и заголовок окон «**Токены**…» и «**Настройки машины**» изменяются в зависимости от того, какая рабочая станция или группа выбрана в окне «**Список машин**» (подробнее см. п.п. 3.2.4.2 и 3.2.4.3 настоящего руководства).

- вкладка **Основная панель настроек клиентов**.

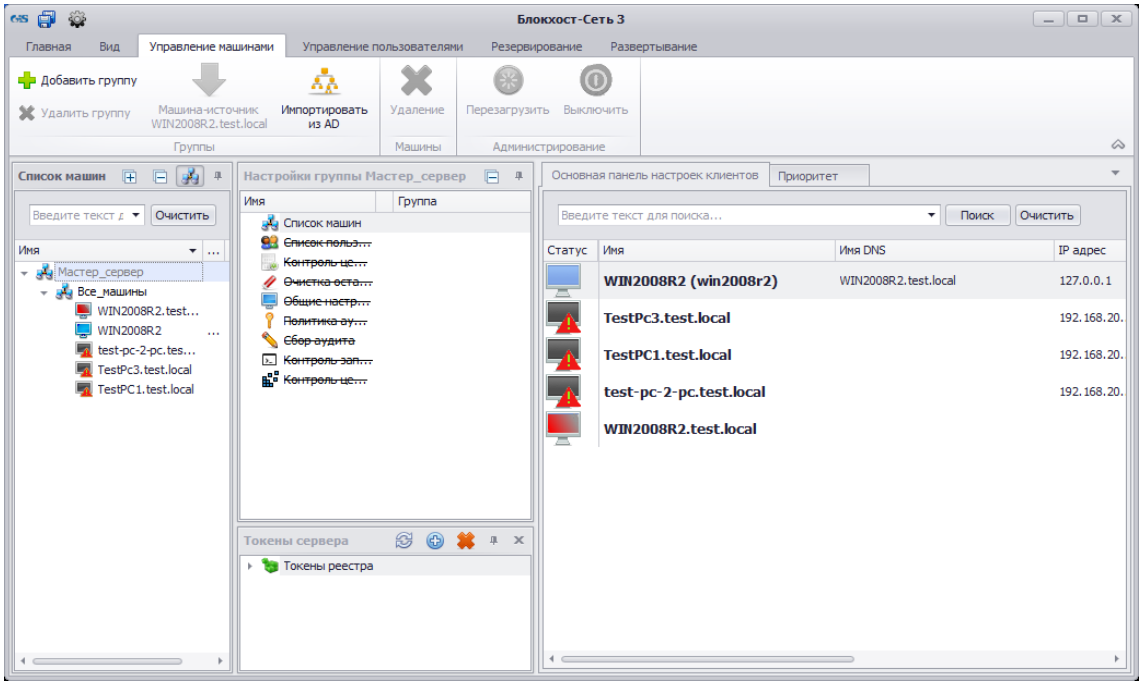


Рисунок 3.4 – Серверная консоль администрирования СЗИ «Блокхост-Сеть 3»

Локальная консоль отображает настройки СЗИ «Блокхост-Сеть 3» только текущей рабочей станции. Настройки механизмов СЗИ в серверной консоли отображаются отдельно для каждой контролируемой рабочей станции. Настройка механизмов защиты СЗИ «Блокхост-Сеть 3» в обеих консолях идентична.

Из серверной консоли СЗИ «Блокхост-Сеть 3 также возможно удаленное управление контролируемыми рабочими станциями (пункты главного меню ***Управление машинами***):

- перезагрузить рабочую станцию;
- выключить рабочую станцию.

3.2.1 Удаленное администрирование параметров СЗИ 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 3» (если в окне **«Список машин»** выделена группа, см. пример на рис. 3.5).

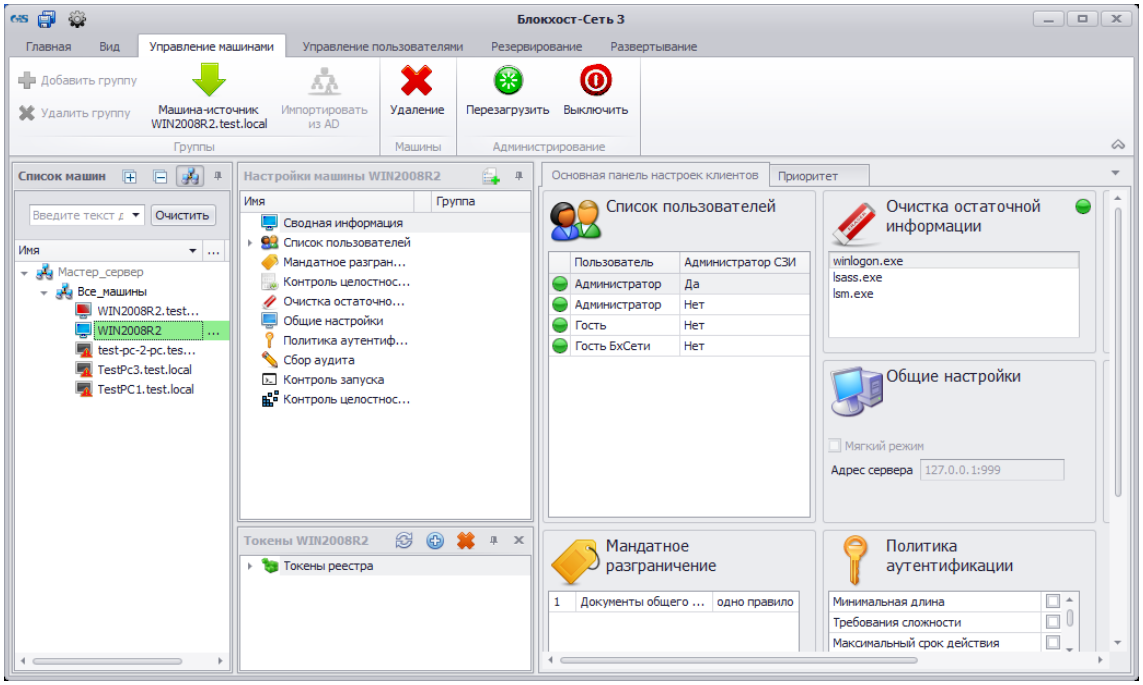


Рисунок 3.5 – Список контролируемых станций

В консоли администрирования СЗИ могут отображаться следующие пиктограммы контролируемых рабочих станций:

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

– 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;

– 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);

– рабочая станция включена, службы СЗИ на ней запущены, происходит процесс загрузки настроек СЗИ рабочей станции на сервер СЗИ;

– рабочая станция включена, службы СЗИ на ней запущены, для возможности изменения настроек СЗИ из серверной консоли необходимо обновить версию

установленной на рабочей станции клиентской части СЗИ.

В контекстном меню контролируемой рабочей станции в серверной консоли имеется пункт ***Обновить*** (рис. 3.6). Выбрав этот пункт контекстного меню можно обновить отображение всех настроек СЗИ конкретной 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.

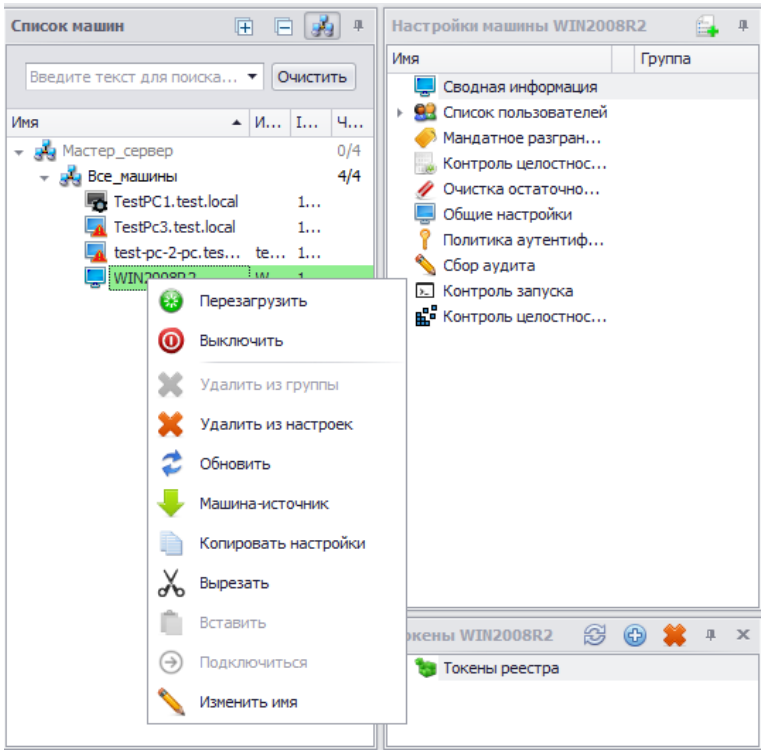


Рисунок 3.6 – Обновление отображения настроек СЗИ рабочей станции

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. 3.7). 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 все***. После сохранения внесенных изменений в настройки механизмов СЗИ повторить операцию обновления их отображения для текущей рабочей станции.

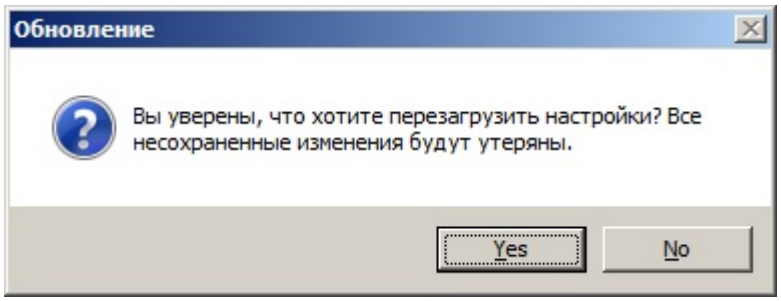


Рисунок 3.7 – Окно-предупреждение о потере внесенных изменений

3.2.2 Локальная консоль администрирования СЗИ «Блокхост-Сеть 3»

3.2.2.1 Основные операции меню локальной консоли СЗИ «Блокхост-Сеть 3»

Меню расположено в верхней части окна локальной консоли и предназначено для управления СЗИ «Блокхост-Сеть 3». Меню позволяет выполнять следующие операции:

- управление настройками пользователей, добавленных в СЗИ рабочей станции (пункты меню ***Управление пользователями***);
- репликация пользовательских механизмов разграничения доступа между пользователями рабочей станции (пункты меню ***Главная →Копировать и Главная →Вставить***);
- резервное копирование и восстановление настроек механизмов СЗИ рабочей станции (пункты меню ***Резервирование***);
- сохранение произведенных настроек СЗИ «Блокхост-Сеть 3» для текущей рабочей станции (пункты меню ***Главная →Сохранить все***);

Необходимо сохранять произведенные изменения в настройках СЗИ рабочей станции перед выходом из локальной консоли администрирования.

3.2.2.2 Резервное копирование и восстановление настроек СЗИ рабочей станции

Резервное копирование настроек СЗИ рабочей станции подразумевает сохранение в зашифрованном файле текущих настроек механизмов СЗИ данной рабочей станции.

Сохранение настроек СЗИ 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;
2) выбрать пункт меню **Резервирование →Резервирование настроек клиента**;
3) в открывшемся окне «**Сохранение настроек**» (рис. 3.8):

- 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.

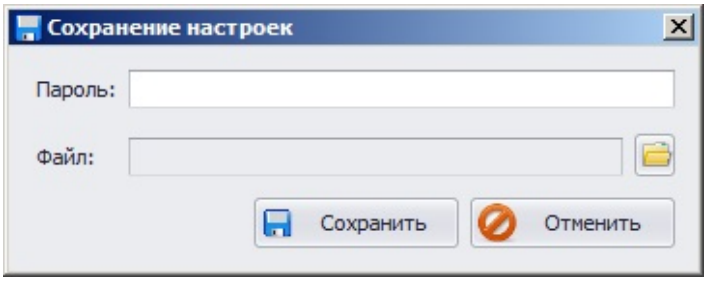


Рисунок 3.8 – Окно сохранения настроек СЗИ

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

1) выделить в окне **«Список машин»** рабочую станцию;
2) выбрать пункт меню Р***езервирование →Восстановление настроек клиента***;
3) в открывшемся окне «**Восстановление настроек**» (рис. 3.9):

- 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***.

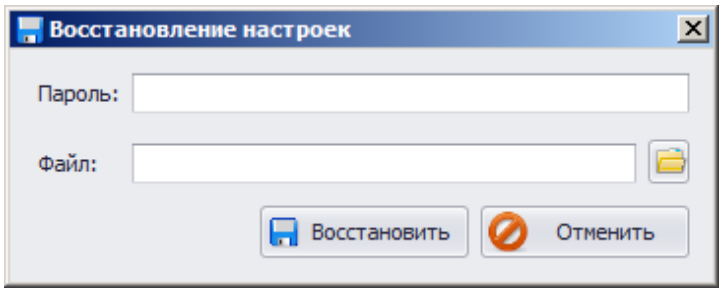


Рисунок 3.9 – Окно восстановления настроек СЗИ

3.2.3 Серверная консоль администрирования СЗИ «Блокхост-Сеть 3»

3.2.3.1 Основные операции меню серверной консоли СЗИ «Блокхост-Сеть 3»

Меню расположено в верхней части окна серверной консоли и предназначено для управления СЗИ «Блокхост-Сеть 3». Меню позволяет выполнять следующие операции:

- создание и удаление групп рабочих станций (пункты меню ***Управление машинами →Добавить группу и Управление машинами →Удалить группу***);
- удаление рабочих станций из списка контролируемых текущим сервером СЗИ (пункт меню ***Управление машинами →Удаление***);
- добавление рабочих станций, с установленным СЗИ, в список контролируемых текущим сервером СЗИ (пункт меню ***Развертывание →Ручное развертывание***);
- удаленное управление контролируемыми рабочими станциями (перезагрузка, выключение: пункты меню ***Управление машинами →Перезагрузить и Управление машинами →Выключить***);
- управление настройками пользователей, добавленных в СЗИ контролируемых рабочих станций (пункты меню ***Управление пользователями***);
- репликация пользовательских механизмов и механизмов станции разграничения доступа между контролируемыми рабочими станциями и их пользователями (пункты меню ***Главная →Копировать и Главная →Вставить***);
- резервное копирование и восстановление настроек текущего сервера СЗИ и контролируемых им рабочих станций (пункты меню ***Резервирование***);
- сохранение произведенных настроек СЗИ «Блокхост-Сеть 3» для текущей рабочей станции (пункт меню ***Главная →Сохранить все***);
- сохранение произведенных настроек СЗИ «Блокхост-Сеть 3» для всех контролируемых рабочих станций (пункт меню ***Главная →Сохранить все***);
- сохранение произведенных настроек на текущем сервере СЗИ «Блокхост-Сеть 3» (пункт меню ***Главная →Сохранить настройки сервера***).

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

3.2.3.2 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**» (см. пример на рис. 3.8):

- 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 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. 3.10);

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.

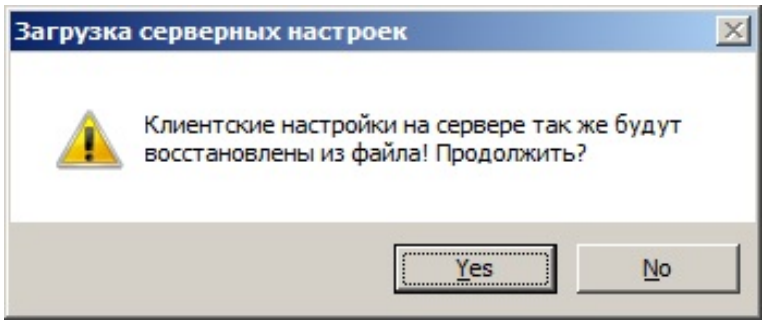


Рисунок 3.10 – Подтверждение восстановления настроек клиентской части СЗИ

3) в открывшемся окне «**Восстановление настроек**» (рис. 3.11):

- 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»**;
- нажать кнопку ***Восстановить***:

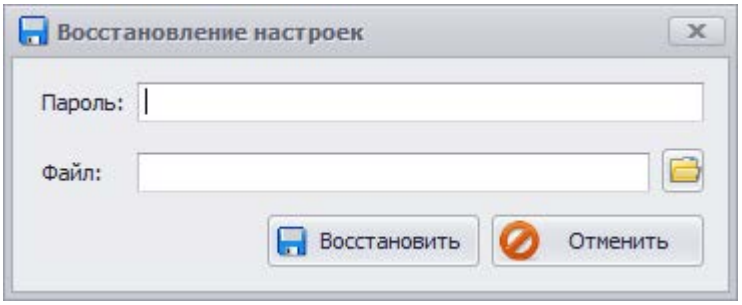


Рисунок 3.11 – Окно восстановления настроек сервера СЗИ

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.

3.2.3.3 Резервное копирование и восстановление настроек СЗИ контролируемой на сервере 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).

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

Порядок выполнения резервного копирования настроек СЗИ рабочей станции в серверной консоли администрирования полностью аналогичен порядку резервирования настроек СЗИ рабочей станции в локальной консоли и подробно описан в п. 3.2.2.2 настоящего руководства.

При необходимости восстановить настройки СЗИ контролируемой рабочей станции также можно из серверной консоли администрирования. Порядок восстановления

настроек СЗИ рабочей станции из серверной консоли администрирования полностью аналогичен порядку восстановления настроек СЗИ рабочей станции в локальной консоли и подробно описан в п. 3.2.2.2 настоящего руководства.

При работе в серверной консоли администрирования СЗИ запрещается при помощи механизма резервного копирования настроек СЗИ переносить настройки СЗИ с одной контролируемой рабочей станции на другую.

3.2.4 Дочерние окна серверной и локальной консолей администрирования

Все дочерние окна серверной и локальной консолей 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:

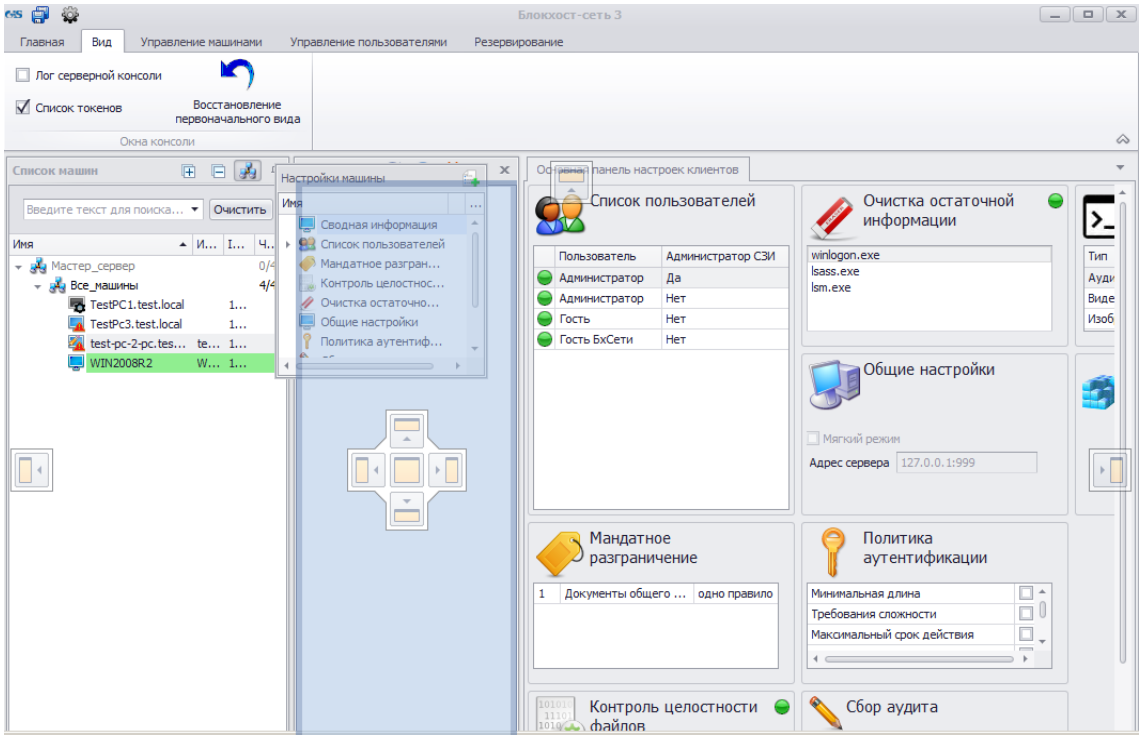


Рисунок 3.12 – Перемещение дочерних окон в окне консоли администрирования

При нажатии на кнопку ***Скрывать автоматически*** , расположенную в правом углу заголовка дочерних окон, их можно свернуть – при этом вкладка, при наведении указателя мыши на которую окно раскроется, будет привязана к левой (для окон **«Список машин»**, **«Настройки машины/группы»** и **«Токены»**) или нижней (для окна **«Лог»**) границе окна консоли администрирования СЗИ.

Для отображения или закрытия дочерних окон **«Токены»** и **«Лог»** необходимо, соответственно, установить или снять флажок напротив имени соответствующего окна в меню ***Вид*** (на рис. 3.13 приведен пример меню ***Вид*** серверной консоли администрирования СЗИ). Для закрытия окон **«Токены»** и **«Лог»** можно также

воспользоваться кнопкой закрытия окна, которая располагается в правом верхнем углу окна.

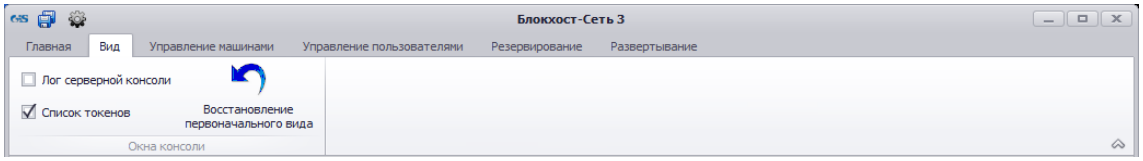


Рисунок 3.13 – Меню «Вид» серверной консоли администрирования СЗИ

Переход между окнами (вкладками) серверной и локальной консолей администрирования СЗИ возможен с использованием «горячих» клавиш. После нажатия комбинации клавиш **<Ctrl>+<Tab>** открывается окно перехода между окнами (вкладками) консоли администрирования СЗИ (рис. 3.14). 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.

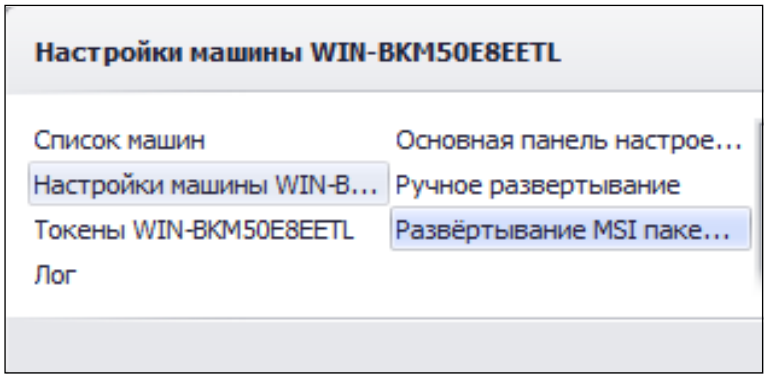


Рисунок 3.14 – Перемещение между окнами (вкладками) с использованием «горячих» клавиш

Внутри окон (вкладок) 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 и т.д.) в выбранном окне консоли.

3.2.4.1 Окно «Список машин»

В окне **«Список машин»** серверной консоли администрирования СЗИ (рис. 3.15) отображаются все рабочие станции, контролируемые на текущем сервере безопасности СЗИ. Рабочие станции могут быть добавлены в список контролируемых данным сервером СЗИ в меню ***Развертывание*** - ***Ручное развертывание***.

Для каждой из контролируемых на сервере СЗИ рабочих станций в окне **«Список машин»** отображается ее имя на сервере СЗИ (графа ***Имя***), имя DNS и IP-адрес. Также в графе ***Численность*** отображается общая численность рабочих станций-клиентов СЗИ, которые контролируются на сервере безопасности. Если в окне **«Список машин»**

установлен режим отображения групп рабочих станций (нажата кнопка ***Показывать группы***), то численность указывается отдельно для каждой из групп.

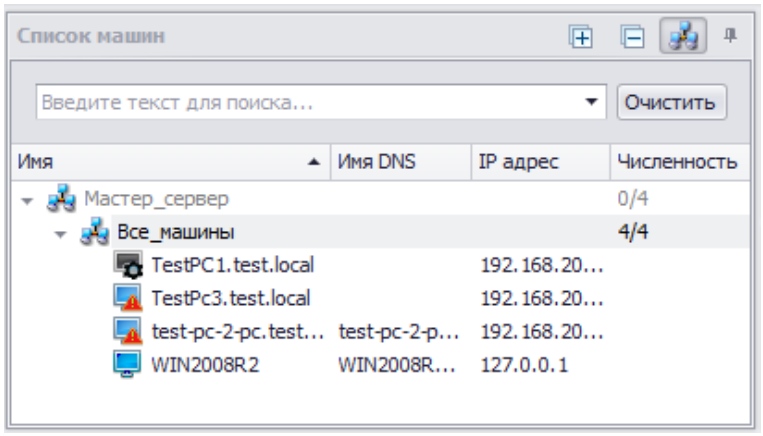


Рисунок 3.15 – Окно «Список машин» серверной консоли администрирования СЗИ

В окне **«Список машин»** локальной консоли администрирования СЗИ отображается только локальная рабочая станция.

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

- кнопки ***Раскрыть все узлы*** и ***Свернуть все узлы*** – расположены в заголовке окна и предназначены, соответственно, для раскрытия списка сгруппированных рабочих станций или отображения только групп рабочих станций;
- кнопка ***Показывать группы*** – расположена в заголовке окна и предназначена для отображения созданных администратором безопасности групп рабочих станций. Кнопка есть только в серверной консоли администрирования;
- кнопка ***Скрывать автоматически*** – служит для минимизации окна, вкладка с заголовком окна привязана к левому краю окна консоли;
- 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***. Поле ввода есть только в серверной консоли администрирования;
- кнопка ***Очистить*** – очищает поле ввода от введенного значения фильтра. Кнопка есть только в серверной консоли администрирования.

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

3.2.4.2 Окно «Настройки машины»

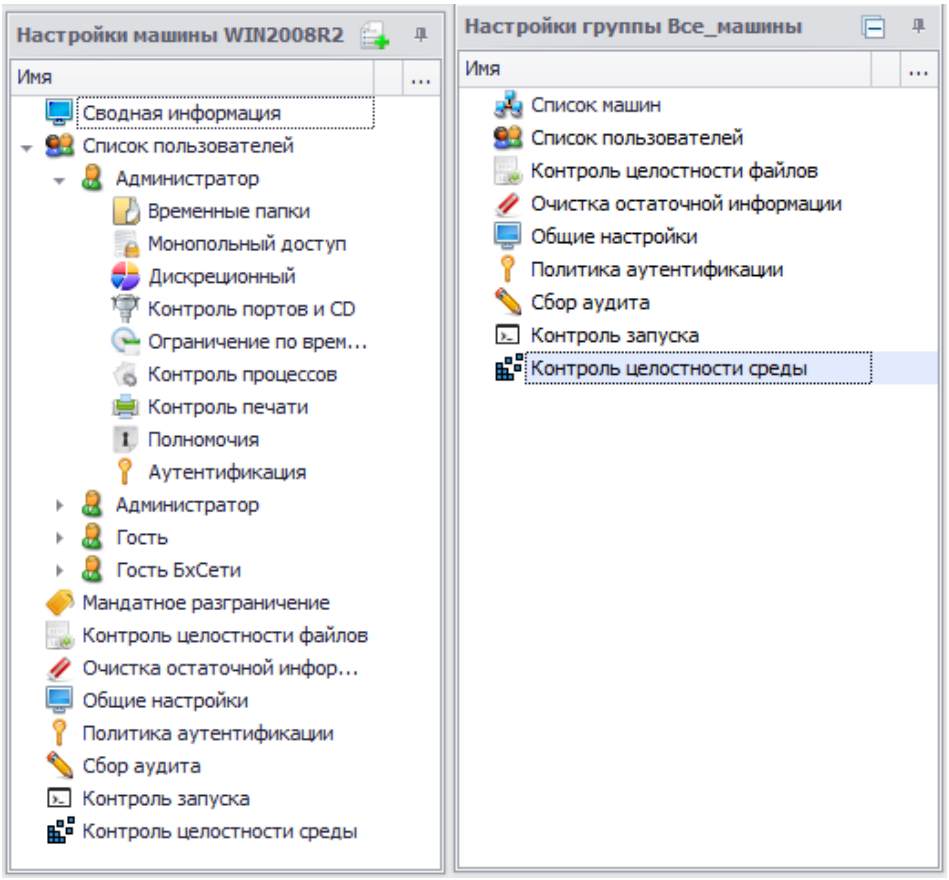
В локальной консоли администрирования СЗИ в окне **«Настройки машины»**

отображены все настраиваемые механизмы разграничения доступа и защиты информации, выделенной в окне **«Список машин»** локальной рабочей станции. Никаких дополнительных элементов управления (кнопок) окно **«Настройки машины»** в локальной консоли не имеет.

В серверной консоли администрирования СЗИ содержимое и заголовок окна зависит от того, какой объект выделен в окне **«Список машин»**:

- рабочая станция – окно имеет заголовок **«Настройки машины <имя_машины_на_сервере_СЗИ>»** с кнопкой ***Скрывать автоматически*** и в ней содержится список всех настраиваемых пользовательских механизмов и механизмов станции СЗИ выделенной в окне «**Список машин**» рабочей станции;
- группа (рис. 3.16) – окно имеет заголовок **«Настройки группы <имя_группы>».** В окне расположены элементы управления:
  - кнопка ***Скрыть неиспользуемые настройки*** – служит для скрытия отображения в окне механизмов СЗИ, настройки которых не будут передаваться на рабочие станции группы при синхронизации. После нажатия кнопка изменяется на ***Показать неиспользуемые настройки***;
  - кнопка ***Скрывать автоматически*** – служит для минимизации окна, вкладка с заголовком окна привязана к левому краю окна консоли;
  - параметр ***Список машин*** – для отображения в **Основной панели настроек клиентов** списка входящих в группу рабочих станций;
  - список пользовательских механизмов и механизмов станции разграничения доступа и защиты информации.

Подробнее о механизме синхронизации настроек механизмов СЗИ на рабочих станциях, включенных в группу в серверной консоли администрирования СЗИ, см. п. 7.1 «Групповая репликация механизмов защиты информации станции» настоящего руководства.



а) б)

Рисунок 3.16 – Окно «Настройки …» серверной консоли администрирования СЗИ

3.2.4.3 Окно «Токены»

В локальной консоли администрирования СЗИ в окне **«Токены»** отображаются, сгруппированные по типам, все подключенные к рабочей станции персональные идентификаторы.

Заголовок и содержимое окна **«Токены»** в серверной консоли администрирования СЗИ 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»** (рис. 3.17), 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.

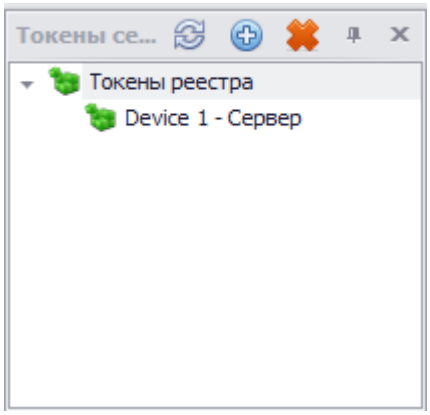


Рисунок 3.17 – Окно «Токены» серверной консоли администрирования СЗИ

В заголовке окна **«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;
- кнопка ***Скрывать автоматически*** – служит для минимизации окна, вкладка с заголовком окна привязана к левому краю окна консоли;
- кнопка ***Закрыть*** – предназначена для закрытия окна. После закрытия окна «**Токены**» для его отображения в окне консоли администрирования СЗИ необходимо отметить пункт меню ***Вид*** →***Список токенов.***

При выборе носителя в окне **«Токены»** возможна настройка его параметров во вкладке **Настройки токена** консоли администрирования СЗИ (подробнее о настройке параметров персонального идентификатора во вкладке **Настройки токена** см. п. 6.2.6 «Механизм идентификаторов входа» настоящего руководства).

3.2.4.4 Окно «Лог»

В окне **«Лог»** отображается результат действий, выполняемых администратором безопасности в консоли администрирования СЗИ. Все сообщения, выводимые в окно **«Лог»**, также регистрируются в файле *short_log.log*, расположенном в каталоге *%LOCALAPPDATA%\BlockPost\Log* профиля пользователя, запустившего консоль.

В случае запуска локальной или серверной консоли администрирования СЗИ 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*, расположенном в каталоге *%LOCALAPPDATA%\BlockPost\Log* профиля

пользователя, запустившего консоль.

В заголовке окна **«Лог»** расположены кнопки ***Скрывать автоматически*** и ***Закрыть***, которые служат, соответственно, для минимизации и закрытия окна **«Лог»** в консоли администрирования СЗИ. После закрытия окна **«Лог»** для его отображения в окне консоли администрирования СЗИ необходимо отметить соответствующий пункт меню ***Вид***.

3.2.4.5 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 3.18 приведен вид вкладки для настройки механизма контроля целостности и дискреционного разграничения доступа.

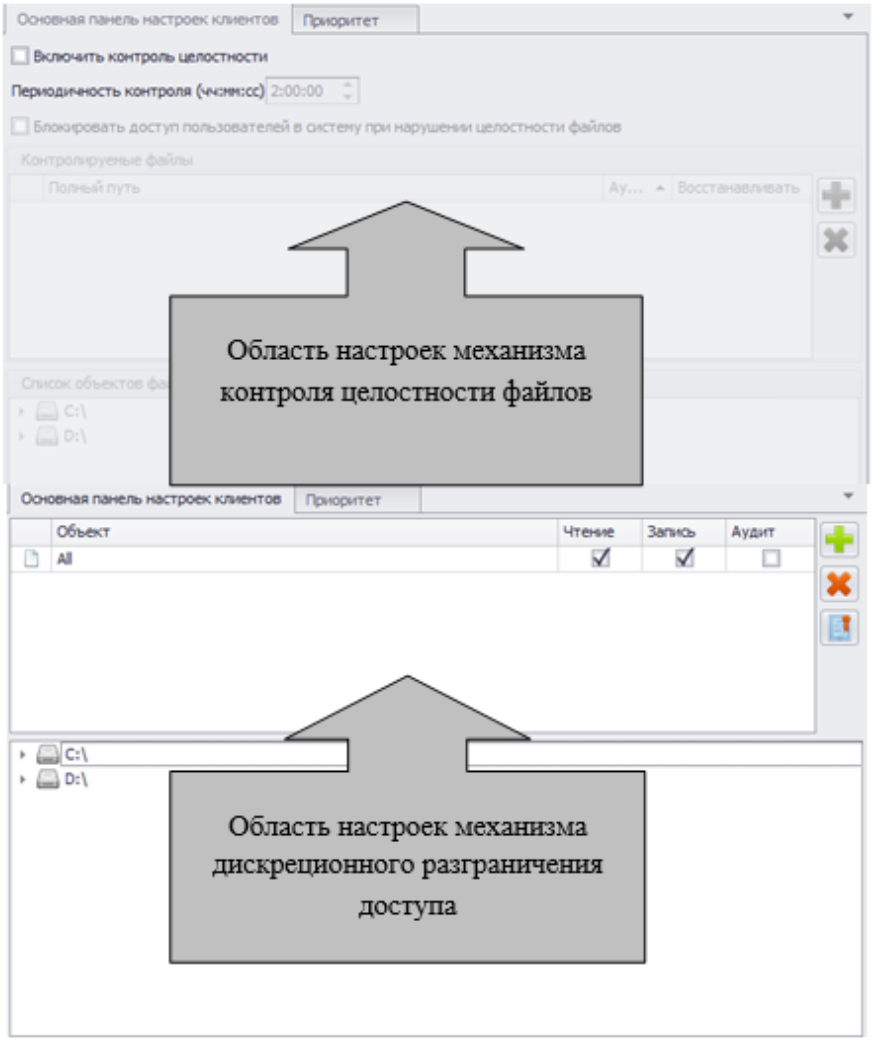


Рисунок 3.18 – Настройки механизмов СЗИ в Основной панели настроек клиентов

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. 3.18), 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.

При редактировании механизмов СЗИ группы в **Основной панели настроек клиентов** отображается файловая структура рабочей станции, выбранной в качестве источника.

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 3.19 показано контекстное меню настройки отображения при выборе механизма настройки параметров пользователей (***Список пользователей***):

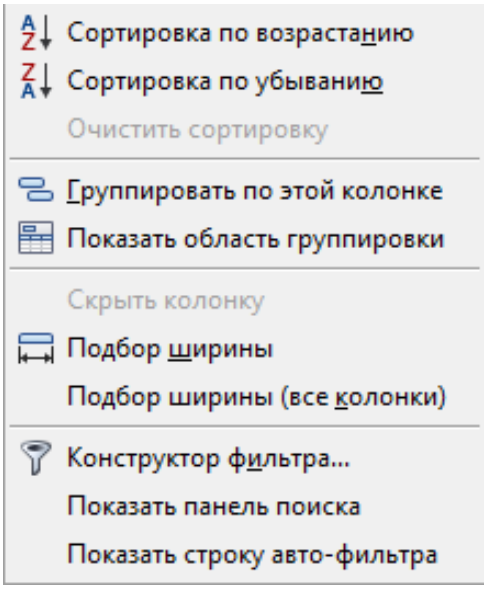


Рисунок 3.19 – Контекстное меню настройки отображения списка объектов (ресурсов)

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. 3.20), в котором можно задать параметры, в соответствии с которыми будут отображены объекты.

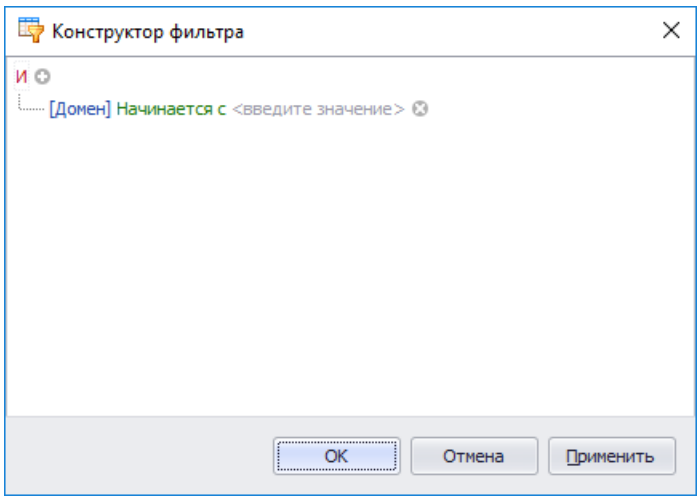


Рисунок 3.20 – Окно конструктора фильтра отображения списка объектов

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 оператора 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 на сервере СЗИ рабочих станций

Для централизованного администрирования СЗИ «Блокхост-Сеть 3» администратору безопасности необходимо:

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

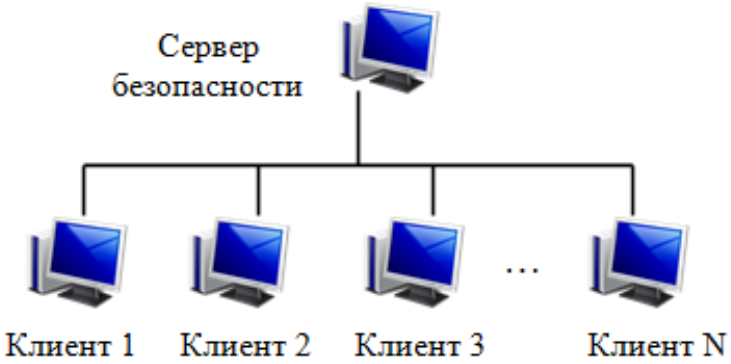


Рисунок 3.21 – Группа рабочих станций

2) Установить серверную часть СЗИ «Блокхост-Сеть 3» на рабочее место администратора безопасности (рис. 3.22) и с использованием ключевого носителя администратора 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 3» на рабочее место администратора безопасности описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство по инсталляции (вариант с удаленным управлением)».

Рисунок 3.22 – Установка и настройка серверной части СЗИ на рабочем месте администратора

3) Установить клиентские части СЗИ «Блокхост-Сеть 3» на защищаемые рабочие станции (локально, или из серверной консоли администрирования СЗИ, или из консоли системы развертывания СЗИ «Блокхост-Сеть 3»):

Рисунок 3.23 – Рабочие станции, подключенные к серверу

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

Рисунок 3.24 – Экспорт настроек на носитель

5) Импортировать с сервера СЗИ настройки и загрузить их на каждую из рабочих станций, вручную сгенерированных в серверной консоли администрирования СЗИ:

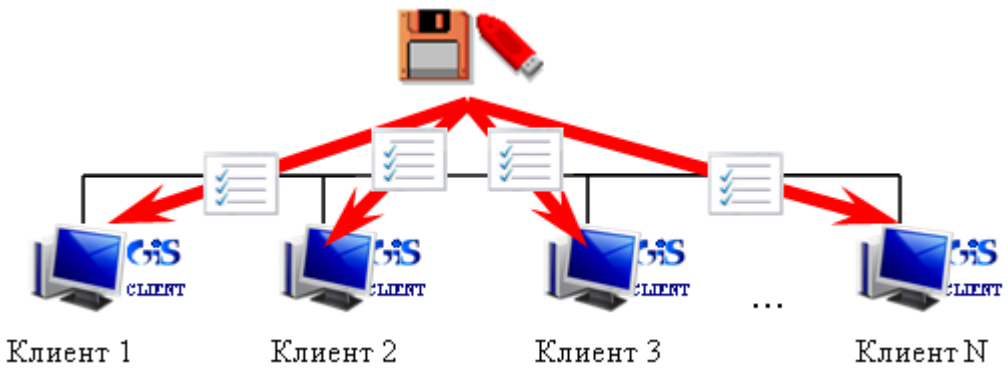


Рисунок 3.25 – Импорт и загрузка настроек на защищаемые рабочие станции

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:

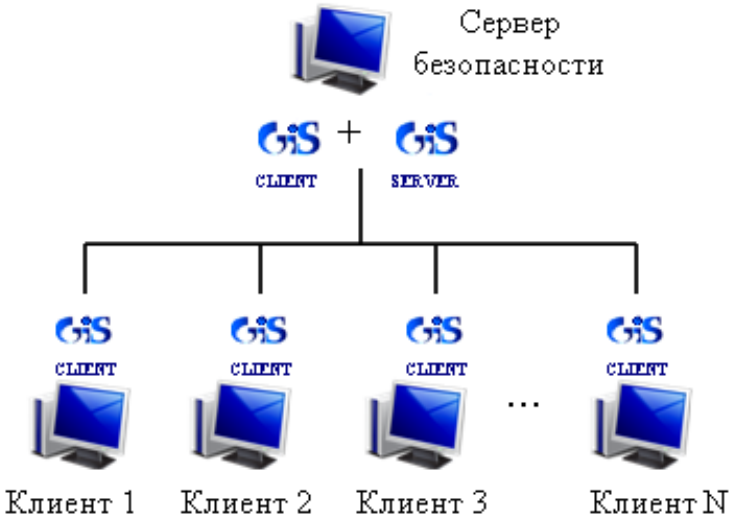


Рисунок 3.26 – Контроль безопасности рабочих станций сервером СЗИ

3.3.2 Настройка серверной части СЗИ «Блокхост-Сеть 3»

Настройка параметров сетевого взаимодействия сервера СЗИ с рабочими станциями, контролируемыми текущим сервером, выполняется администратором в серверной консоли СЗИ «Блокхост-Сеть 3» в следующей последовательности:

1) В серверной консоли администрирования СЗИ «Блокхост-Сеть 3» нажать кнопку ***Настройка параметров сервера « »***, расположенную в левом верхнем углу окна программы;

2) В открывшейся вкладке **Параметры сервера** (рис. 3.27) доступны для изменения следующие параметры:

- ***Идентификатор машины по умолчанию*** – в данном поле указывается идентификатор рабочей станции-клиента СЗИ, с использованием которого будет устанавливаться первичное подключение клиента к серверу СЗИ. После установки соединения с сервером СЗИ этот идентификатор автоматически будет заменен на уникальный. 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 к серверу. Для возможности изменения данного параметра необходимо отметить пункт ***Редактировать***, расположенный справа от поля 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;
- ***Пароль подключения подчиненного сервера*** – на главном сервере СЗИ указывается пароль, при помощи которого осуществляется взаимодействие подчиненного и главного серверов СЗИ;
- ***Пароль подключения*** – на подчиненном сервере СЗИ указывается пароль, при помощи которого осуществляется взаимодействие подчиненного и главного серверов СЗИ;
- ***IP-адрес*** и ***Порт*** – на подчиненном сервере СЗИ указывается IP-адрес и номер TCP-порта главного сервера СЗИ, по которым будет происходить подключение подчиненного сервера к главному серверу СЗИ. Для возможности изменения данного параметра необходимо отметить пункт ***Редактировать***, расположенный справа от поля ввода номера порта сервера.

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

В области *Управление лицензиями* вкладки **Параметры сервера** 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 на сервере лицензий.

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

Для корректного совершения операции по добавлению на сервер СЗИ новой серверной лицензии на сервере должен быть отключен параметр безопасности локальной политики ОС Windows ***Системная криптография: использовать FIPS совместимые алгоритмы для шифрования, хеширования и подписывания.***

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

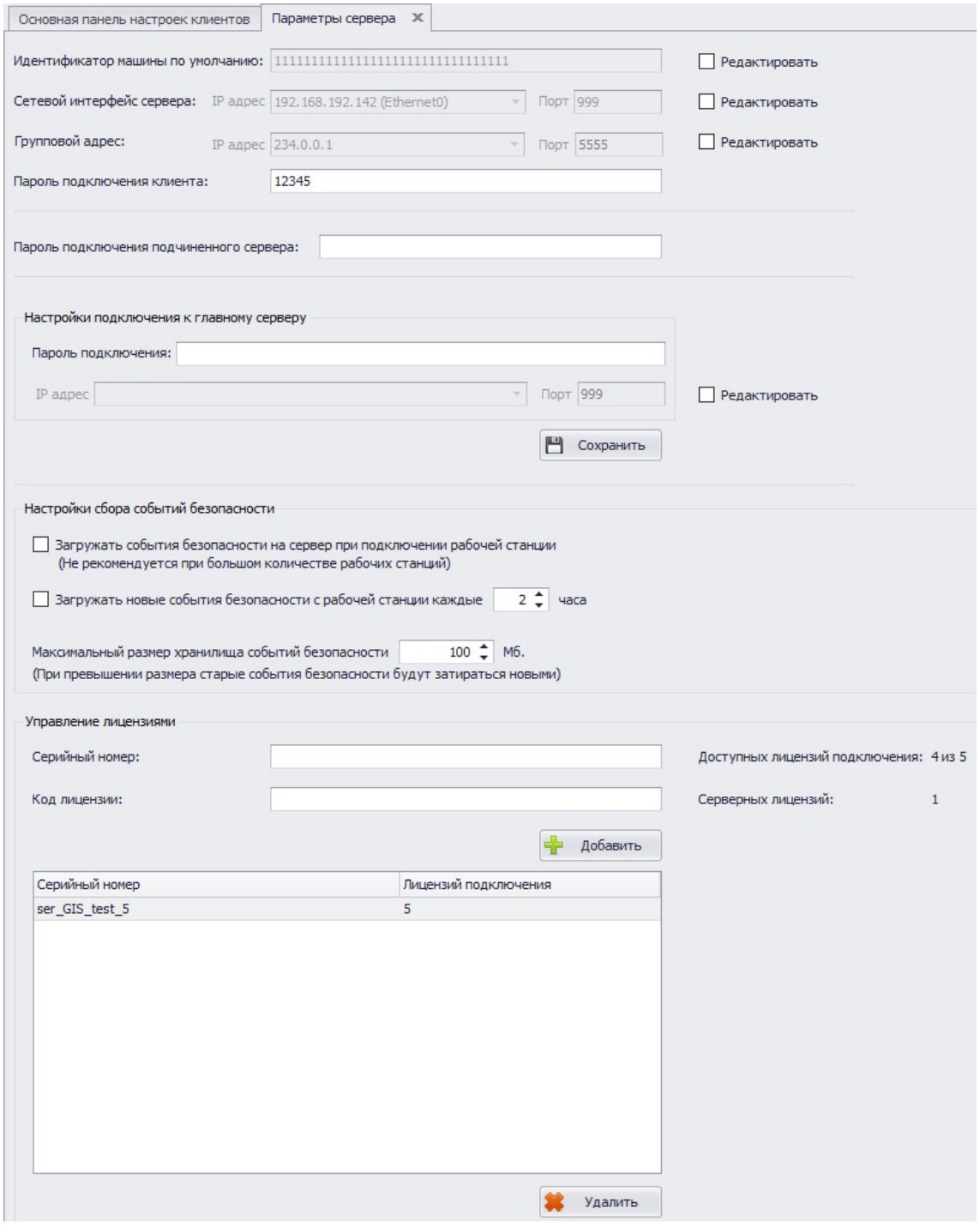


Рисунок 3.27 – Настройка параметров сервера

3.3.3 Порядок формирования списка контролируемых рабочих станций

В серверной консоли СЗИ «Блокхост-Сеть 3» можно добавить на текущий сервер СЗИ рабочие станции из вкладки **Ручное развертывание**.

Общий алгоритм действий администратора безопасности по формированию списка контролируемых рабочих станций из вкладок **Ручное развертывание** включает в себя следующие шаги:

1) В серверной консоли СЗИ в окне **«Список машин»** выделить группу, в которую будут добавлены рабочие станции, в окне **«Настройки группы»** выделить параметр ***Список машин*** и открыть вкладку **Ручное развертывание**. Открытие вкладки осуществляется путем выбора соответствующего пункта главного меню **Развертывание**:

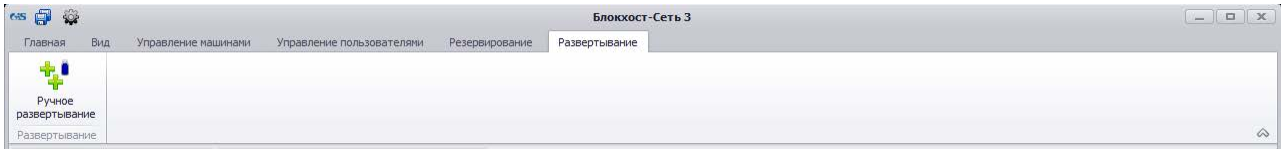


Рисунок 3.28 – Меню «Развертывание»

Пункт меню **Ручное развертывание** становится активными только в том случае, если в окне «***Список машин***» выделена группа, в которую будут добавлены новые рабочие станции.

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**.

Во вкладке **Ручное развертывание** (рис. 3.29) 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.

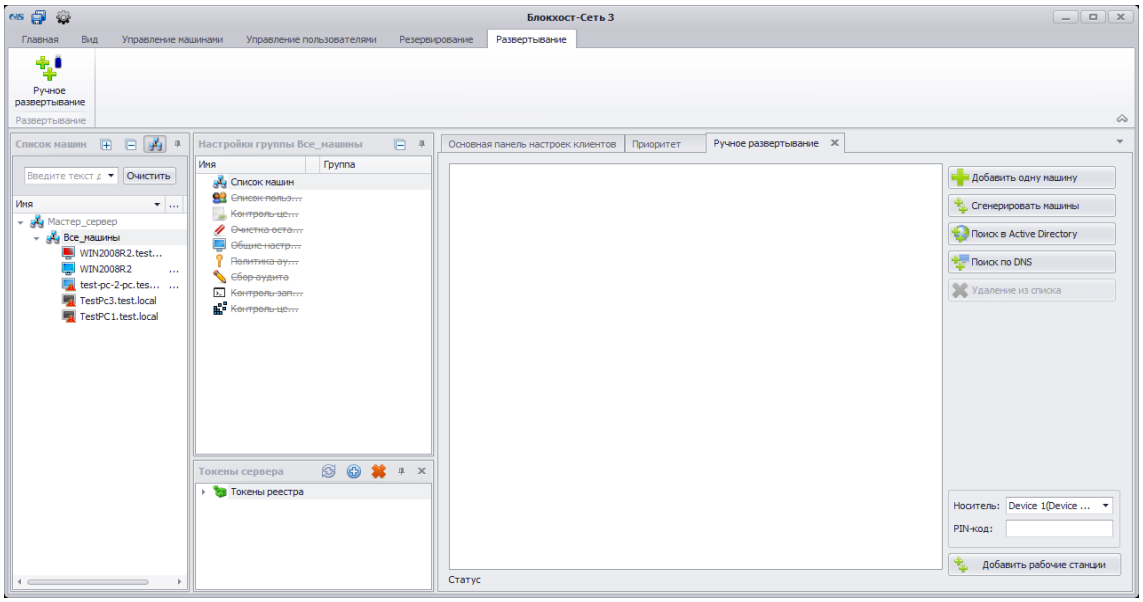


Рисунок 3.29 – Вкладка «Ручное развертывание»

3.3.3.1 Добавление контролируемых рабочих станций

Добавление рабочих станций в СЗИ «Блокхост-Сеть 3» осуществляется через консоль системы развертывания и аудита. Подробно процесс добавления контролируемых рабочих станций описан в разделе 3 «Развертывание» документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

3.3.3.2 Импорт структуры объектов Active Directory на сервер СЗИ

В СЗИ «Блокхост-Сеть 3» реализована возможность импорта на сервер СЗИ рабочих станций, как составных единиц структуры объектов Active Directory – при таком импорте на сервере СЗИ создается группа рабочих станций с именем, соответствующим имени объекта AD и в нее добавляются все рабочие станции, входящие в выбранный объект AD.

Для импорта рабочих станций из структуры объектов AD администратору безопасности необходимо выполнить следующие действия в серверной консоли администрирования СЗИ:

1) В окне «**Управление машинами**» выделить группу ***Мастер_сервер*** и выбрать пункт главного меню ***Управление машинами →Импортировать из AD***;

Если группа ***Мастер_сервер*** не отображается в окне **«Список машин»**, то необходимо нажать кнопку ***Показывать группы***  , расположенную в заголовке окна, для перехода в режим отображения групп рабочих станций.

2) В открывшемся окне **«Импорт структуры разделов из Active Directory»** (рис. 3.30) 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, затем нажать кнопку ***Подключить***.

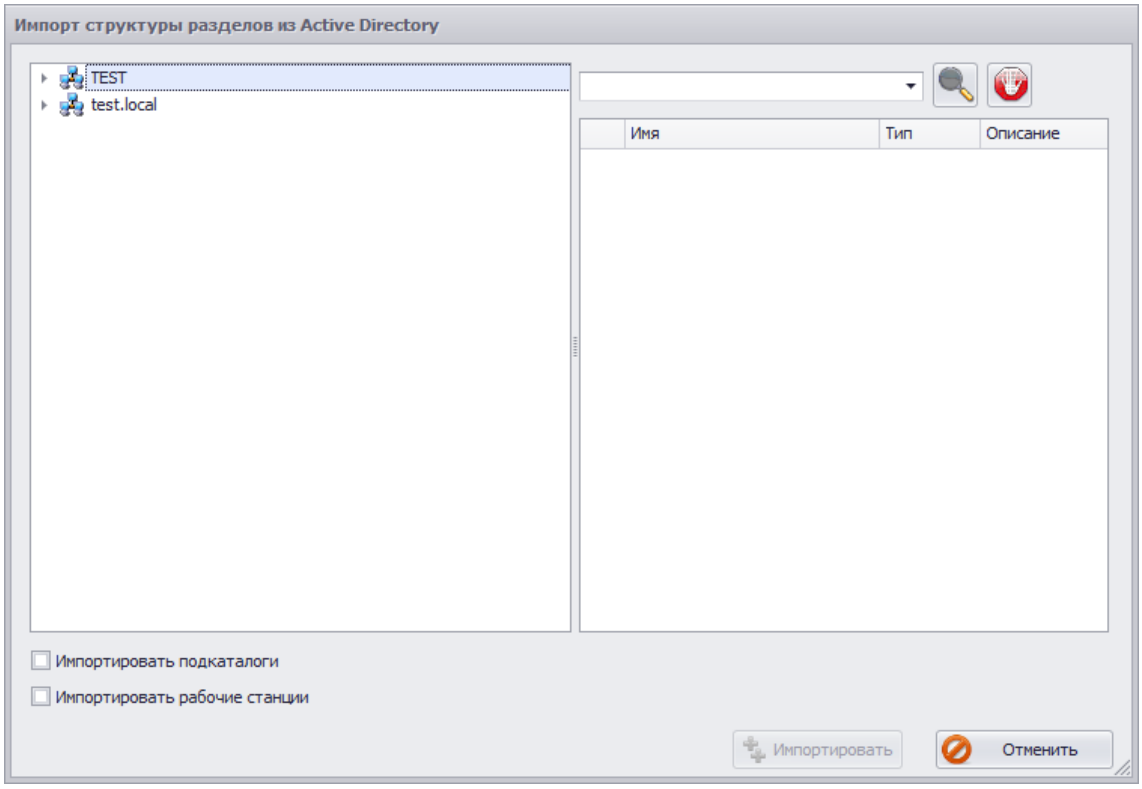


Рисунок 3.30 – Окно импорта структуры разделов из Active Directory

3) В отобразившейся в окне **«Импорт структуры разделов из Active Directory»** структуре объектов Active Directory выделить объект, в котором находятся добавляемые рабочие станции (в примере на рис. 3.31 – это объект ***Computers***), отметить параметр ***Импортировать рабочие станции*** и нажать кнопку ***Импортировать***.

В результате на сервере СЗИ будет создана группа рабочих станций, имя которой совпадает с именем выбранного объекта AD, и в нее будут добавлены все рабочие станции, которые входят в выбранный объект AD, если эти рабочие станции не были добавлены на сервер СЗИ ранее каким-либо другим способом.

Если при импорте структуры объектов AD не отмечать параметр ***Импортировать рабочие станции***, то на сервере СЗИ будет создана только группа рабочих станций, имя которой совпадает с именем выбранного объекта AD, – рабочие станции, входящие в выбранный объект AD не будут добавлены на сервер СЗИ.

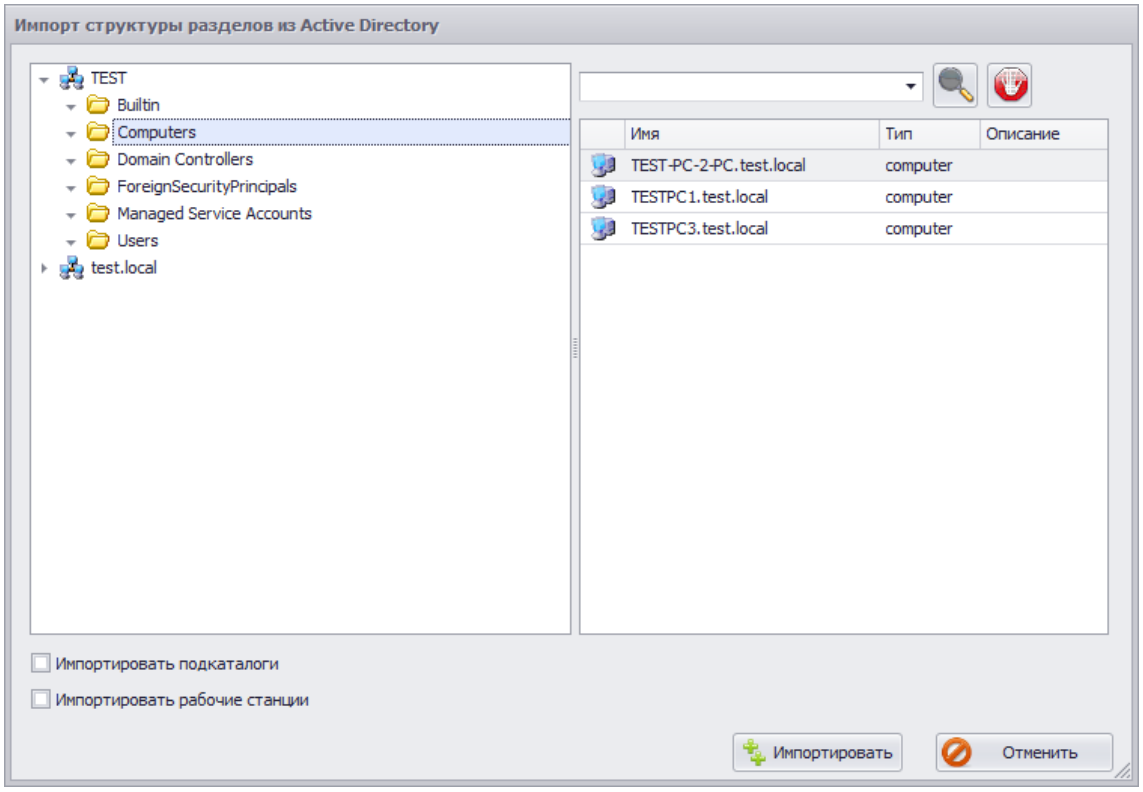


Рисунок 3.31 – Отображение списка рабочих станций в структуре объектов AD

Если отметить параметр ***Импортировать подкаталоги***, то на сервер СЗИ будут добавлены группы рабочих станций, иерархически повторяющие структуру объектов AD. При отмеченном параметре ***Импортировать рабочие станции***, в группы рабочих станций, добавленные на сервер СЗИ, будут добавлены и рабочие станции, входящие в выделенный и во все вложенные в него объекты AD:

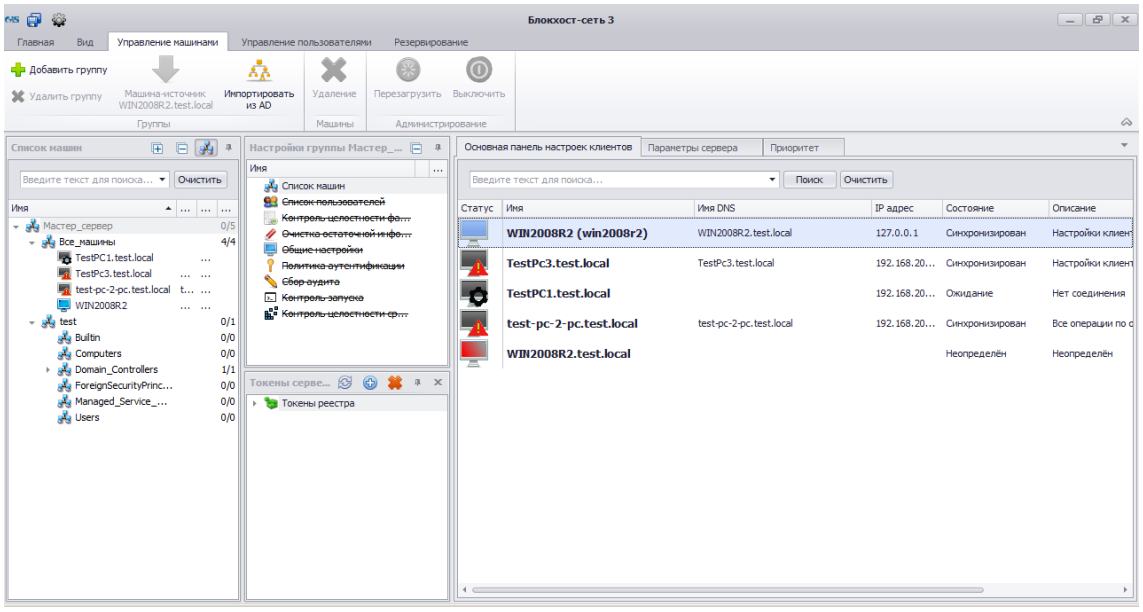


Рисунок 3.32 – Импортированная на сервер СЗИ структура объектов AD

3.4 Иерархия серверов СЗИ

В СЗИ «Блокхост-Сеть 3» существует возможность распространения настроек СЗИ с одного (**главного**) сервера СЗИ на рабочие станции, которые подключены к другому (**подчиненному**) серверу СЗИ. Для осуществления такой возможности администратору безопасности необходимо выполнить следующие действия:

1) В серверной консоли администрирования СЗИ **главного** сервера СЗИ ввести пароль для подключения подчиненного сервера СЗИ (см. п. 3.4.1 Настройка главного сервера СЗИ» настоящего руководства).

2) В серверной консоли администрирования СЗИ **подчиненного** сервера ввести параметры подключения к главному серверу СЗИ (см. п. «3.4.2 Настройка подчиненного сервера СЗИ» настоящего руководства).

3) В серверной консоли администрирования СЗИ **главного** сервера настроить механизмы СЗИ для группы рабочих станций, в которую входит подчиненный сервер, и выполнить синхронизацию настроек группы (подробнее о синхронизации см. раздел 7 «Группирование объектов» настоящего руководства).

4) В серверной консоли администрирования СЗИ подчиненного сервера выполнить синхронизацию механизмов СЗИ на рабочие станции, подключенные к подчиненному серверу СЗИ (подробнее о синхронизации см. раздел 7 «Группирование объектов» настоящего руководства).

Также существует возможность полного управления настройками СЗИ подчиненного сервера. Подробнее см. п. 3.4.4. «Передача настроек механизмов СЗИ в консоль подчиненного сервера».

3.4.1 Настройка главного сервера СЗИ

Настройка главного сервера СЗИ для возможности подключения к нему подчиненного сервера заключается в установке пароля для подключения подчиненного сервера СЗИ к главному.

Для установки пароля, с использованием которого будет происходить подключение подчиненного сервера СЗИ к главному, необходимо выполнить в серверной консоли администрирования главного сервера СЗИ следующие действия:

1) Нажать кнопку ***Настройка параметров сервера***  , расположенную в левом верхнем углу окна серверной консоли администрирования СЗИ.

2) В открывшейся вкладке **Параметры сервера** (см. пример на рис. 3.33) ввести пароль подключения подчиненного сервера в соответствующее поле:

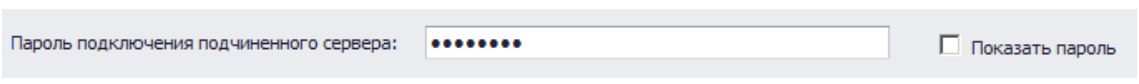


Рисунок 3.33 – Поле ввода пароля подключения подчиненного сервера СЗИ

3) Нажать кнопку ***Сохранить***, расположенную во вкладке **Параметры сервера**.

3.4.2 Настройка подчиненного сервера СЗИ

Настройка подчиненного сервера СЗИ для возможности подключения к главному серверу заключается во вводе параметров подключения к главному серверу СЗИ.

Для ввода параметров подключения к главному серверу СЗИ необходимо в серверной консоли администрирования СЗИ подчиненного сервера:

1) Нажать кнопку ***Настройка параметров сервера***  , расположенную в левом верхнем углу окна серверной консоли администрирования СЗИ.

2) В открывшейся вкладке **Параметры сервера** в области *Настройки подключения к главному серверу* ввести в поле ***Пароль подключения*** пароль, который был указан в поле ***Пароль подключения подчиненного сервера*** в серверной консоли администрирования СЗИ главного сервера (см. пример на рис. 3.34).

3) Отметить параметр ***Редактировать*** и ввести в соответствующие поля IP-адрес и TCP-порт (по умолчанию ***999***) главного сервера СЗИ:

Рисунок 3.34 – Поле ввода пароля подключения подчиненного сервера СЗИ

4) Нажать кнопку ***Сохранить***, расположенную во вкладке **Параметры сервера**.

3.4.3 Просмотр настроек СЗИ рабочих станций на подчиненном сервере СЗИ

После выполнения настроек соединения на главном и подчиненном серверах СЗИ в серверной консоли администрирования СЗИ главного сервера в списке машин группы ***Все_машины*** появится подчиненный сервер, и станет доступна возможность **просмотра** настроек СЗИ рабочих станций, подключенных к подчиненному серверу, в том числе и настройки СЗИ клиентской части подчиненного сервера.

Выполнить настройку механизмов СЗИ подчиненного сервера из серверной консоли главного сервера СЗИ нельзя.
Также нельзя выполнить настройку механизмов СЗИ подчиненного сервера и подключенных к нему рабочих станций из окна открытой на главном сервере СЗИ консоли администрирования СЗИ подчиненного сервера – консоль администрирования СЗИ подчиненного сервера открывается на главном сервере в режиме ***Чтение***.

> Настройка механизмов СЗИ, подключенных к подчиненному серверу рабочих станций, в том числе и самого подчиненного сервера, может быть выполнена в консоли администрирования СЗИ главного сервера с использованием механизма синхронизации настроек СЗИ группы рабочих станций, в которую входит подчиненный сервер.

Для перехода к просмотру настроек СЗИ рабочих станций, подключенных к подчиненному серверу СЗИ необходимо:

1) в окне **«Список машин»** серверной консоли администрирования главного сервера СЗИ выделить подчиненный сервер;

2) щелкнуть по его имени правой кнопкой мыши и в открывшемся контекстном меню выбрать пункт ***Подключиться***:

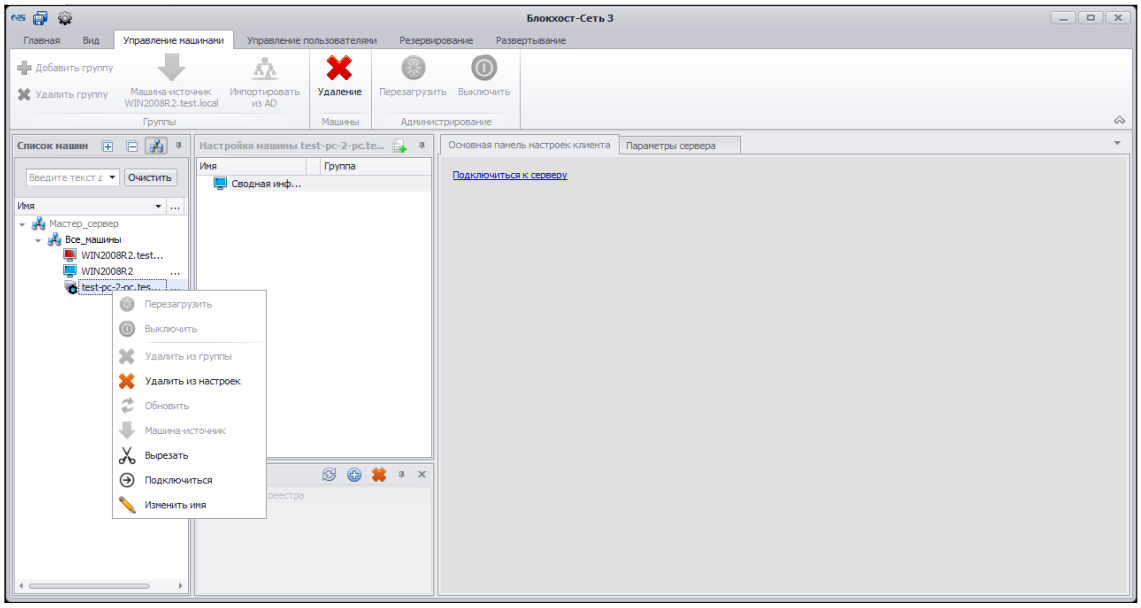


Рисунок 3.35 – Контекстное меню подчиненного сервера СЗИ

3) в открывшейся консоли администрирования СЗИ подчиненного сервера просмотреть настройки СЗИ подчиненного сервера и подключенных к нему рабочих станций-клиентов:

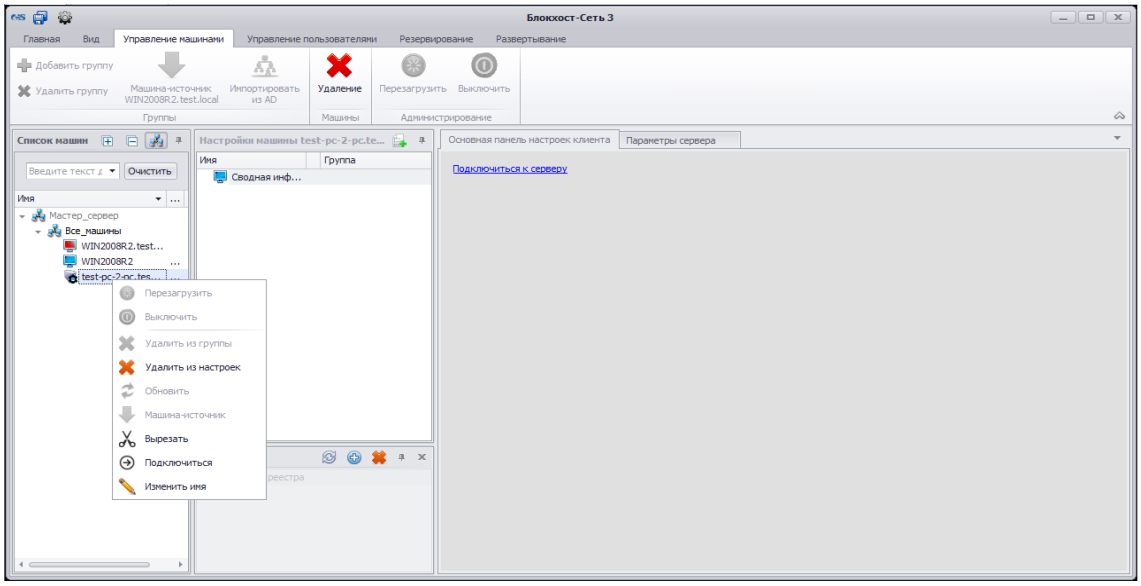


Рисунок 3.36 – Серверная консоль администрирования СЗИ подчиненного сервера

В заголовке окна серверной консоли администрирования СЗИ подчиненного сервера отображается имя учетной записи подчиненного сервера.

3.4.4 Передача настроек механизмов СЗИ в консоль подчиненного сервера

В серверной консоли администрирования СЗИ главного сервера существует возможность непосредственного редактирования настроек СЗИ подчиненного сервера и рабочих станций, которые на нем контролируются. При выделении в окне **«Список машин»** имени подчиненного сервера в **Основной панели настроек клиента** отобразится надпись: ***Подключиться к серверу*** (рис. 3.37).

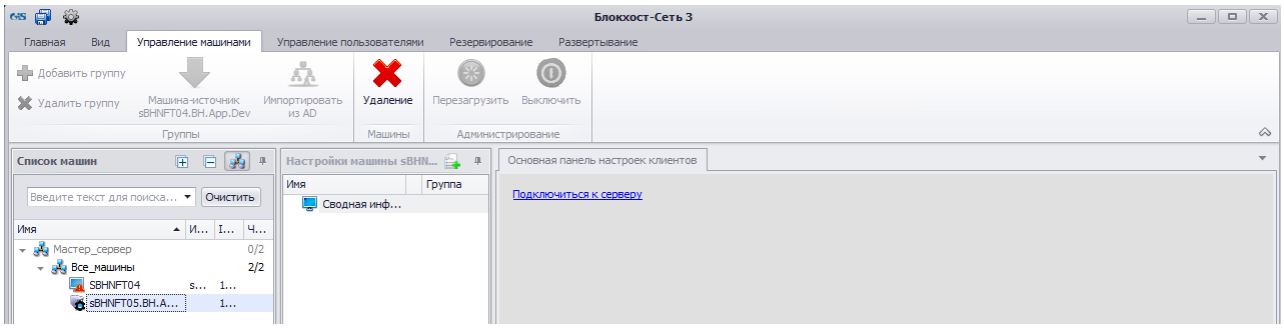


Рисунок 3.37 – Передача настроек механизмов СЗИ подчиненному сервера

АБ может подключиться к серверной консоли подчиненного сервера для управления настройками подчиненного сервера. При подключении к серверу открывается серверная консоль подчиненного сервера в режиме «Только для чтения». Для управления настройками подчиненного сервера необходимо нажать на кнопку «» для проверки полного доступа к консоли, подключиться к консоли подчиненного сервера и выполнить все необходимые настройки механизмов.

Если полный доступ к консоли уже используется на подчиненном сервере, АБ будет выведено сообщение об ошибке (рисунок 3.38).

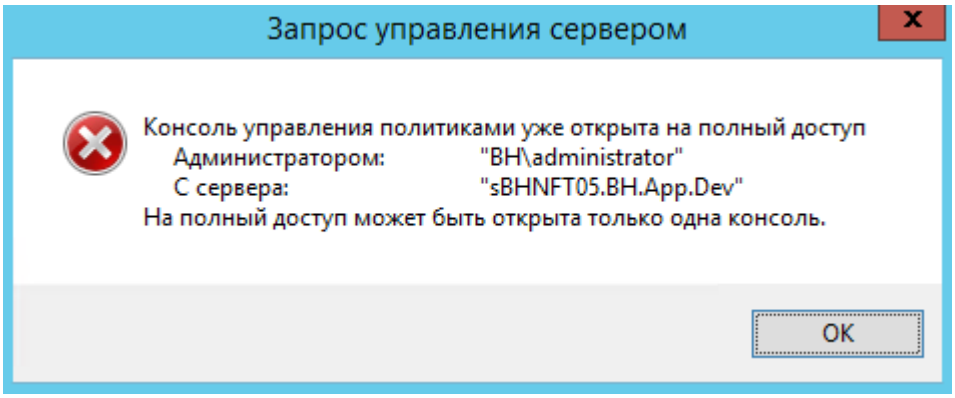


Рисунок 3.38 – Ошибка сохранения изменений в настройках механизмов СЗИ

Для передачи настроек СЗИ «Блокхост-Сеть 3» также реализована возможность передачи настроек механизмов СЗИ, выполненных в серверной консоли главного сервера в серверную консоль подчиненного сервера.

Для передачи настроек механизмов СЗИ в серверную консоль подчиненного сервера необходимо в серверной консоли главного сервера выполнить настройку механизмов СЗИ для группы рабочих станций, в которую входит подчиненный сервер, и сохранить внесенные изменения в параметры настроек механизмов станции СЗИ группы, для чего выбрать пункт меню ***Главная*** → ***Сохранить все***, или нажать кнопку ***Сохранить все*** , расположенную в левом верхнем углу консоли администрирования СЗИ

В результате настройки, выполненные в серверной консоли администрирования СЗИ главного сервера, будут переданы в группу ***Мастер_сервер*** консоли администрирования СЗИ подчиненого сервера, откуда автоматически распространятся на все группы рабочих станций, которые имеются в серверной консоли администрирования СЗИ подчиненного сервера.

4 Защищенный вход в систему

4.1 Вход в систему

Подсистема аутентификации СЗИ «Блокхост-Сеть 3» основана на единовременном применении политики аутентификации, использующейся в домене Windows, и политики аутентификации, установленной для пользователя (группы пользователей) в СЗИ. Если идентификационные данные учетной записи пользователя (группы пользователей) не удовлетворяют хотя бы одной из этих политик, то попытка входа пользователя в ОС будет неудачной.

В подсистеме аутентификации СЗИ «Блокхост-Сеть 3» существует несколько режимов работы:

- вход в систему по паролю, вводимому пользователем с клавиатуры;
- вход в систему по ключевому носителю с паролем (пароль в зашифрованном виде хранится на ключевом носителе);
- вход в систему с предъявлением цифрового сертификата, записанного на ключевом носителе.

Более подробно о режимах аутентификации СЗИ см. п. «4.2 Виды входа в ОС» настоящего руководства.

Общая схема работы механизма аутентификации пользователя в СЗИ «Блокхост-Сеть 3» реализована следующим образом: идентификационные данные пользователя (имя учетной записи, пароль и, в случае двухфакторной аутентификации, предъявленный аппаратный идентификатор пользователя и PIN-код доступа к нему) проверяются на контролере домена и в локальной базе данных клиента СЗИ. На контроллере домена осуществляется проверка введенных имени учетной записи и пароля пользователя. СЗИ «Блокхост-Сеть 3» осуществляет следующие проверки (в зависимости от выбранного режима аутентификации):

- соответствие пароля требованиям сложности, установленным в СЗИ;
- сверка введенного пароля с копией в локальной базе данных клиента СЗИ (в режиме аутентификации пользователя без использования аппаратного идентификатора);
- PIN-код доступа к предъявленному аппаратному идентификатору пользователя;
- наличие у учетной записи пользователя возможности интерактивного входа в ОС Windows.

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

Механизм аутентификации СЗИ «Блокхост-Сеть 3» можно полностью отключить, активировав ***Мягкий режим*** работы СЗИ (подробнее о ***Мягком режиме*** работы СЗИ см.

п. «6.2.5 Механизм мягкого режима» настоящего руководства). При включенном ***Мягком режиме*** вход в операционную систему может выполнить любой доменный или локальный пользователь рабочей станции, если это не противоречит установленным в домене политикам.

Мягкий режим работы, а также режим аутентификации ***Доверять аутентификации Windows*** (данный режим автоматически устанавливается при добавлении новых учетных записей в СЗИ) используются для первичной настройки средства защиты, до начала эксплуатации. В данных режимах средство защиты не обеспечивает выполнение заявленных функций безопасности. Эксплуатировать СЗИ в описанных режимах для защиты станции **запрещено**.

Реализованный в СЗИ «Блокхост-Сеть 3» механизм двухфакторной аутентификации позволяет усилить защищенность входа рабочей станции за счет использования, помимо идентификационных данных пользователя, аппаратных идентификаторов.

В СЗИ «Блокхост-Сеть 3» основными возможностями механизма защиты входа являются:

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

Основными функциями администратора безопасности по защите входа в систему с использованием СЗИ «Блокхост-Сеть 3» являются:

- организация и поддержка работы пользователей с аппаратными персональными идентификаторами;
- управление режимом входа пользователей в систему и режимом усиленной аутентификации;
- настройка параметров временной блокировки экрана (настройка осуществляется средствами ОС Windows).

Организация и поддержка работы пользователей включает в себя выдачу пользователям аппаратных идентификаторов, настройку режимов аутентификации, обеспечение доступа пользователей к ресурсам компьютеров.

В СЗИ «Блокхост-Сеть 3» 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.

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 3», описанное в пункте 4.1.2 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 входа в ОС в безопасном режиме

Необходимо обратить внимание на то, что войти в ОС в безопасном режиме на рабочую станцию с установленным СЗИ «Блокхост-Сеть 3» можно только под встроенной учетной записью администратора ОС Windows (домена).

4.1.1 Особенности работы с цифровыми сертификатами пользователей

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

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.

4.1.2 Виды аутентификации при входе в систему

При загрузке системы предусмотрены следующие виды входа в систему (в данном разделе приведен пример аутентификации в ОС Windows 7/Server 2008R2 рис. 4.1):

- вход с предъявлением электронного идентификатора ruToken, eToken, SafeNet eToken; JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, Avest Token, ESMART Token;
- вход с предъявлением отчуждаемого носителя (USB-накопитель/дискета);

- вход по сертификату;
- вход использованием персонального идентификатора пользователя, хранящегося в реестре Windows (значок появляется при условии, что одному или более пользователей в СЗИ присвоен носитель данного вида);
- вход пользователя без предъявления электронного идентификатора.

Рисунок 4.1 – Аутентификация в ОС Windows Server 2008R2

4.1.2.1 Аутентификация с предъявлением электронного идентификатора/отчуждаемого носителя/персонального идентификатора пользователя, хранящегося в реестре Windows

Для аутентификации в системе с предъявлением электронного идентификатора, отчуждаемого носителя или персонального идентификатора пользователя в реестре Windows, необходимо подключить электронный идентификатор/отчуждаемый носитель/персональный идентификатор пользователя в реестре Windows, затем нажать кнопку с необходимым типом носителя и заполнить следующие поля (рис. 4.2):

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

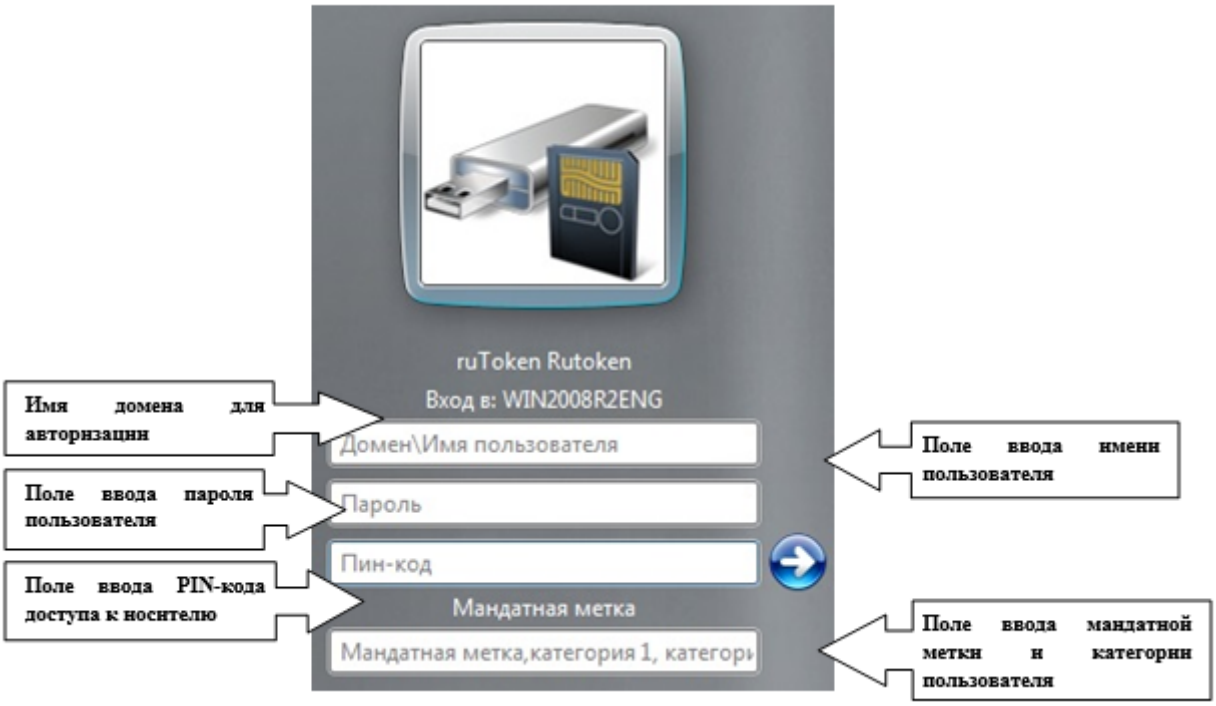


Рисунок 4.2 – Аутентификация в ОС Windows Server 2008R2 с предъявлением ruToken

4.1.2.2 Аутентификация по сертификату пользователя

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

Для аутентификации по сертификату необходимо подключить персональный электронный идентификатор (eToken/SafeNet eToken/JaCarta/ESMART Token/Avest Token/ruToken), содержащий сертификат пользователя и нажать кнопку ***Вход со смарт-картой <Имя пользователя>*** (рис. 4.1). В появившемся окне (рис. 4.3) нужно в соответствующие поля ввести PIN-код подключенного носителя и перечисленные через запятую и без пробелов значение мандатной метки и наименования категорий, присвоенных пользователю (независимо от значения мандатной метки пользователя в СЗИ, **первый вход в ОС** он должен выполнить, указав значение метки, **равное 1**, **без ввода имен категорий**, это необходимо для корректного создания профиля пользователя операционной системой). Остальные данные пользователя будут автоматически считаны с носителя.

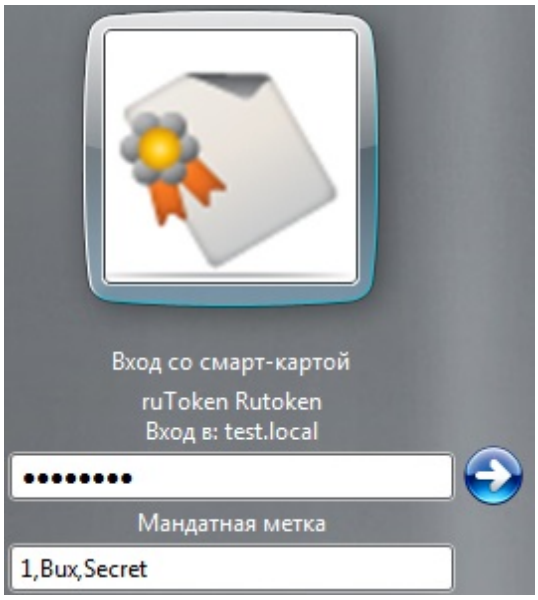


Рисунок 4.3 – Вход ОС Windows Server 2008R2 по сертификату

4.1.2.3 Вход без токена

В СЗИ «Блокхост-Сеть 3» существует возможность входа пользователей в ОС по паролю без предъявления ключевого носителя. Такая возможность по умолчанию есть у встроенного в ОС администратора. Администратор безопасности может предоставить возможность входа в ОС без предъявления персонального идентификатора и другим пользователям (подробнее о настройке параметров пользователей в СЗИ см. раздел 5.3 настоящего документа).

Для входа пользователя в ОС без предъявления ключевого носителя необходимо нажать кнопку ***Вход пользователя*** (см. рис. 4.1) и заполнить поля, показанные на рисунке 4.4:

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

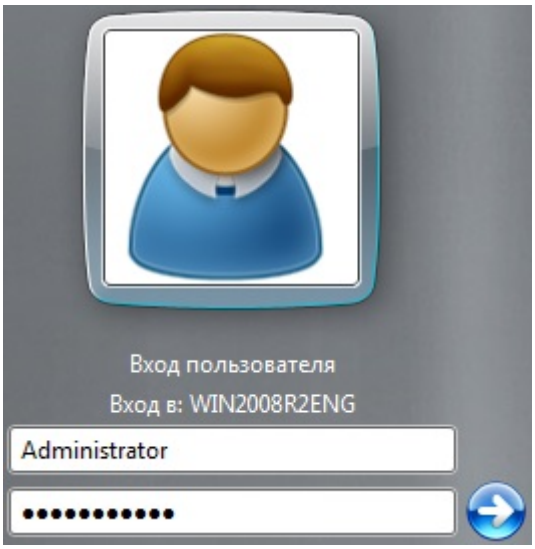


Рисунок 4.4 – Вход пользователя в ОС Windows Server 2008R2 без предъявления ключевого носителя

4.2 Виды входа в ОС

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

В СЗИ «Блокхост-Сеть 3» поддерживаются два варианта ввода идентификационных данных пользователя при входе в систему:

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

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

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

Подробнее работа функции ***Автовход*** рассмотрена в п.4.2.3 настоящего руководства.

4.2.1 Стандартная аутентификация

После появления приглашения на вход в систему (см. рис. 4.1) необходимо выбрать тип идентификатора входа в ОС, в открывшемся окне ввести идентификационные данные пользователя, PIN-код доступа к аппаратному идентификатору и значение мандатной метки, с которой пользователь выполнит вход в систему.

Если пользователь осуществляет вход в ОС Windows 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 поле ***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 3», при использовании режима двухфакторной аутентификации пользователя, существует возможность сохранения пароля пользователя на персональном идентификаторе (ключевом носителе). Такая возможность может использоваться для того, чтобы у пользователя не было необходимости запоминать пароль и вводить его при каждом входе в систему. Порядок смены пароля описан в разделе 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 пункте 4.1.2 настоящего руководства) пользователю необходимо:

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

Реакция СЗИ на такие действия зависит от информации о пароле, содержащейся в

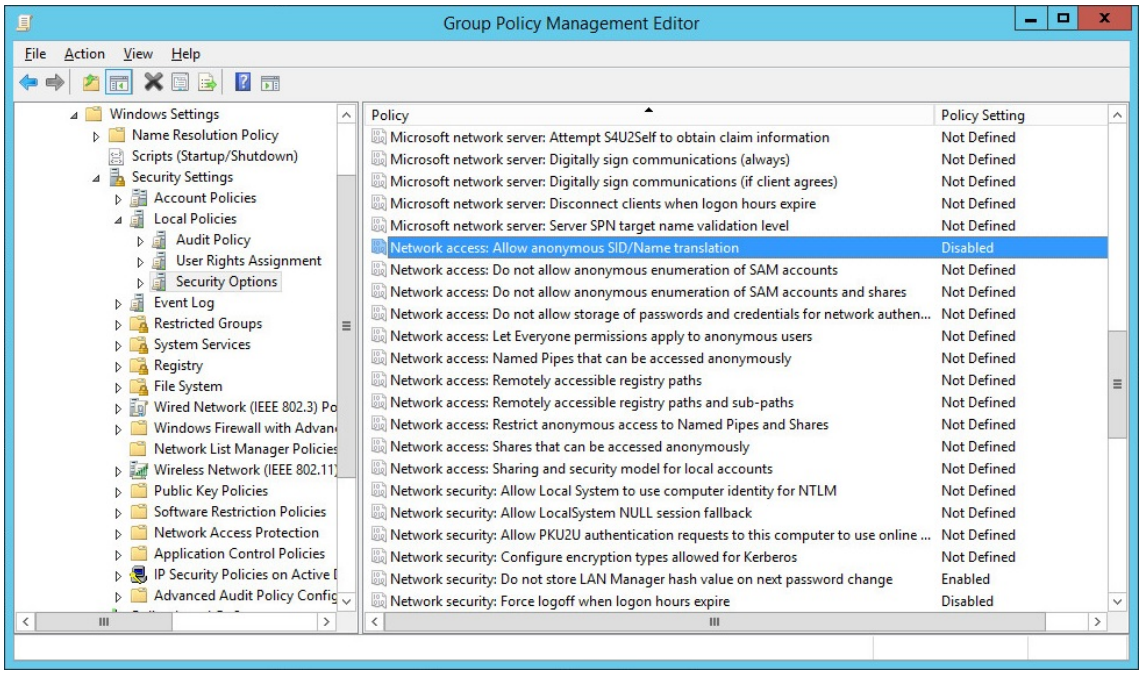
персональном идентификаторе. Возможны следующие варианты:

- 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).

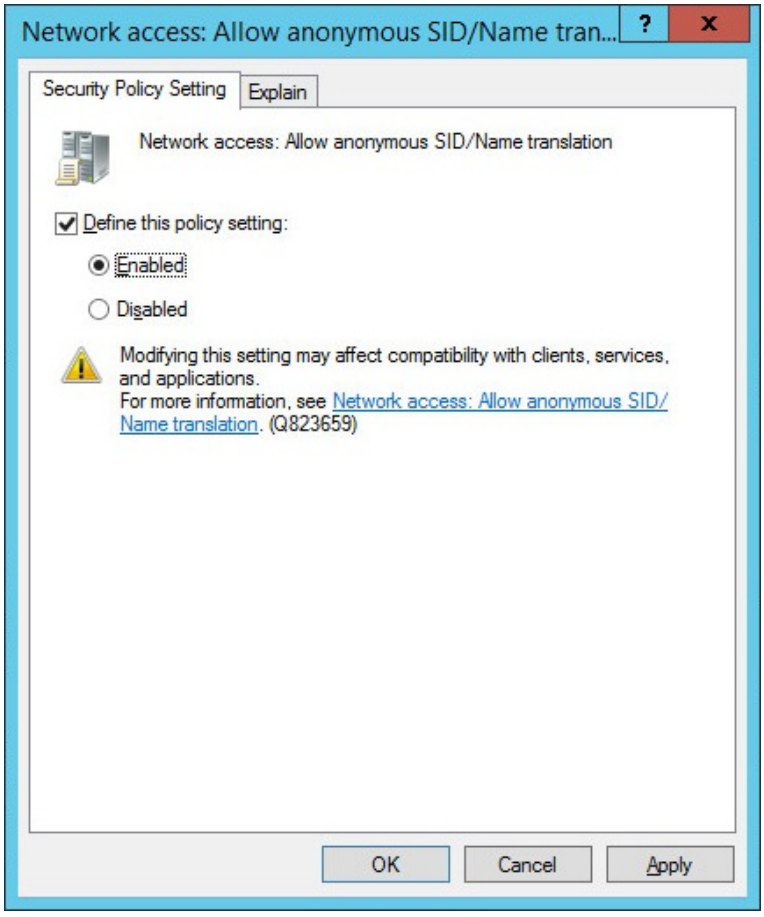
Если в персональном идентификаторе содержится актуальный пароль, то после успешной проверки прав пользователя на вход в систему продолжится загрузка операционной системы. В процессе загрузки на экран будут выводиться сообщения о выполняемых механизмами ОС действиях.

Если идентификатор содержит другой пароль, или пароль на идентификаторе отсутствует, на экране появится сообщение о неверном пароле. После ознакомления с сообщением (нажатие кнопки ***ОК***) произойдет возврат в диалог ввода идентификационной информации пользователя (см. примеры на рисунках в пункте 4.1.2 настоящего руководства), в котором необходимо выбрать домен, ввести имя пользователя и его актуальный пароль, PIN-код доступа к персональному идентификатору и мандатную метку. В случае трехкратного ввода неправильного пароля, операционная система перезагрузится.

Для корректной работы механизма входа на контролируемую рабочую станцию по персональному идентификатору, с сохраненным на нём паролем, на контроллере домена должен быть включен параметр групповой политики безопасности домена ***Доступ к сети: Разрешить трансляцию анонимного SID в имя*** (***Network Access: Allow anonymous SID/Name translation***): в окне редактирования параметров безопасности групповой политики домена по умолчанию (рис. 4.5, а) выбрать пункт ***Параметры безопасности →Локальные политики →Параметры безопасности*** (на рисунках приведены настройки параметров в англоязычной ОС) 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. 4.5, б) отметить параметры ***Определить указанный ниже параметр политики*** и ***Включить***.



а)



б)

Рисунок 4.5 – 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 3», при использовании режима двухфакторной аутентификации пользователя, доступна функция ***Автовход***. Она позволяет организовать вход пользователя в систему без отображения окна аутентификации СЗИ «Блокхост-Сеть 3».

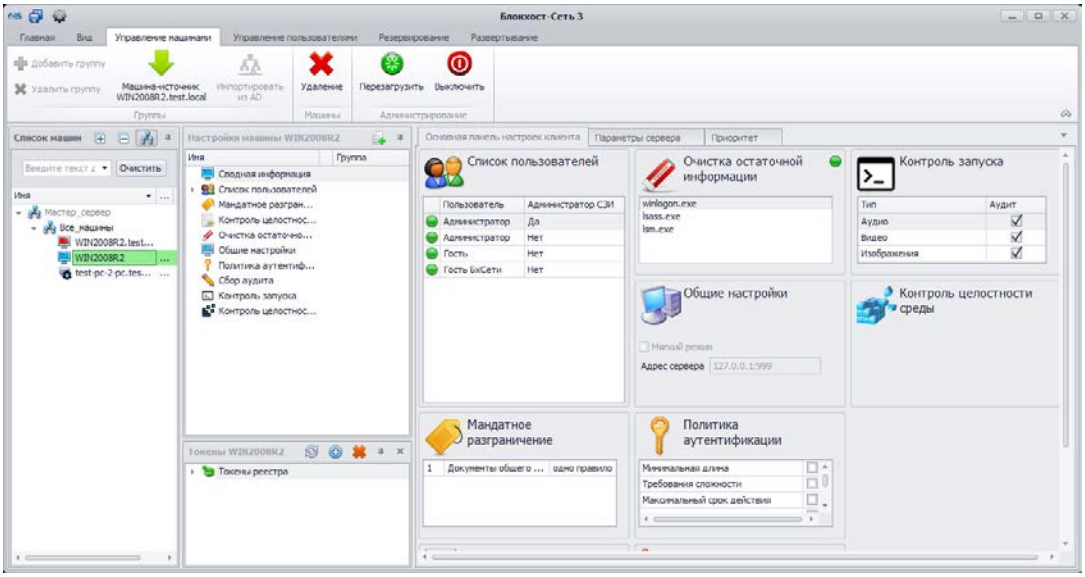
После включения данной опции, при загрузке ОС происходит автоматический вход в систему под учетной записью указанного пользователя, при этом интерактивная работа пользователя блокируется с целью обеспечения защиты информации от несанкционированного использования (окно блокировки интерактивной сессии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

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

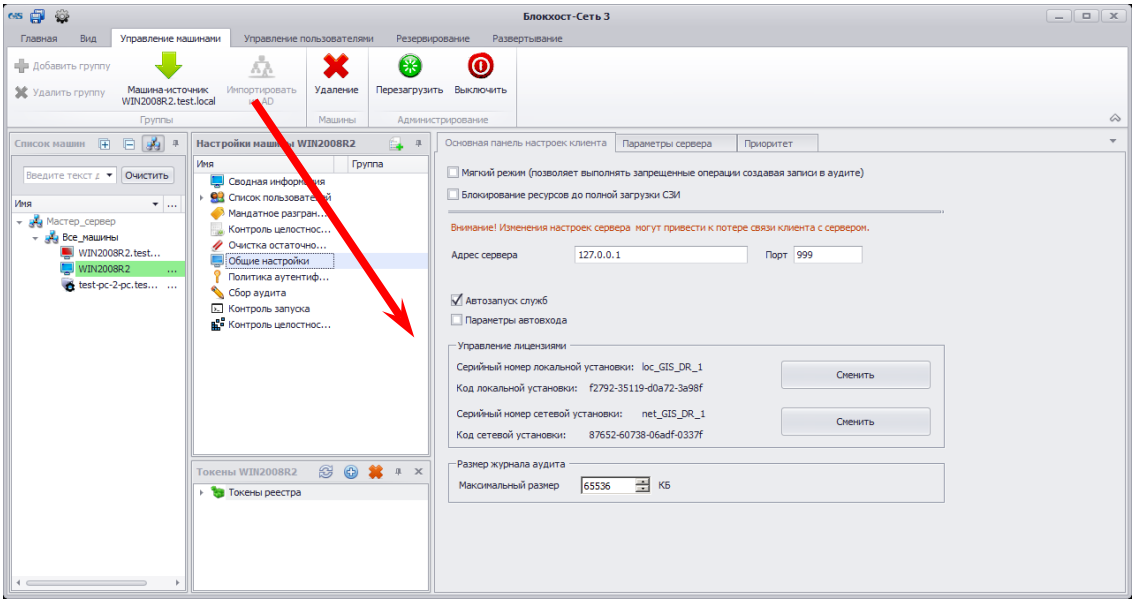
1) Сохранить пароль пользователя, от имени которого будет осуществляться автоматический вход в ОС, на его персональный идентификатор (подробнее о способах сохранения пароля пользователя на персональный идентификатор см. раздел 4.4 и пункт 5.2.2 настоящего руководства).

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. 4.6, а). В обоих случаях в **Основной панели настроек клиентов** отобразятся настраиваемые параметры контролируемой рабочей станции (рис. 4.6, б).



а)



б)

Рисунок 4.6 – Отображение настраиваемых параметров рабочей станции

4) В **Основной панели настроек клиентов** отметить параметр ***Параметры автовхода***.

5) В появившейся области ввода параметров автовхода (рис. 4.7):

- 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.

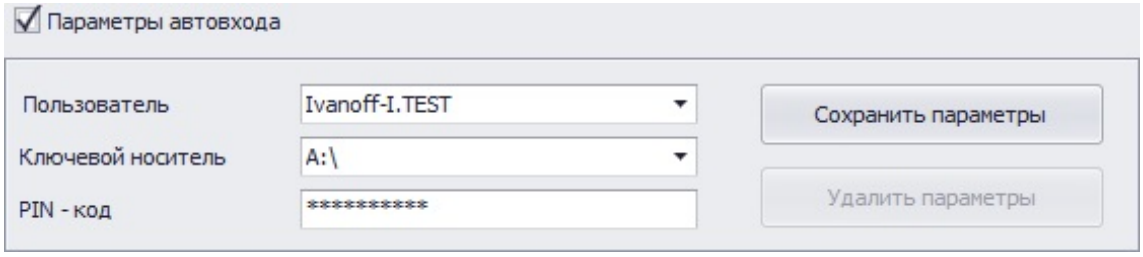


Рисунок 4.7 – Область ввода параметров автовхода

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

6) Для сохранения произведенных настроек нажать кнопку ***Сохранить параметры***, расположенную в области ***Параметры автовхода*** (см. рис. 4.7). Появится сообщение об успешном сохранении настроек (рис. 4.8). 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 3».

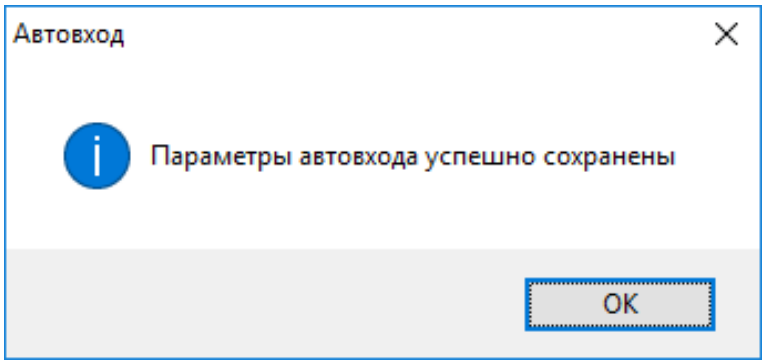


Рисунок 4.8 – Информационное сообщение о сохранении параметров

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 п *Параметры автовхода* нажать кнопку ***Удалить параметры*** (см. рис. 4.7). При этом в реестр редактируемой рабочей станции будут внесены соответствующие изменения, и появится сообщение об удалении параметров автовхода:

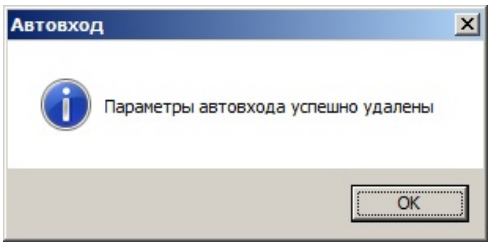


Рисунок 4.9 – Информационное сообщение об удалении параметров автовхода

4.2.4 Аутентификация в мягком режиме

В СЗИ «Блокхост-Сеть 3» доступна аутентификация пользователя только средствами ОС Windows – при этом идентификационные данные пользователя проверяются только средствами операционной системы, а СЗИ только осуществляет проверку в своей базе наличия учетной записи пользователя, выполняющего вход в ОС.

Данный режим аутентификации используется при ***Мягком режиме работы*** СЗИ. В данном режиме средство защиты не обеспечивает выполнение заявленных функций безопасности.

4.2.5 Запуск приложений от имени неавторизованного в ОС пользователя

В СЗИ «Блокхост-Сеть 3» реализован механизм аутентификации пользователя от имени, которого происходит запуск приложений. Для того чтобы запустить приложение от имени пользователя, отличающегося от пользователя, вошедшего в систему, необходимо в окне авторизации ввести имя пользователя и пароль.

При аутентификации пользователя, от имени которого производится запуск приложения, пользователю автоматически назначается уровень доступа (мандатная метка и категории), равный уровню доступа сессии авторизованного в ОС текущего пользователя. В случае несовпадения максимального уровня доступа пользователя и уровня доступа пользователя текущей сессии – уровень доступа текущей сессии превышает максимальный уровень доступа пользователя – попытка запуска любого приложения от имени такого пользователя будет запрещена, а в журнал аудита СЗИ будет внесена запись о неудачной аутентификации.

Подсистема аутентификации СЗИ «Блокхост-Сеть 3» осуществит проверку идентификационных данных пользователя, наличие разрешения/запрета на доступ к запускаемому процессу. В случае положительного результата проверки приложение будет запущено. В случае отрицательного – в окне авторизации появится сообщение об ошибке запуска приложения.

4.3 Операция смены пароля пользователя

Выполнить операцию смены пароля пользователя можно следующими способами:

- самостоятельно пользователем – через диалоговое окно СЗИ «Блокхост-Сеть 3» (рисунок 4.10);
- администратором безопасности – из консоли администрирования СЗИ «Блокхост-Сеть 3» (п. 5.2.1 «Изменение общих параметров учетной записи пользователя»).

4.3.1 Смена пароля через диалоговое окно «Блокхост-Сеть 3»

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

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

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

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

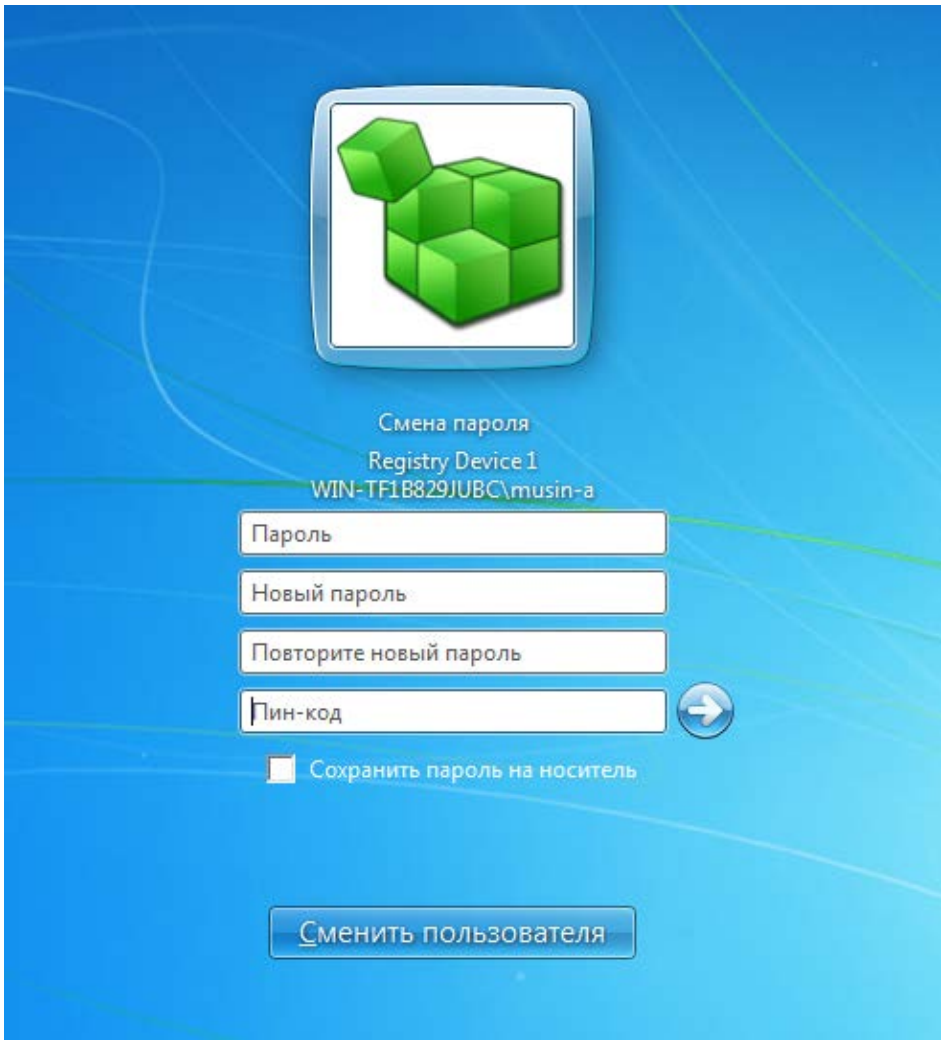


Рисунок 4.10 – Диалоговое окно смены пароля в ОС Windows Server 2008R2

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

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

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

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

4.3.2 Смена пароля через консоль администрирования СЗИ Блокхост-Сеть 3»

В СЗИ «Блокхост-Сеть 3» существует возможность смены пароля пользователя, зарегистрированного в СЗИ на контролируемой рабочей станции, из консоли администрирования СЗИ. Подробно процесс смены пароля пользователя, зарегистрированного в СЗИ на контролируемой рабочей станции, рассмотрен в п. 5.2.1 «Изменение общих параметров учетной записи пользователя» настоящего руководства.

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

Если пароль пользователя был изменен вне СЗИ «Блокхост-Сеть 3» (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.

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

- нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**;
- в отобразившемся меню нажать кнопку-ссылку ***Сменить пароль (Change a password);***
- в открывшемся диалоге смены пароля (см. примеры на рис. 4.10) 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 3» не следует использовать символы русского алфавита.

Операция смены PIN-кода персонального идентификатора пользователя может быть произведена следующими способами:

- самостоятельно пользователем – через диалоговое окно СЗИ «Блокхост-Сеть 3» (в случае несоответствия PIN-кода требованиям установленной политики безопасности или в случае установки АБ требования смены PIN-кода в консоли администрирования, рисунок 4.11);
- администратором безопасности – из консоли администрирования СЗИ «Блокхост-Сеть 3» (пункт 6.2.5. «Механизм идентификаторов входа» настоящего документа).

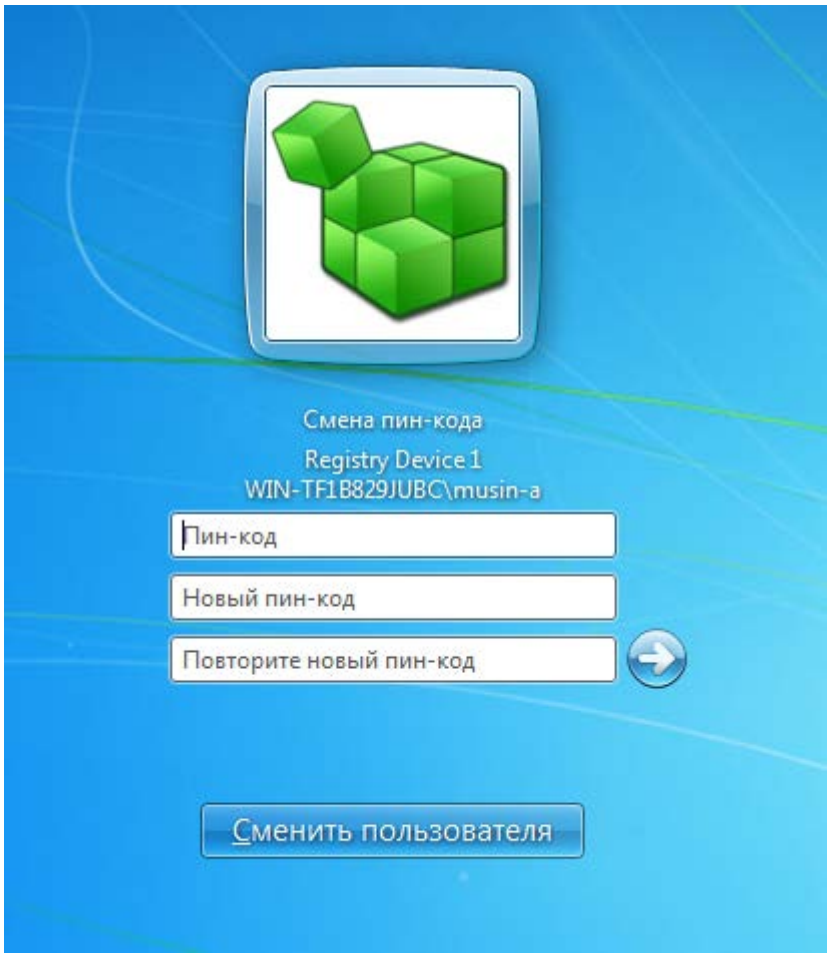


Рисунок 4.11 – Диалоговое окно смены PIN-кода в ОС Windows Server 2008R2

В случае изменения PIN-кода электронного идентификатора (через консоль администрирования СЗИ) 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

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

1) Нажмите комбинацию клавиш **<Ctrl>+<Alt>+<Del>.**

2) Нажмите кнопку ***Блокировать компьютер/Lock this computer***.

3) Клавиатура и экран монитора будут заблокированы.

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

Разблокировать компьютер может только работающий на нем пользователь.

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

В результате откроется диалог ввода данных работающего за компьютером пользователя (пример показан на рисунке 4.12). 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.

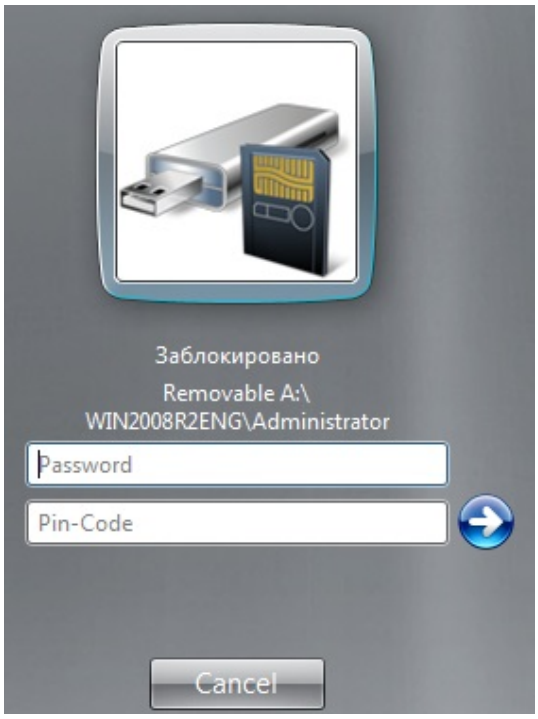


Рисунок 4.12 – Ввод данных пользователя для разблокировки в ОС Windows Server 2008R2

При нажатии на кнопку ***Отмена*** (***Cancel***) в диалоге разблокировки системы (см. рис. 4.12) будет произведен возврат состояния компьютера в режим блокировки.

4.6.2 Автоматическая блокировка компьютера при отключении ключевого носителя

Для рабочих станций-клиентов СЗИ «Блокхост-Сеть 3», **включенных в домен**, можно настроить автоматическую блокировку ОС в момент изъятия (отключения) из

компьютера ключевого носителя пользователя. Для этого необходимо воспользоваться механизмом настройки групповых политик домена:

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

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

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

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

Для разблокировки пользователю необходимо вставить свой ключевой носитель в компьютер и произвести действия по авторизации, описанные в пункте 4.6.1 настоящего руководства.

Если для пользователя установлен режим аутентификации ***Стандартная аутентификация ОС Windows*** (подробнее см. п. 5.2.1.5 «Изменение способа аутентификации пользователя» настоящего руководства), или СЗИ работает в ***Мягком режиме*** (подробнее см. п. 6.2.5 «Механизм мягкого режима» настоящего руководства), и пользователь осуществлял вход в ОС с использованием аппаратного идентификатора, то для разблокировки рабочей станции все равно необходимо вставить в компьютер ключевой носитель, который использовался при входе пользователя в систему.

4.6.3 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 пункте 4.1.2 настоящего руководства.

5 Пользователи в СЗИ «Блокхост-Сеть 3»

Для формирования политик безопасности администратору безопасности необходимо определить список субъектов доступа – список учетных записей пользователей и групп пользователей, к которым будут применяться настройки механизмов разграничения доступа и защиты информации.

В СЗИ «Блокхост-Сеть 3» существует возможность добавления в список пользователей СЗИ рабочей станции учетных записей локального пользователя рабочей станции, доменного пользователя, группы пользователей из Active Directory, встроенной группы «Все пользователи БхСети».

5.1 Добавление пользователей в СЗИ «Блокхост-Сеть 3»

5.1.1 Общий порядок добавления пользователей в СЗИ «Блокхост-Сеть 3»

Для добавления учетной записи пользователя (группы пользователей) в СЗИ «Блокхост-Сеть 3» на контролируемую рабочую станцию (группу рабочих станций) администратору безопасности необходимо осуществить следующие действия в консоли администрирования СЗИ:

1) В окне **«Список машин»** выбрать рабочую станцию (группу), на которую необходимо добавить учетную запись пользователя (группы пользователей), 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:

- области выбора источника учетной записи;
- области выбора учетной записи пользователей (включая встроенную группу «Все пользователи БхСети») с полем ввода критериев поиска учетных записей;
- области добавляемых в СЗИ пользователей.

Из окна добавления пользователей можно добавить в СЗИ учетную запись существующего локального пользователя контролируемой рабочей станции, создать нового локального пользователя на контролируемой рабочей станции, добавить учетную запись пользователя (группы пользователей) домена или встроенную группу «Все пользователи БхСети».

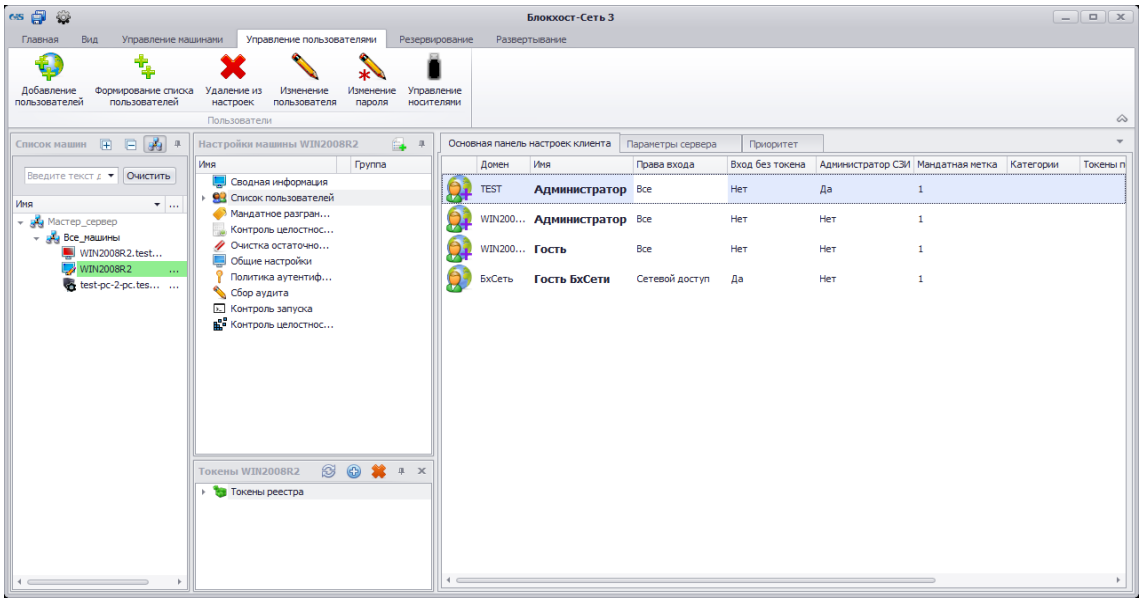


Рисунок 5.1 – Список пользователей в СЗИ рабочей станции

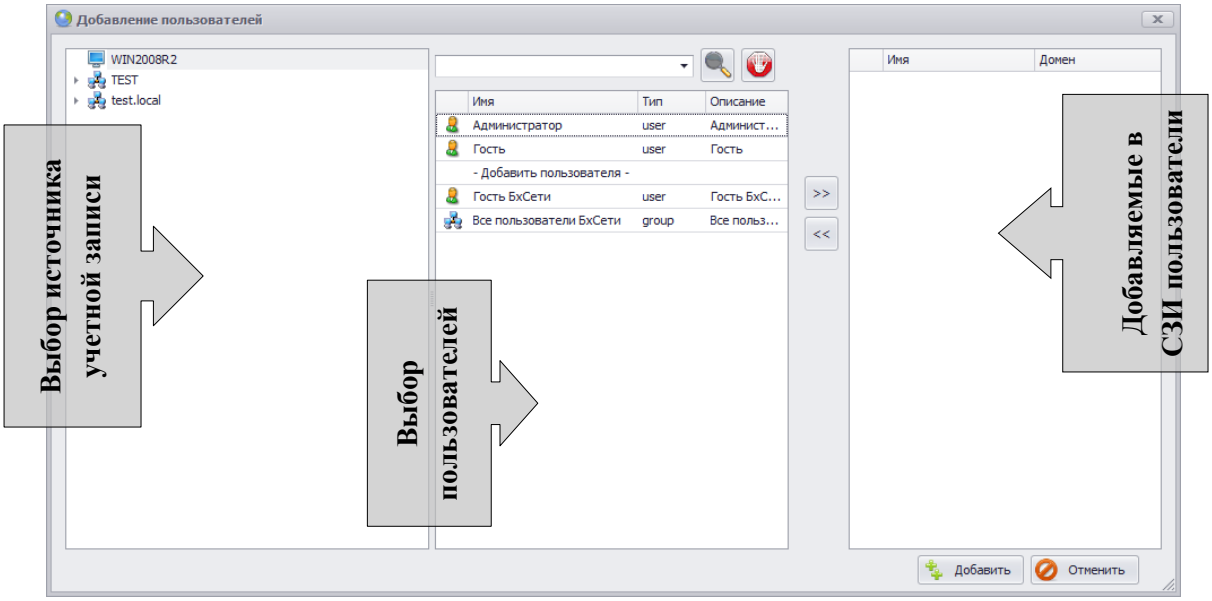


Рисунок 5.2 – Окно добавления пользователей в СЗИ

4) В окне «**Добавление пользователей»** необходимо:

- выбрать источник учетной записи: рабочая станция или домен;
- выделить необходимую учетную запись (с помощью клавиш <**Ctrl**> или <**Shift**> можно выделить сразу несколько учетных записей);
- с помощью кнопки [>>] перенести выбранную учетную запись в поле добавляемых пользователей;
- нажать кнопку ***Добавить***.

Окно **«Добавление пользователей»** закроется, а добавленные учетные записи появятся в списке пользователей СЗИ рабочей станции. Добавленным в СЗИ учетным

записям автоматически устанавливается режим аутентификации только средствами ОС Windows (отмечен параметр ***Доверять аутентификации Windows***), назначается мандатная метка равная **1**, все типы входа на рабочую станцию. В дальнейшем учетной записи пользователя можно присвоить аппаратный идентификатор и изменить остальные параметры, установленные по умолчанию (подробнее см. п. «5.2 Редактирование параметров учетных записей в СЗИ» настоящего руководства).

Нельзя изменить мандатную метку и назначить мандатные категории учетной записи группы пользователей, а также присвоить ей аппаратный идентификатор.

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

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 и без указания категорий.** Это необходимо для корректного создания профиля пользователя операционной системой.

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

Все пользователи СЗИ «Блокхост-Сеть 3», включены в группу **Все пользователи БхСети**. Настройки данной группы приоритетны для всех пользователей. По умолчанию для группы **Все пользователи БхСети** заданы стандартные параметры безопасности.

5.1.2 Особенности добавления в СЗИ доменных учетных записей

При добавлении в список пользователей СЗИ учетных записей групп пользователей необходимо учитывать особенности работы в ОС Windows учетных записей групп пользователей, имеющих общие идентификаторы безопасности (SID).

При добавлении в СЗИ «Блокхост-Сеть 3» учетной записи пользователя (группы пользователей) домена необходимо:

1) В окне «**Добавление пользователя**» (см. рис. 5.2) выбрать домен в качестве источника учетной записи.

2) В открывшемся окне доменной идентификации ввести учетные данные пользователя домена (в частности – администратора домена), при необходимости

отметить параметр ***Запомнить учетные данные*** и нажать кнопку ***Подключить*** (рис. 5.3).

Параметр ***Запомнить учетные данные*** служит для кэширования в памяти консоли администрирования СЗИ введенных для авторизации в домене данных учетной записи только на время работы консоли – при следующем запуске консоли администрирования СЗИ для авторизации в домене вновь потребуется ввод учетных данных пользователя домена.

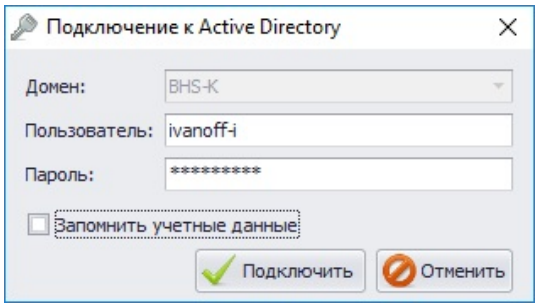


Рисунок 5.3 – Окно доменной идентификации пользователя

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:

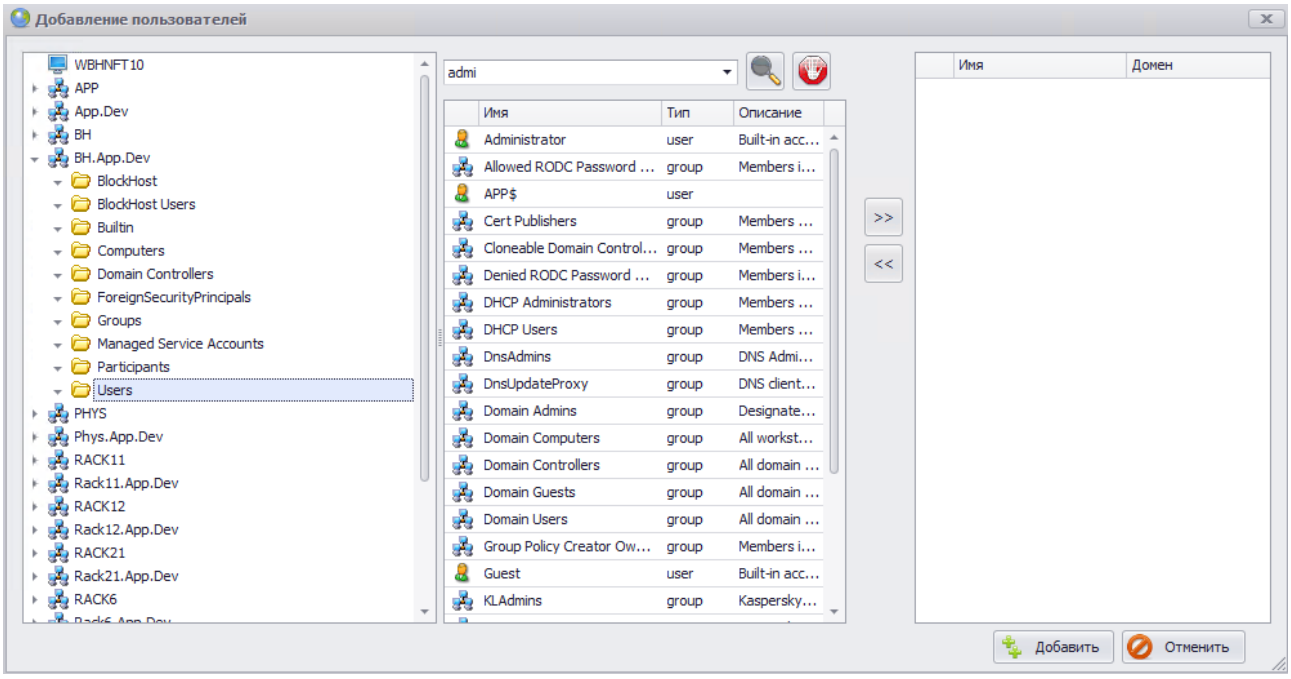


Рисунок 5.4 – Добавление доменного пользователя

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***).

В верхней части области выбора учетных записей пользователей доступен поиск по заданному критерию (рисунок 5.4). Для осуществления поиска необходимо ввести в поле требуемое значение и нажать кнопку «  ». По кнопке «  » поиск по введенному значению прекратится.

4) Выделить учетную запись добавляемого пользователя (группы пользователей) и с помощью кнопки  перенести выбранную учетную запись в поле добавляемых пользователей.

5) Нажать кнопку ***Добавить***. Окно «**Добавление пользователей**» закроется, а добавленная учетная запись появится в списке пользователей. Добавленной учетной записи автоматически устанавливается режим аутентификации только средствами ОС Windows (отмечен параметр ***Доверять аутентификации Windows***), назначается мандатная метка равная **1**, все типы входа на рабочую станцию. В дальнейшем учетной записи пользователя можно присвоить аппаратный идентификатор и изменить остальные параметры учетной записи пользователя, установленные в СЗИ по умолчанию (подробнее см. п. «5.2 Редактирование параметров учетных записей в СЗИ» настоящего руководства).

Нельзя изменить мандатную метку и назначить мандатные категории учетной записи группы пользователей, а также присвоить ей аппаратный идентификатор.

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

При работе СЗИ на рабочей станции в сети, в которой имеется несколько доменов, с установленными доверенными отношениями, следует учитывать особенности работы с учетными записями пользователей с общими SID или входящими в группы, имеющие общие идентификаторы безопасности. Например, добавленной в список пользователей СЗИ рабочей станции группе ***Пользователи домена (Domain Users)*** одного домена, с установленными для нее настройками механизмов СЗИ, точно такие же настройки механизмов СЗИ получат и все пользователи, входящие в группу ***Пользователи домена (Domain Users)*** доменов, между которыми в локальной сети установлены доверенные отношения. То есть доступ к ресурсам рабочей станции получат все пользователи, входящие в группу ***Пользователи домена (Domain Users)*** всех доменов.

5.1.3 Добавление в СЗИ нескольких учетных записей

Для добавления в СЗИ нескольких учетных записей пользователей (групп пользователей) необходимо:

1) В окне **«Добавление пользователей»** (см. рис. 5.4) сформировать (с помощью кнопок >> и <<) список добавляемых учетных записей (для выделения сразу нескольких учетных записей можно воспользоваться клавишами **<Ctrl>** или **<Shift>**).

2) Нажать кнопку ***Добавить***. В результате все выбранные учетные записи отобразятся в списке пользователей контролируемой рабочей станции во вкладке **Основная панель настроек клиентов**. Всем добавленным таким образом учетным записям автоматически устанавливается режим аутентификации только средствами ОС Windows (отмечен параметр ***Доверять аутентификации Windows***), назначается мандатная метка равная **1**, все типы входа на рабочую станцию. В дальнейшем каждой учетной записи пользователя можно присвоить аппаратный идентификатор и изменить остальные параметры учетной записи пользователя, установленные в СЗИ по умолчанию (подробнее см. п. 5.2 «5.2Редактирование параметров учетных записей в СЗИ» настоящего руководства).

Нельзя изменить мандатную метку и назначить мандатные категории учетной записи группы пользователей, а также присвоить ей аппаратный идентификатор.

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

Для возможности удаленного (сетевого) доступа пользователей к ресурсам контролируемой рабочей станции (клиента СЗИ), а также для запуска служб СЗИ, запускаемых от имени учётной записи пользователя, на рабочей станции (клиенте СЗИ), 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***.

5.1.4 Создание нового локального пользователя

В локальной и серверной консолях администрирования СЗИ «Блокхост-Сеть 3» существует возможность создания учетной записи локального пользователя на контролируемой рабочей станции.

Возможность создания на контролируемой рабочей станции учетной записи локального пользователя из серверной консоли администрирования СЗИ появляется только после запуска на ней служб СЗИ «Блокхост-Сеть 3».

Для создания нового локального пользователя и последующего добавления его в список пользователей СЗИ редактируемой рабочей станции администратору безопасности необходимо в консоли администрирования:

1) В окне **«Добавление пользователей»** (см. рис. 5.2) выделить рабочую станцию в качестве источника списка учетных записей.

2) В поле выбора пользователей дважды щелкнуть левой кнопкой мыши на пункте ***-Добавить пользователя-***.

3) В открывшемся окне **«Создание локального пользователя»** (рис. 5.5):

- 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;

При добавлении пользователя в СЗИ и при смене его пароля администратором через консоль администрирования СЗИ запрещено использовать символы звездочка «*» и номер «№» в пароле. При изменении пароля пользователем стандартными средствами Windows использование символов звездочка «*» и номер «№» не запрещается.

- установить параметр ***Требовать смену пароля при следующем входе в систему*** для принудительной смены введенного администратором пароля нового пользователя;
- нажать кнопку ***Создать***.

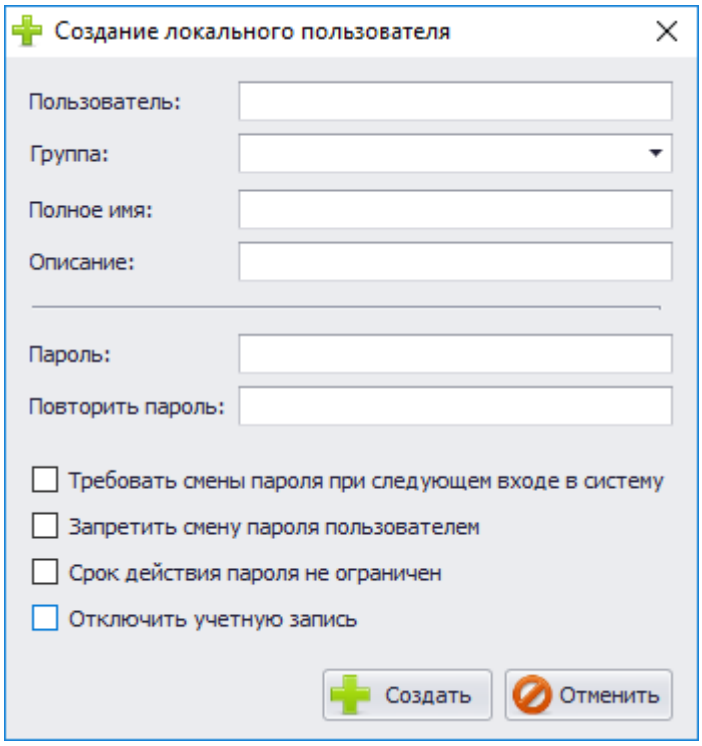


Рисунок 5.5 – Окно «Создание локального пользователя»

Окно **«Создание локального пользователя»** консоли администрирования СЗИ повторяет окно **«Новый пользователь»** консоли **mmc** операционной системы Windows. Действия администратора по созданию нового пользователя в консоли администрирования СЗИ «Блокхост-Сеть 3» повторяют аналогичные действия администратора ОС Windows.

4) В окне добавления пользователей (см. рис. 5.2) выделить созданную учетную запись и с помощью кнопки >> перенести ее в поле добавляемых в СЗИ пользователей.

5) Нажать кнопку ***Добавить***. Созданная учетная запись локального пользователя появится в списке пользователей СЗИ рабочей станции. Добавленному в СЗИ пользователю автоматически устанавливается режим аутентификации только средствами ОС Windows, назначается мандатная метка равная **1**, все типы входа на рабочую станцию. В дальнейшем пользователю можно присвоить аппаратный идентификатор и изменить остальные параметры учетной записи пользователя, установленные по умолчанию (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.

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

5.1.5 Особенности учетной записи Гость БхСети

В СЗИ «Блокхост-Сеть 3» реализована возможность работы гостевой учетной записи пользователей с ресурсами контролируемой рабочей станции. Механизм работы гостевой учетной записи пользователей заключается в следующем:

- при первоначальной установке СЗИ в список его пользователей добавляется учетная запись **Гость БхСети**;
- данной учетной записи разрешен только сетевой вход (интерактивный вход у данной учетной записи запрещен);
- по умолчанию учетной записи **Гость БхСети у**становлены полные права на доступ к локальным дискам контролируемой рабочей станции;
- настройки механизмов СЗИ, установленные для учетной записи **Гость БхСети**, присваиваются всем учетным записям, 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 учетной записи **Гость БхСети** возможны все операции по настройке механизмов СЗИ (см. подраздел «6.1 Настройка пользовательских механизмов разграничения доступа» настоящего руководства). Также в дальнейшем при необходимости можно заблокировать учетную запись **Гость БхСети** (подробнее см. п. 5.2 «5.2 Редактирование параметров учетных записей в СЗИ» настоящего руководства).

Удалить учетную запись **Гость БхСеть** из списка пользователей СЗИ рабочей станции нельзя.

При обновлении СЗИ существующая учетная запись **Гость (Guest)** конвертируется в учетную запись **Гость БхСеть.**

5.2 Редактирование параметров учетных записей в СЗИ

5.2.1 Изменение общих параметров учетных записей пользователей

Учетные записи пользователей (групп пользователей) из списка добавленных в СЗИ можно редактировать в консоли администрирования СЗИ «Блокхост-Сеть 3». В консоли администрирования СЗИ могут быть изменены следующие параметры учетной записи пользователя:

- имя пользователя (только для учетной записи пользователя);
- пароль (только для учетной записи пользователя);
- классификационный уровень доступа пользователя (группы пользователей): мандатная метка и категории;
- тип входа на рабочую станцию;
- способ аутентификации в ОС.

5.2.1.1 Изменение имени учетной записи пользователя

Изменение имени учетной записи пользователя из консоли администрирования СЗИ «Блокхост-Сеть 3» влечет за собой изменение имени этой учетной записи в СЗИ «Блокхост-Сеть 3» и в ОС Windows или в домене, в зависимости от того локальная это учетная запись или учетная запись пользователя домена.

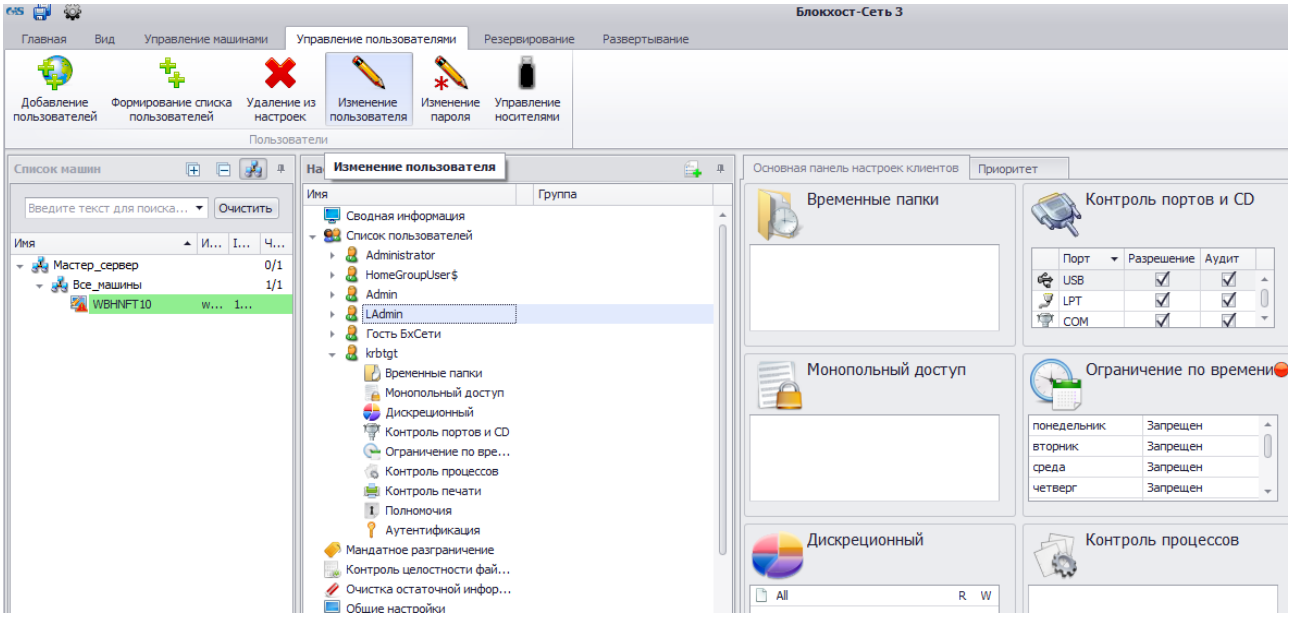


Рисунок 5.6 – Изменение учетной записи пользователя

Для изменения имени локальной учетной записи пользователя администратору безопасности следует:

1) В консоли администрирования СЗИ 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 (рисунок 5.6).

2) В окне **«Настройки машины»** выбрать пункт ***Список пользователей***.

3) В **Основной панели настроек клиентов** выделить редактируемую учетную запись пользователя и выбрать пункт меню ***Управление пользователями →Изменение пользователя***.

4) В открывшемся окне **«Изменение пользователя»** (рисунок 5.7) ввести новое имя учетной записи пользователя в соответствующее поле ввода и нажать кнопку ***Изменить***. Нажатие кнопки ***Отменить*** позволит выйти из окна без изменения параметров учетной записи пользователя.

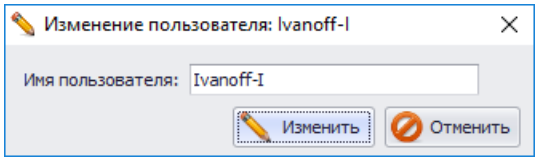


Рисунок 5.7 – Окно редактирования имени учетной записи пользователя

Для изменения имени доменной учетной записи пользователя администратору безопасности следует:

1) В окне **«Изменение пользователя»** (см. пример на рис. 5.7) ввести в поле ***Пользователь*** новое имя и нажать кнопку ***Изменить***.

2) В открывшемся окне доменной аутентификации (см. пример на 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 изменение параметров учетной записи пользователя в СЗИ выбрав пункт меню ***Главная*** → ***Сохранить все***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

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

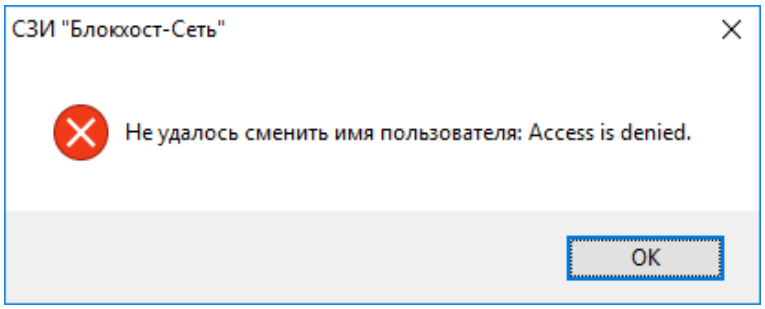


Рисунок 5.8 – Информационное сообщение об ошибке изменения имени пользователя

После нажатия на кнопку ***ОК*** откроется диалоговое окно с предложением сменить имя этого пользователя только в СЗИ «Блокхост-Сеть 3»:

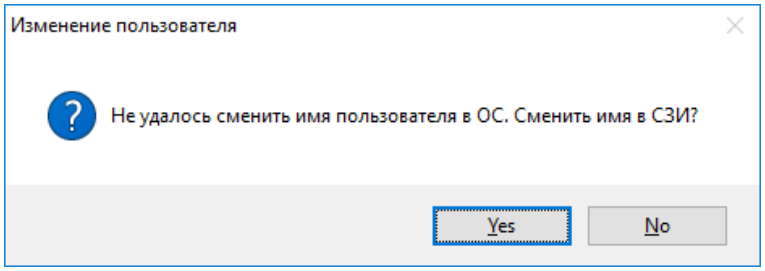


Рисунок 5.9 – Запрос на изменение имени пользователя в СЗИ

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 (см. пример на рис. 5.6) и после внесения необходимых изменений ввести в окно доменной аутентификации (см. пример на рис. 5.3) корректные данные администратора домена.

5.2.1.2 Изменение мандатной метки и назначение категорий учетной записи пользователя

Нельзя изменить мандатную метку и назначить категории учетной записи группы пользователей.

Для изменения мандатной метки учетной записи пользователя администратору безопасности необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ раскрыв пункт ***Все_машины***, выделить рабочую станцию, мандатная метка учетной записи пользователя которой будет изменяться.

2) В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать учетную запись пользователя, мандатная метка которой будет изменяться, и затем выбрать пункт ***Аутентификация*** или, выделив учетную запись пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Аутентификация***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 5.10).

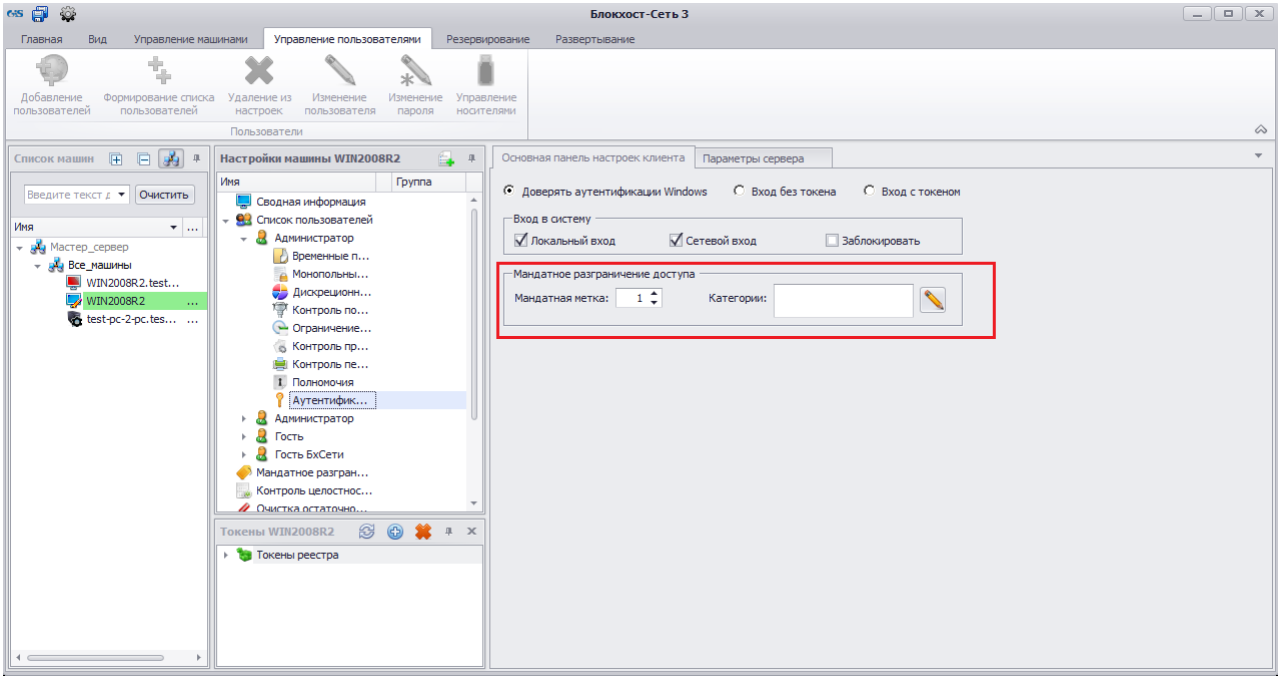


Рисунок 5.10 – Изменение мандатной метки учетной записи пользователя

3) в **Основной панели настроек клиентов** (рис. 5.10) ввести необходимое значение в поле ***Мандатная метка.***

Также изменить значение мандатной метки пользователя можно в списке пользователей **Основной панели настроек клиентов** (см. пример на рис. 5.1), для этого необходимо установить курсор в поле ***Мандатная метка*** выбранного пользователя и ввести необходимое значение.

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

Для назначения учетной записи пользователя **неиерархических категорий** необходимо:

- в **Основной панели настроек клиентов** (см. рис. 5.10) нажать кнопку ***Изменить категории***  , расположенную справа от поля ***Категории***;
- в открывшемся окне **«Список существующих категорий»** выделить необходимую категорию (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить несколько категорий) и нажать кнопку ***Применить*** (рис. 5.11).

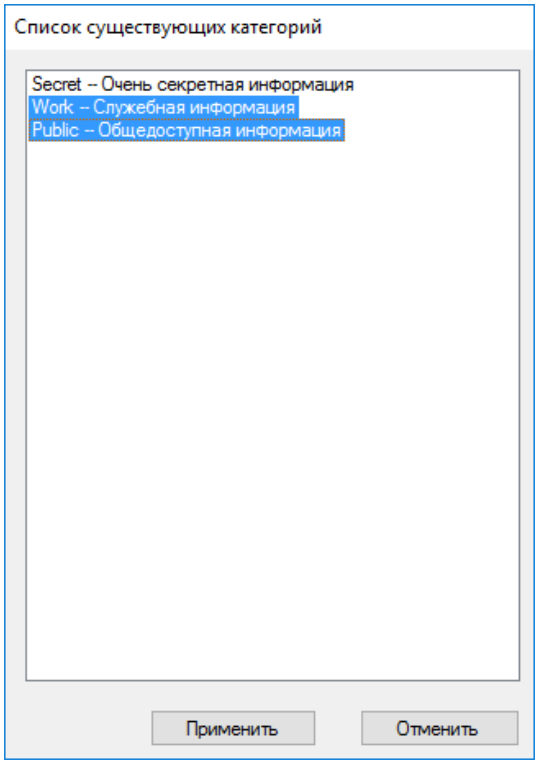


Рисунок 5.11 – Окно выбора категорий

В результате выбранные категории будут отображены в списке поля ***Категории*** в **Основной панели настроек клиентов**:

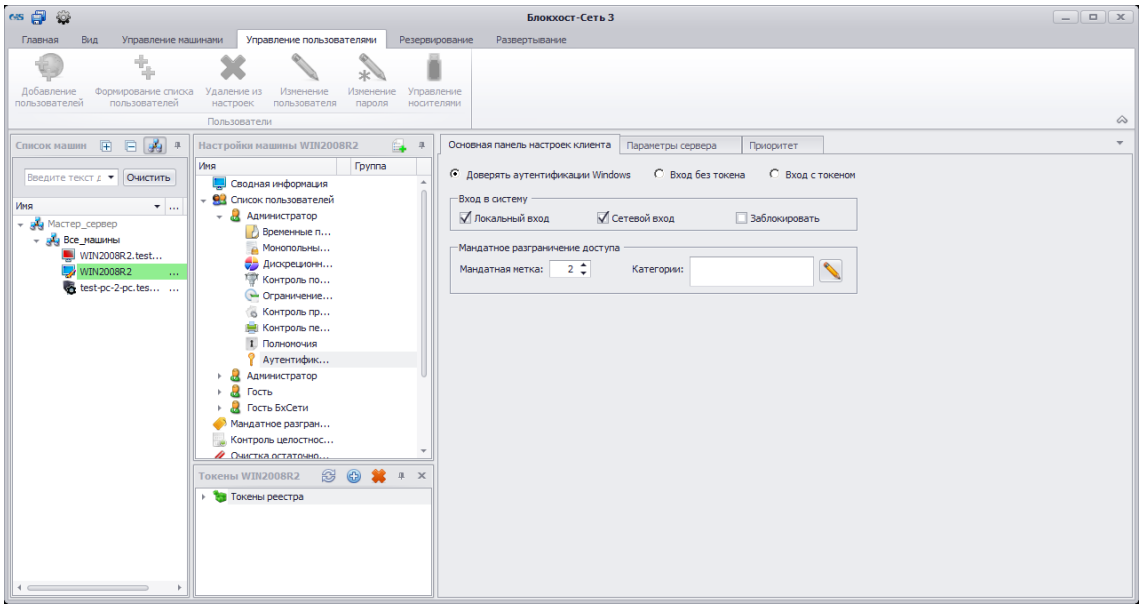


Рисунок 5.12 – Список неиерархических категорий пользователя

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

5.2.1.3 Изменение типа входа учетной записи в ОС рабочей станции

Для изменения типа входа учетной записи пользователя (группы пользователей) в ОС контролируемой рабочей станции администратору безопасности необходимо в **Основной панели настроек клиентов** (рисунок 5.13) отметить необходимый тип входа: ***Локальный вход*** и/или ***Сетевой вход*** (есть возможность предоставить пользователю оба типа входа).

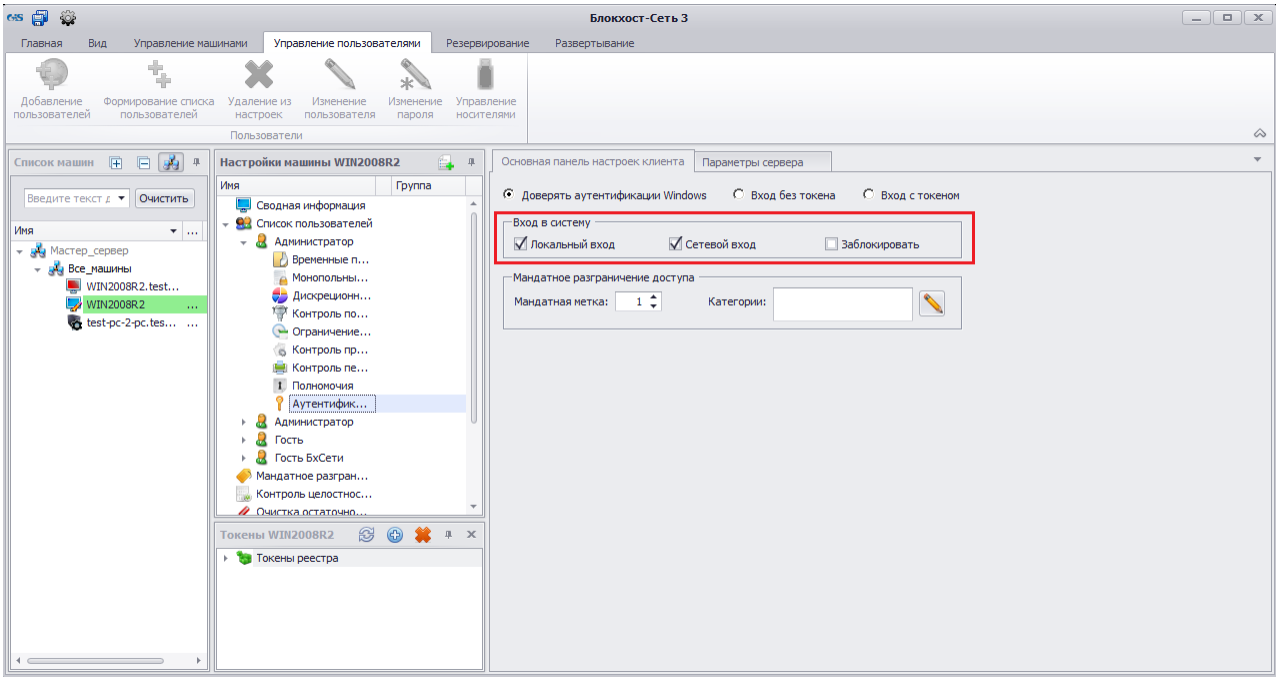


Рисунок 5.13 – Изменение типа входа учетной записи в систему

Изменить тип входа пользователя в ОС рабочей станции также можно в списке пользователей **Основной панели настроек клиентов**. Для этого необходимо щелкнуть правой кнопкой мыши на существующем значении типа входа пользователя (в столбце *Права входа*) и в открывшемся контекстном меню выбрать требуемое значение:

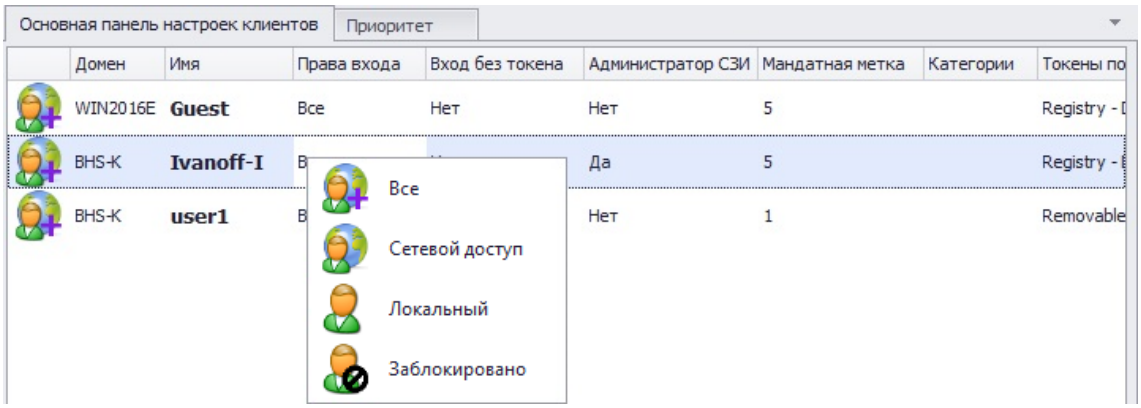


Рисунок 5.14 – Контекстное меню выбора типа входа пользователя

Для предоставления пользователю права входа в ОС контролируемой рабочей станции без использования персонального идентификатора следует отметить один из параметров: ***Доверять аутентификации Windows*** или ***Вход без токена*** (подробнее о входе пользователя в ОС без использования персонального идентификатора см. подпункт 4.1.2.8 настоящего документа).

5.2.1.4 Изменение пароля учетной записи пользователя

Изменение пароля учетной записи пользователя из консоли администрирования СЗИ

«Блокхост-Сеть 3» влечет за собой изменение пароля этой учетной записи в ОС Windows или в домене, в зависимости от того локальная это учетная запись или учетная запись пользователя домена.

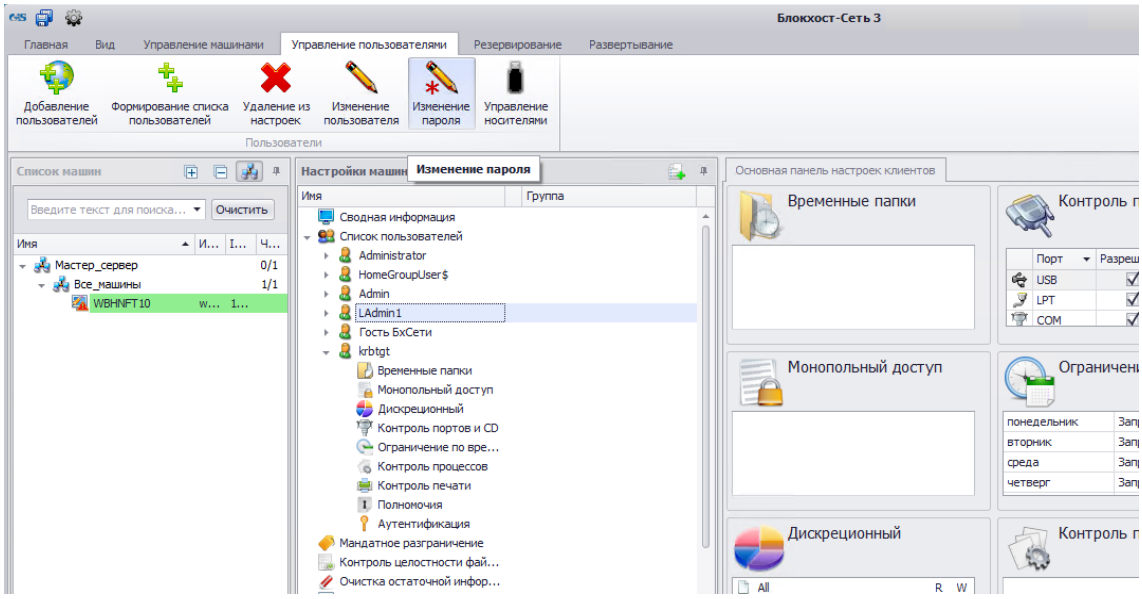


Рисунок 5.15 – Изменение пароля учетной записи пользователя

Для изменения пароля учетной записи локального пользователя ОС Windows администратору безопасности следует:

1) В консоли администрирования в окне «**Список машин**» выбрать рабочую станцию, пароль учетной записи 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*** (рисунок 5.15).

3) В **Основной панели настроек клиентов** выделить учетную запись пользователя и выбрать пункт меню ***Управление пользователями →Изменение пароля***.

4) Откроется окно **«Изменение пароля пользователя»** (рис. 5.16), в котором администратор безопасности должен ввести новый пароль пользователя и его подтверждение в соответствующие поля.

При смене пароля пользователя через консоль администрирования СЗИ запрещен ввод в окно **«Изменение пароля пользователя»** символов звездочка «*» и номер «№».

5) После ввода нового пароля учетной записи 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.

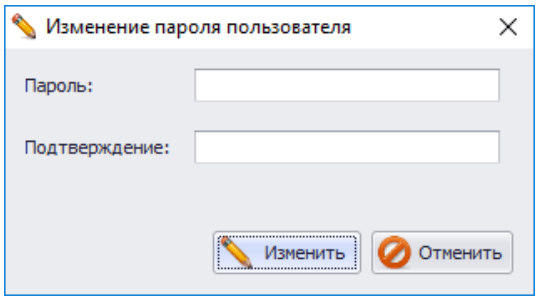


Рисунок 5.16 – Окно изменения пароля пользователя

Для изменения пароля учетной записи пользователя домена администратору безопасности следует:

1) Повторить действия по смене пароля учетной записи локального пользователя, приведенные выше в п.п. 1-5.

2) В открывшееся окно доменной аутентификации (см. пример на рис. 5.3) ввести логин и пароль учетной записи пользователя, входящего в группу администраторов домена. При успешной авторизации в домене, произойдет изменение пароля 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 изменение параметров учетной записи пользователя в СЗИ выбрав пункт меню ***Главная→ Сохранить все***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

В случае если в окно доменной аутентификации (см. пример на 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:

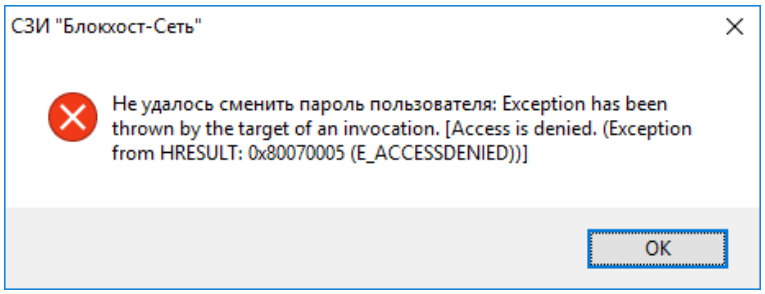


Рисунок 5.17 – Сообщение об ошибке изменения пароля пользователя домена

После закрытия окна с сообщением об ошибке изменения пароля пользователя (нажав на кнопку ***ОК*** или кнопку закрытия окна) появится диалоговое окно (рис. 5.18), с предложением изменить пароль учетной записи этого пользователя в СЗИ «Блокхост-

Сеть 3». Нажатие на кнопку ***Да/Yes*** приведет к смене пароля учетной записи пользователя в СЗИ, нажатие на кнопку ***Нет/No*** – отменит все произведенные изменения.

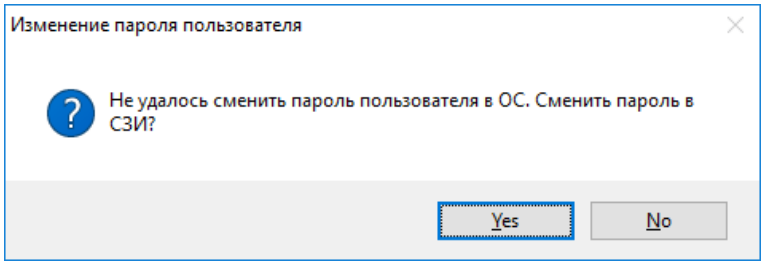


Рисунок 5.18 – Окно подтверждения изменения пароля пользователя в СЗИ

5.2.1.5 Изменение способа аутентификации пользователя в ОС

В СЗИ «Блокхост-Сеть 3» существует три варианта аутентификации пользователя:

- ***Доверять аутентификации Windows*** – аутентификация пользователя осуществляется стандартными средствами ОС Windows (используется только для настройки СЗИ и не обеспечивает выполнение заявленных функций безопасности);
- ***Вход с токеном*** (двухфакторная аутентификация с обязательным предъявлением аппаратного идентификатора пользователя) – проверяется PIN-код доступа к аппаратному идентификатору и идентификационные данные пользователя (введенные логин-пароль или предъявленный сертификат);
- ***Вход без токена*** (аутентификация без обязательного использования аппаратного идентификатора пользователя) – введенные идентификационные данные пользователя (пара логин-пароль) проверяются в ОС Windows, а затем сравниваются со значением, которое хранится в базе СЗИ. Только при положительном результате проверки (идентификационные данные пользователя в ОС и базе СЗИ совпадают) пользователю разрешается вход в систему.

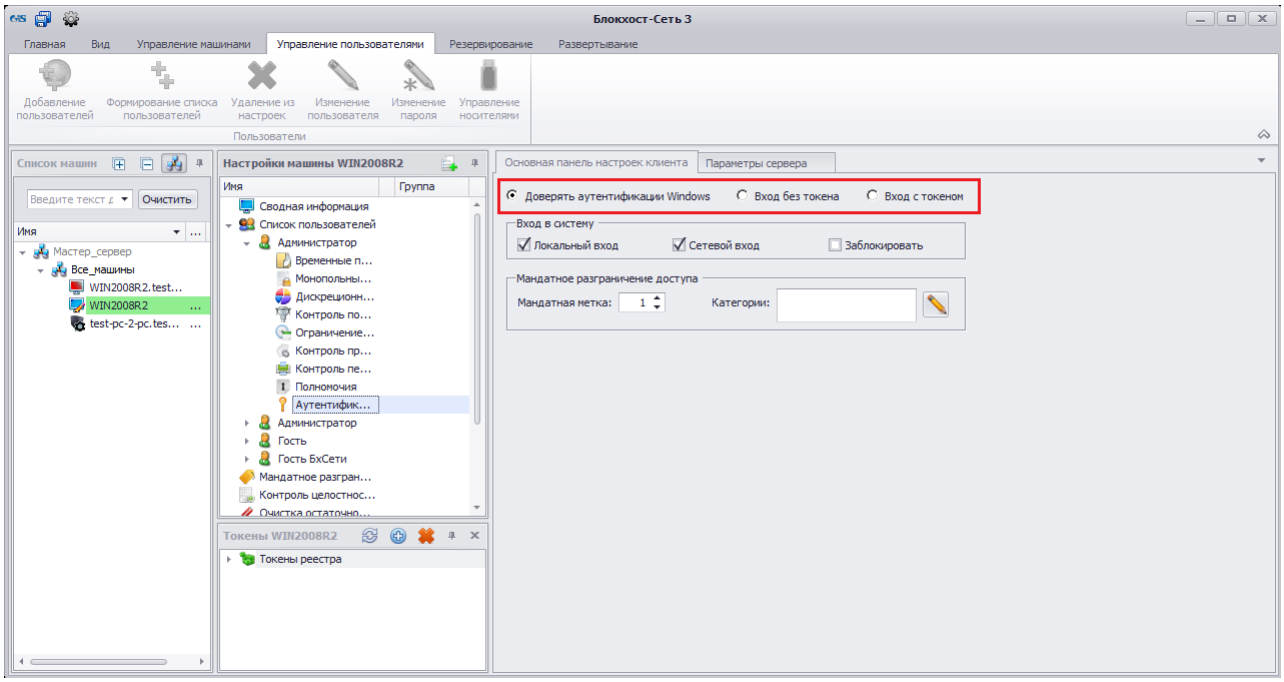


Рисунок 5.19 – Изменение способа аутентификации пользователя

По умолчанию для всех добавленных в СЗИ учетных записей пользователей (групп пользователей) установлен параметр ***Доверять аутентификации Windows***.

Для изменения способа аутентификации учетной записи пользователя (группы пользователей) администратору безопасности необходимо в **Основной панели настроек клиентов** (см. рис. 5.19) отметить параметр, который включает необходимый способ аутентификации.

После изменения параметров аутентификации учетных записей пользователя (групп пользователей) для сохранения внесенных изменений выбрать пункт меню ***Главная*** → ***Сохранить все***, или нажать кнопку ***Сохранить все***  , расположенную в левом верхнем углу консоли администрирования СЗИ.

5.2.1.6 Блокировка учетной записи

В СЗИ «Блокхост-Сеть 3» существует возможность временной блокировки учетной записи пользователя (группы пользователей). Учетная запись пользователя (группы пользователей) может быть заблокирована администратором в момент редактирования параметров пользователя (группы пользователей).

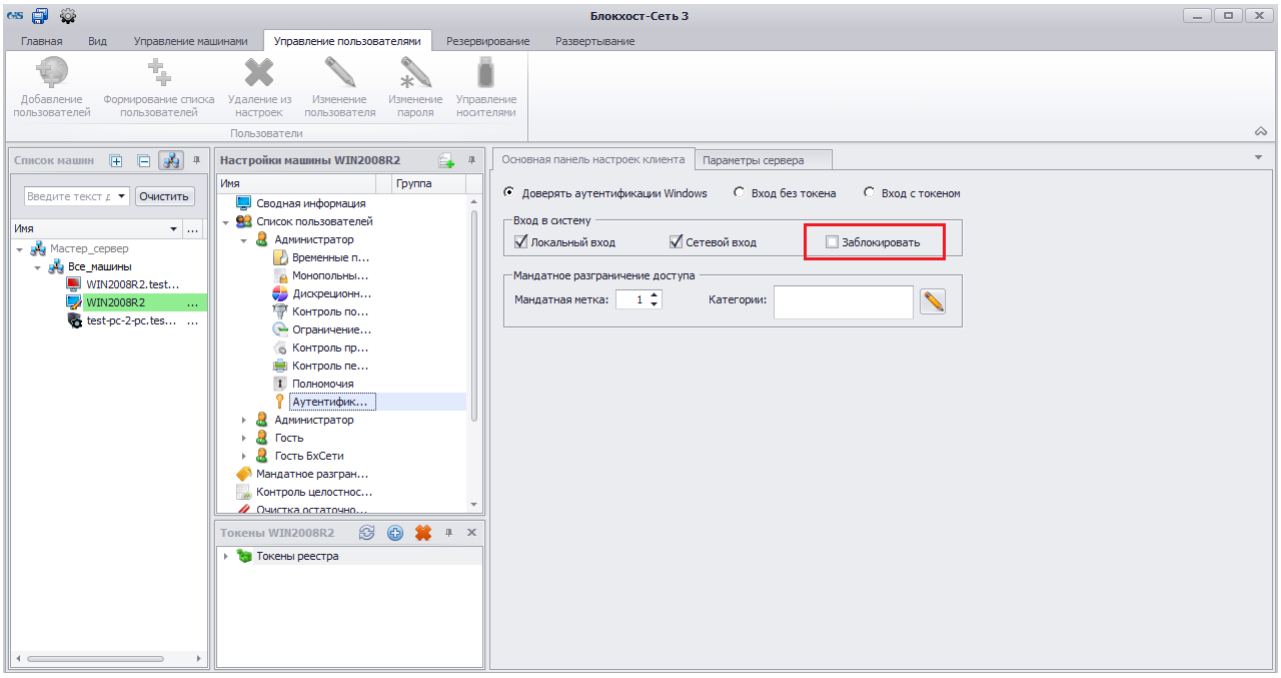


Рисунок 5.20 – Блокировка учетной записи пользователя

Для блокировки учетной записи пользователя (группы пользователей) средствами СЗИ «Блокхост-Сеть 3» администратору безопасности в **Основной панели настроек клиентов** (см. рис. 5.20) необходимо отметить параметр ***Заблокировать***.

Для сохранения внесенных изменений выбрать пункт меню ***Главная→ Сохранить все***, или нажать кнопку ***Сохранить все***  , расположенную в левом верхнем углу консоли администрирования СЗИ.

Настройка отложенной блокировки учетной записи пользователя (группы пользователей) осуществляется при настройке механизма ***Временные ограничения*** (подробнее см. п. 6.1.4 «Разграничение времени доступа в систему» настоящего Руководства).

5.2.2 Управление ключевыми носителями пользователя

В консоли администрирования СЗИ существует возможность управления персональными ключевыми носителями пользователя:

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

5.2.2.1 Добавление пользователю персонального ключевого носителя

Для присвоения пользователю персонального ключевого носителя в СЗИ «Блокхост-Сеть 3» администратору безопасности необходимо:

1) Подключить присваиваемый пользователю персональный ключевой носитель к рабочей станции или серверу безопасности (в зависимости от того, с какого рабочего места осуществляется настройка).

2) В консоли администрирования СЗИ 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*** (см. пример на рис. 5.1).

4) В **Основной панели настроек клиентов** выделить учетную запись пользователя, которому будет присвоен аппаратный идентификатор, и выбрать пункт меню ***Управление пользователями*** →***Управление носителями***.

5) Откроется окно **«Управление носителями»** (рис. 5.21), в котором администратору безопасности доступны операции присвоения пользователю персонального ключевого носителя, блокировки или удаления уже используемого этим пользователем ключевого носителя.

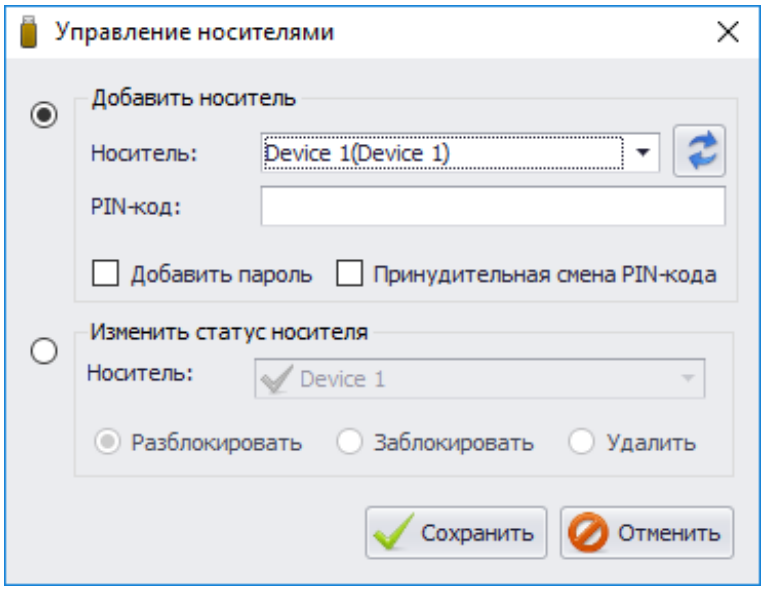


Рисунок 5.21 – Окно управления ключевыми носителями пользователя

6) В окне **«Управление носителями»**:

- отметить маркер в области *Добавить носитель*;
- из выпадающего списка поля ***Носитель*** выбрать имя считывателя, к которому подключен ключевой носитель, присваиваемый пользователю, и ввести PIN-код доступа к нему в соответствующее поле;

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

- при необходимости сохранения на добавляемом носителе пароля пользователя отметить параметр ***Добавить пароль***;
- для того чтобы пользователь при первом использовании нового ключевого носителя изменил PIN-код доступа к нему, необходимо отметить параметр ***Принудительная смена PIN-кода***;
- нажать кнопку ***Сохранить***:
  - если параметр ***Добавить пароль*** не отмечен, появится окно с сообщением об успешном добавлении идентификатора:

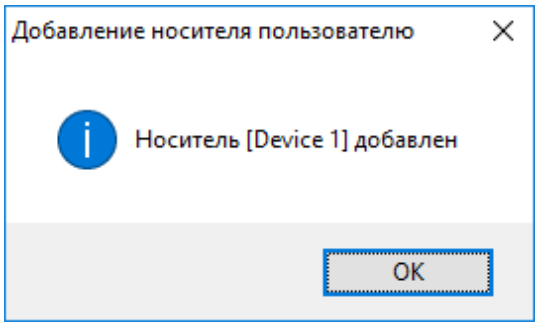


Рисунок 5.22 – Сообщение об успешном добавлении носителя

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

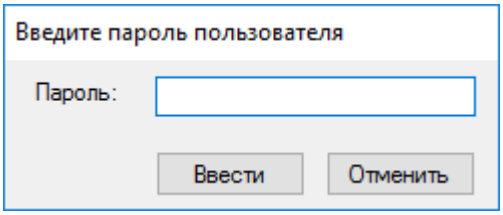


Рисунок 5.23 – Окно ввода пароля редактируемого пользователя

  - при сохранении на носителе пароля пользователя домена, который еще не входил в ОС редактируемой рабочей станции, 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. 5.22).

    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 все***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

5.2.2.2 Блокировка, разблокировка или удаление персонального ключевого носителя пользователя

Администратор безопасности из серверной или локальной консоли администрирования СЗИ может заблокировать (разблокировать) ключевой носитель, назначенный пользователю, или удалить его. Для изменения статуса персонального ключевого носителя пользователя необходимо:

1) В **Основной панели настроек клиентов** выбрать учетную запись пользователя, статус ключевого носителя которого будет изменяться, и выбрать пункт меню ***Управление пользователями →Управление носителями***.

2) В окне **«Управление носителями»** (см. рис. 5.21) отметить маркер области *Изменить статус носителя*.

3) В выпадающем списке поля ***Носитель*** выбрать ключевой носитель пользователя.

4) В зависимости от требуемого с ключевым носителем действия отметить соответствующий параметр:

- ***Заблокировать*** – позволяет запретить использование пользователем для входа в ОС выбранный персональный ключевой носитель;
- ***Разблокировать*** – позволяет разрешить использование ранее заблокированный персональный ключевой носитель;
- ***Удалить*** – позволяет отвязать выбранный персональный ключевой носитель 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 все*** в окне консоли администрирования, или

воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

5.3 Удаление учетных записей из списка пользователей СЗИ «Блокхост-Сеть 3»

Для удаления учетной записи пользователя (группы пользователей) из СЗИ «Блокхост-Сеть 3» администратору безопасности следует:

1) В консоли администрирования СЗИ в окне «**Список машин**» выбрать рабочую станцию, на которой необходимо удалить из списка пользователей СЗИ учетную запись пользователя (группы пользователей), для чего раскрыть пункт ***Все_машины*** и щелкнуть левой кнопкой мыши на имени рабочей станции:

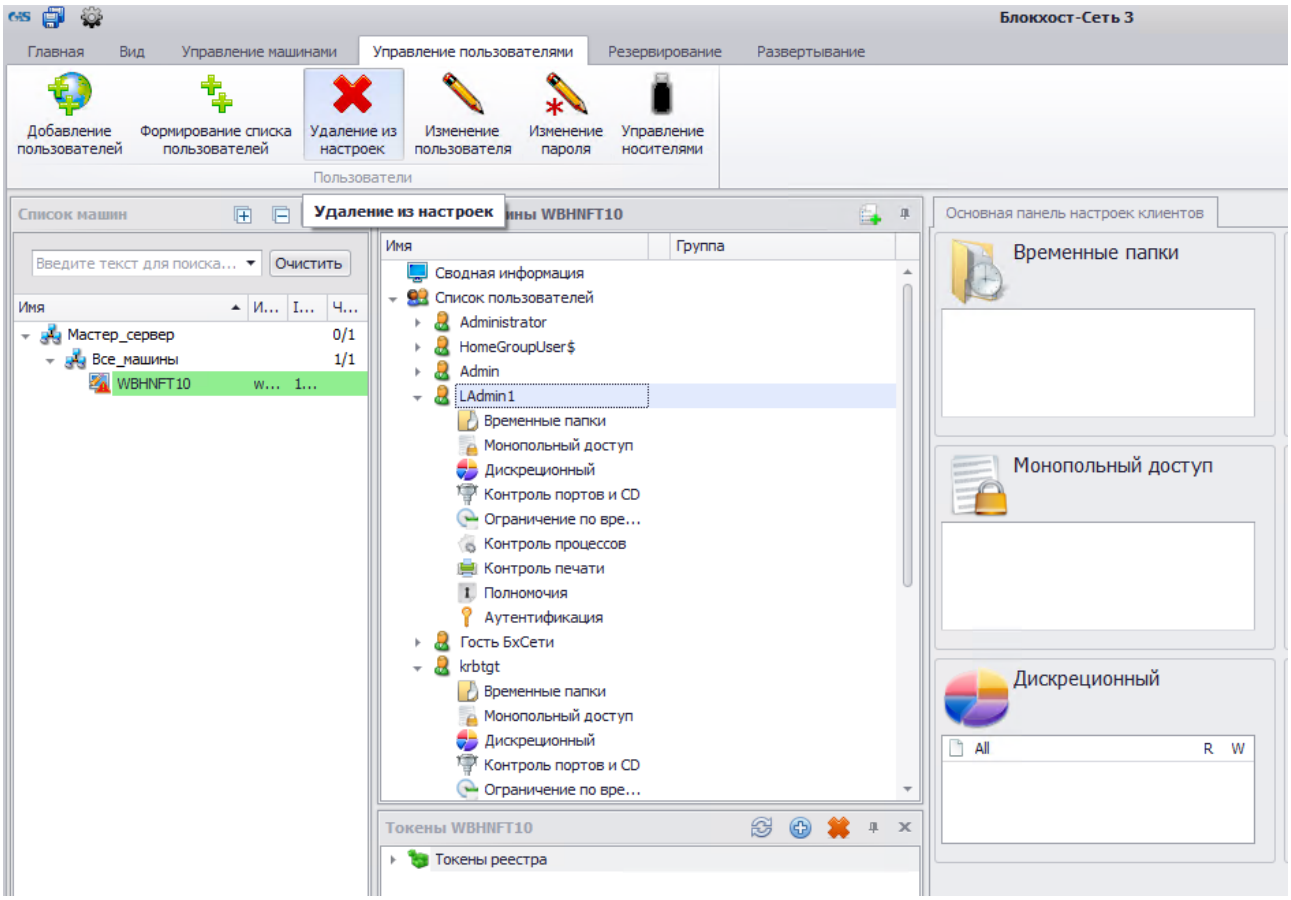


Рисунок 5.24 – Окно ввода пароля редактируемого пользователя

2) В окне «**Настройки машины**» выбрать пункт ***Список пользователей*** (рисунок 5.24).

3) В **Основной панели настроек клиентов** выделить учетную запись удаляемого пользователя (группы пользователей) и выбрать пункт меню ***Управление пользователями*** →***Удаление из настроек*** для его удаления из СЗИ.

4) Подтвердить удаление учетной записи пользователя (группы пользователей) в

появившемся диалоговом окне:

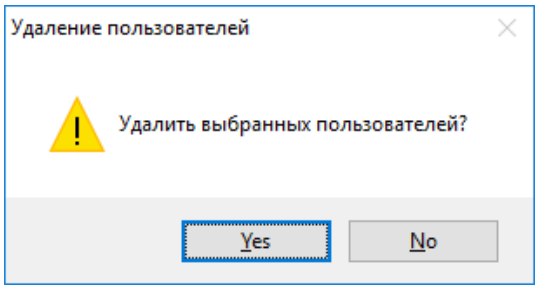


Рисунок 5.25 – Диалоговое окно подтверждения удаления пользователя

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

При удалении учетной записи пользователя (группы пользователей) из списка пользователей в СЗИ «Блокхост-Сеть 3» не происходит удаления его учетной записи из домена (или рабочей станции).

Нельзя удалить из списка пользователей СЗИ рабочей станции учетную запись **Гость БхСеть** и учетные записи пользователей (групп пользователей), которые были добавлены в СЗИ рабочей станции в результате синхронизации политик группы рабочих станций из серверной 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 3». Механизмы разграничения доступа и защиты информации, реализованные в СЗИ «Блокхост-Сеть 3», делятся на:

- **Настройки пользователей** – разграничение доступа пользователей и защиты. Настройки таких механизмов являются строго индивидуальными для каждого зарегистрированного в СЗИ «Блокхост-Сеть 3» пользователя.
- **Настройки станции** – механизмы защиты информации рабочей станции. Настройки таких механизмов производятся АБ для локального компьютера, на котором установлено СЗИ «Блокхост-Сеть 3». Эти механизмы являются общими для всех зарегистрированных в СЗИ «Блокхост-Сеть 3» пользователей.

Для корректного использования дискреционного и мандатного механизма СЗИ «Блокхост-Сеть 3», а также механизма запуска процессов АБ 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 пользовательских механизмов разграничения доступа

Пользовательские механизмы защиты информации настраиваются строго индивидуально для каждого зарегистрированного в СЗИ «Блокхост-Сеть 3» пользователя. В состав пользовательских механизмов СЗИ 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, идентификация и аутентификация пользователей, контроль печати.

Произведенные настройки пользовательских механизмов разграничения доступа вступают в силу после завершения текущего сеанса пользователя или перезагрузки ОС на контролируемой рабочей станции. Следует учесть, что перезагрузка ОС, инициированная из серверной 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 СЗИ вступят в силу.

6.1.1 Дискреционное разграничение доступа к объектам файловой системы

Реализация дискреционного механизма в СЗИ «Блокхост-Сеть 3» заключается в контроле доступа пользователей, в т.ч. и АБ, к объектам файловой системы (логические диски, каталоги и файлы). 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 3» возможны следующие виды доступа:

- **Чтение**. С помощью данного вида доступа санкционируется возможность чтения пользователем 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 АБ может санкционировать такие действия контролируемых пользователей, которые приводят к изменениям информации в объекте, удалению, переименованию и перемещению объекта.

6.1.1.2 Реализация дискреционной модели разграничения доступа

По умолчанию в список объектов файловой системы дискреционного механизма СЗИ «Блокхост-Сеть 3» добавлен файловый объект (ресурс) ***All***, который подразумевает под собой все логические диски, которые доступны пользователю при работе в операционной системе. Параметры доступа, определенные для файлового объекта ***All***, будут применены для всех явно недобавленных в список ресурсов дискреционного механизма СЗИ логических дисков рабочей станции.

Параметры дискреционного доступа, указанные для диска (каталога), автоматически распространяются и на вложенные в него файлы и каталоги. Для изменения параметров доступа к вложенным объектам необходимо добавить их в список объектов дискреционного механизма СЗИ и указать требуемые параметры доступа.

Для того чтобы реализовать с помощью СЗИ «Блокхост-Сеть 3» дискреционную модель разграничения доступа, АБ необходимо выполнить следующие действия:

1) В окне **«Список машин»** консоли администрирования СЗИ раскрыв пункт

Все_машины, выделить рабочую станцию, для которой будет производиться настройка дискреционного механизма.

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***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.1).

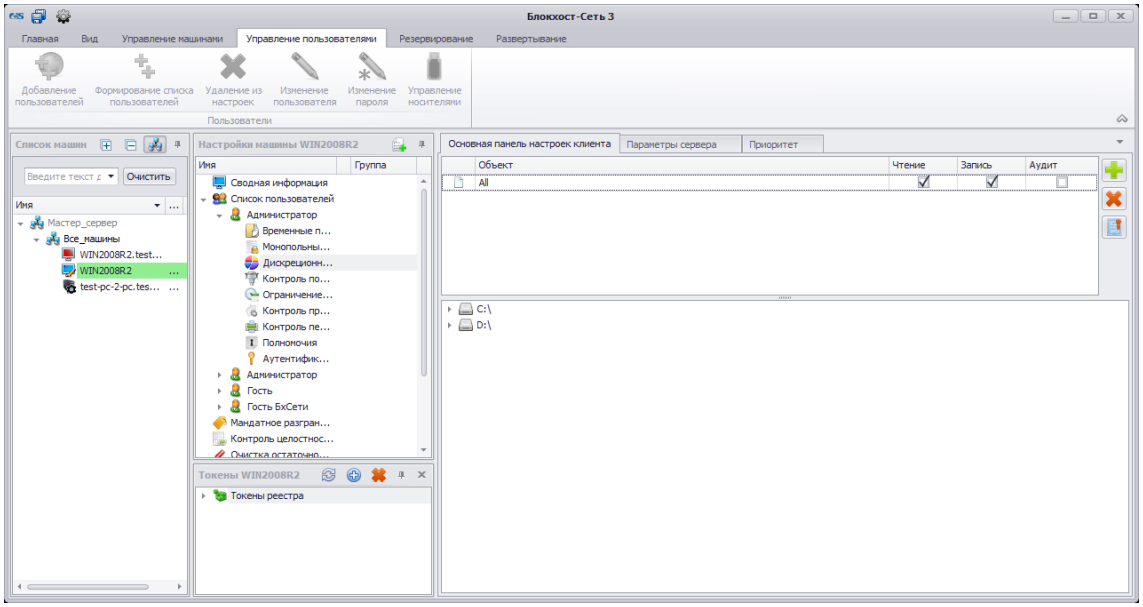


Рисунок 6.1 – Настройка дискреционного механизма разграничения доступа

3) В **Основной панели настроек клиентов** добавить необходимые файловые объекты (ресурсы) на контроль одним из перечисленных ниже способов:

- захватить и перетащить мышью необходимые объекты из дерева ресурсов в область настроек (рис. 6.2);
- нажать кнопку ***Добавить***  , и в открывшемся окне «**Выбор**» (рис. 6.3) выбрать нужный объект (файл или каталог) и нажать кнопку ***Добавить***.

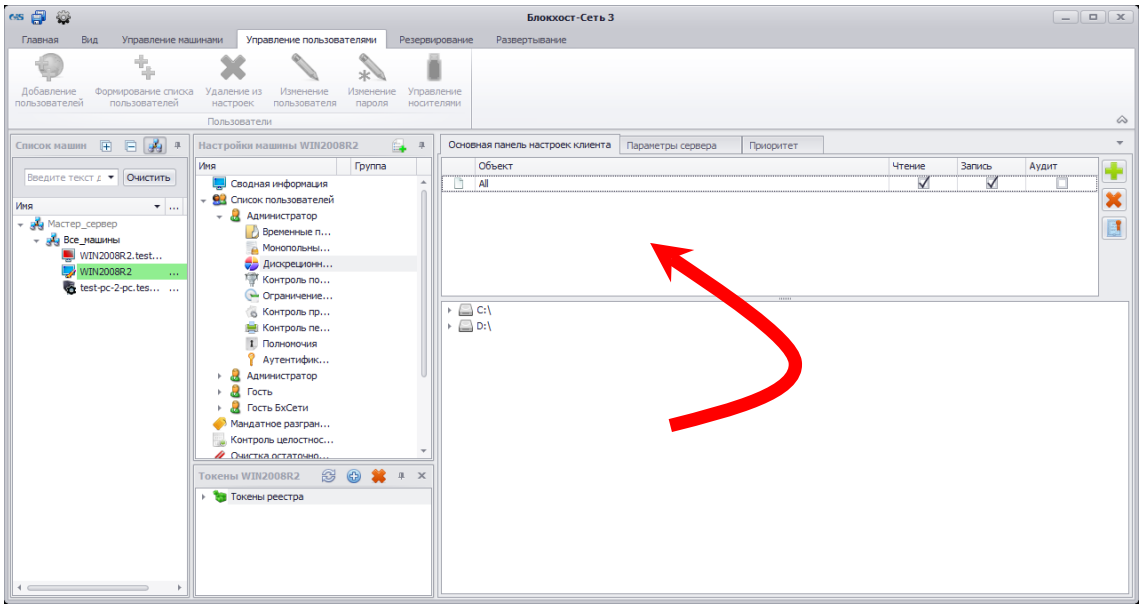


Рисунок 6.2 – Добавление контролируемых объектов в настройки дискреционного механизма

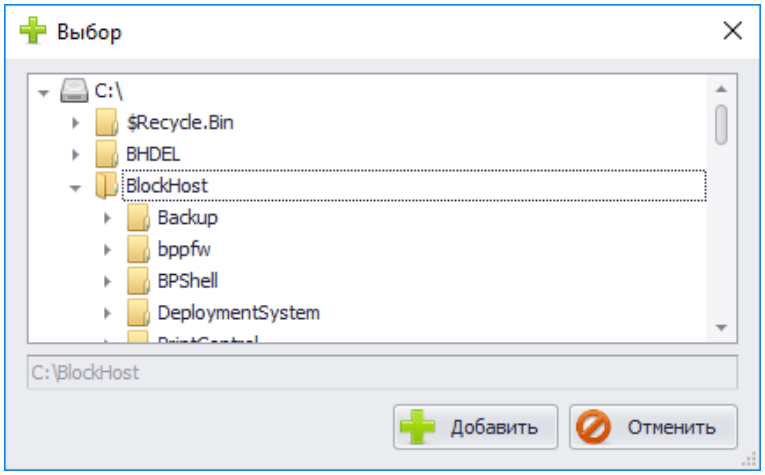


Рисунок 6.3 – Окно выбора файловых объектов

4) Для удаления объектов из списка контролируемых достаточно выделить в области настроек требуемый файловый объект и нажать клавишу **<Del>**. Также для удаления объекта можно воспользоваться кнопкой ***Удалить*** .

5) Для разрешения доступа пользователя к файловому объекту (ресурсу) на чтение и/или запись администратор безопасности должен отметить соответствующие параметры (***Чтение***, ***Запись***) в группе полей, расположенных справа от выбранного объекта файловой системы.

6) При необходимости АБ может разрешить фиксацию событий, связанных с безопасностью информации, содержащейся в данном объекте, в журнал СЗИ «Блокхост-Сеть 3». Для этого в области настроек необходимо отметить параметр ***Аудит***, расположенный в группе полей справа от выбранного объекта файловой

системы (рис. 6.4).

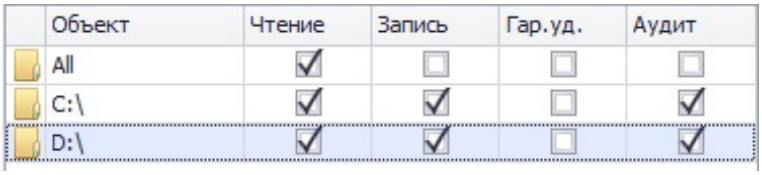


Рисунок 6.4 – Включение настройки аудита в дискреционном механизме разграничения доступа

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

Политика безопасности в СЗИ «Блокхост-Сеть 3» 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 3» 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.

На рисунке 6.5 показан пример дискреционной политики разграничения доступа пользователя к объектам ФС. Из рисунка видно, что пользователю запрещен доступ ко всем дискам (томам), расположенным на рабочей станции, за исключением диска *C:*, правом чтения которого пользователь наделен, при этом 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*, попытки доступа пользователей к которой будут фиксироваться в журнале аудита СЗИ (отмечен параметр ***Аудит***).

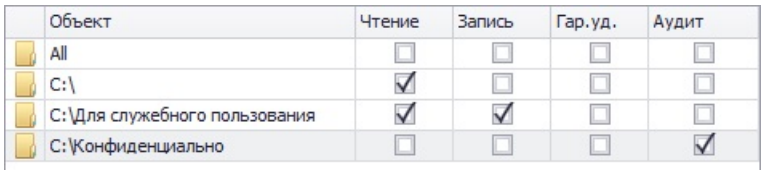


Рисунок 6.5 – Пример дискреционной политики разграничения доступа

Особенность работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа описана в Приложении 2 к настоящему документу.

6.1.2 Разграничение доступа к отчуждаемым физическим носителям информации

В СЗИ «Блокхост-Сеть 3» реализован механизм разграничения доступа пользователей к отчуждаемым носителям информации. Реализация механизма разграничения доступа к отчуждаемым носителям информации в СЗИ «Блокхост-Сеть 3» заключается в предоставлении АБ возможности санкционировать доступ каждого пользователя к следующим устройствам:

- CD- и DVD-дисководам;
- USB-устройствам;
- 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) АБ может воспользоваться дискреционным или мандатным механизмом разграничения доступа, рассмотрев требуемый носитель информации как объект файловой системы.

При использовании механизма мандатного разграничения доступа, для каждого пользователя блокируется доступ к COM-, LPT-, CD-портам.

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, АБ необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ раскрыв пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма разграничения доступа к отчуждаемым носителям информации.

2) В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя/группу пользователей, для которой 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***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.6).

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. 6.6).

4) При необходимости возможна фиксация событий, связанных с доступом к контролируемым объектам, в журнал СЗИ «Блокхост-Сеть 3». Для этого необходимо отметить поле ***Аудит***, расположенное справа от выбранного порта (USB-устройства).

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

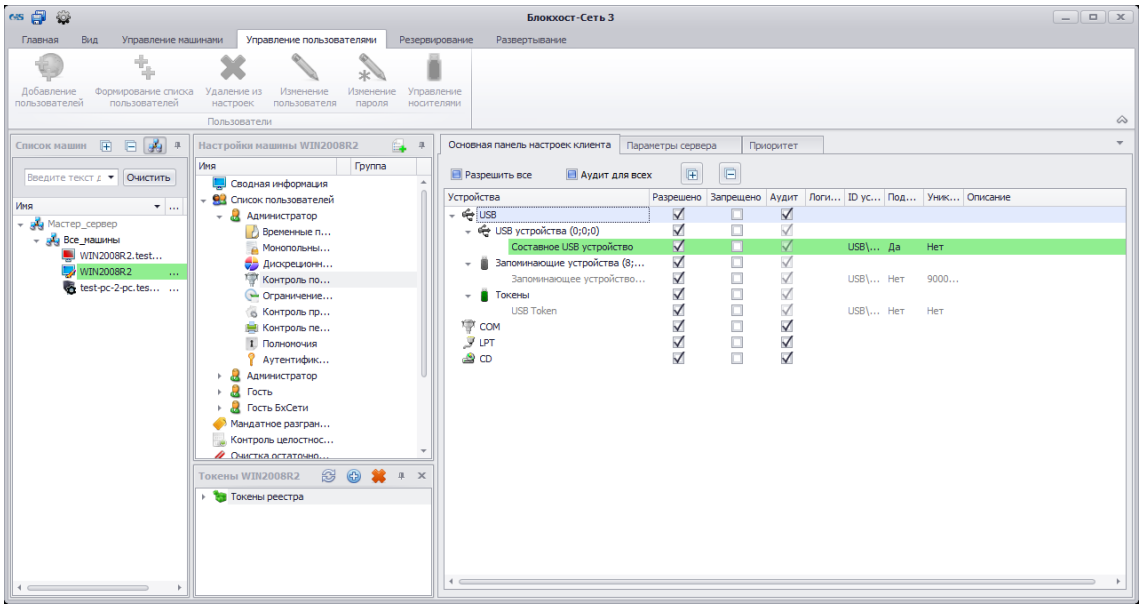


Рисунок 6.6 – Настройка механизма контроля портов

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 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. 6.7). 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.

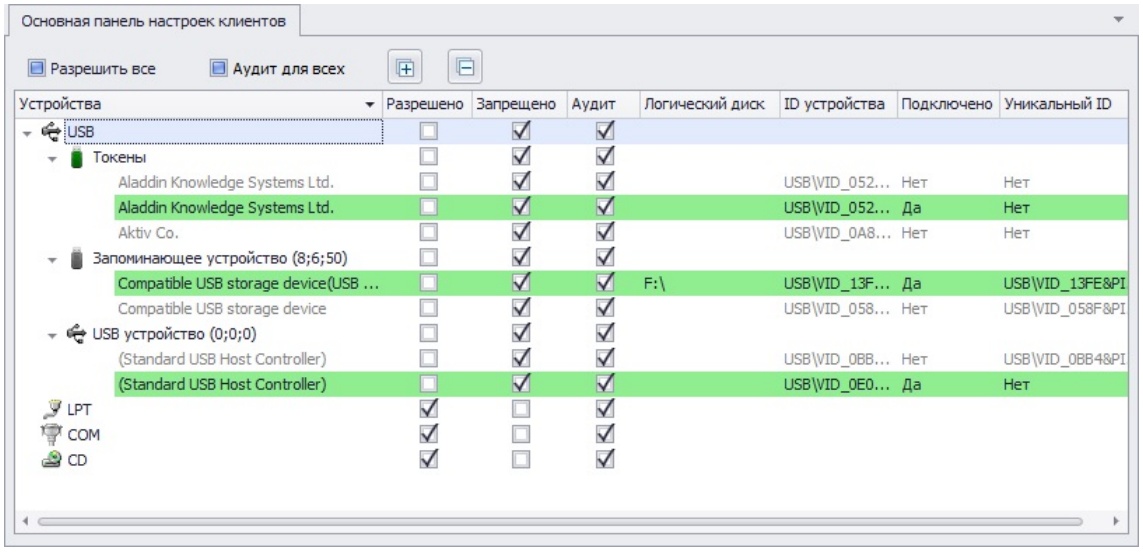


Рисунок 6.7 – Полный запрет доступа к USB-устройствам

В СЗИ «Блокхост-Сеть 3» 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 6.6 и 6.7 к классам USB-устройств относятся ***Запоминающие устройства и Токены***) – установленный параметр ***Запрещено (Разрешено)*** в строке с названием класса устройства запрещает (разрешает) использование всех подключаемых 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 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:

Доступ разрешен:

- всем подключаемым USB-устройствам, если параметр ***Разрешено*** установлен для всего интерфейса **USB**;
- всем подключаемым устройствам одного класса, если установлен параметр ***Разрешено*** для этого класса USB-устройств;
- всем подключаемым одинаковым **моделям одного класса устройств**, если параметр ***Разрешено*** установлен для этой модели USB-устройств.

Доступ запрещен:

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

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

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

6.1.3 Разграничение доступа к запуску процессов

В СЗИ «Блокхост-Сеть 3» 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 создать модель защиты информации типа **модель разрешенных процессов (модель замкнутой среды)**, которая 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 3» 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 замкнутой среды (модели разрешенных процессов)

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

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка модели разрешенных 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. 6.8). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (см. рис. 6.8).

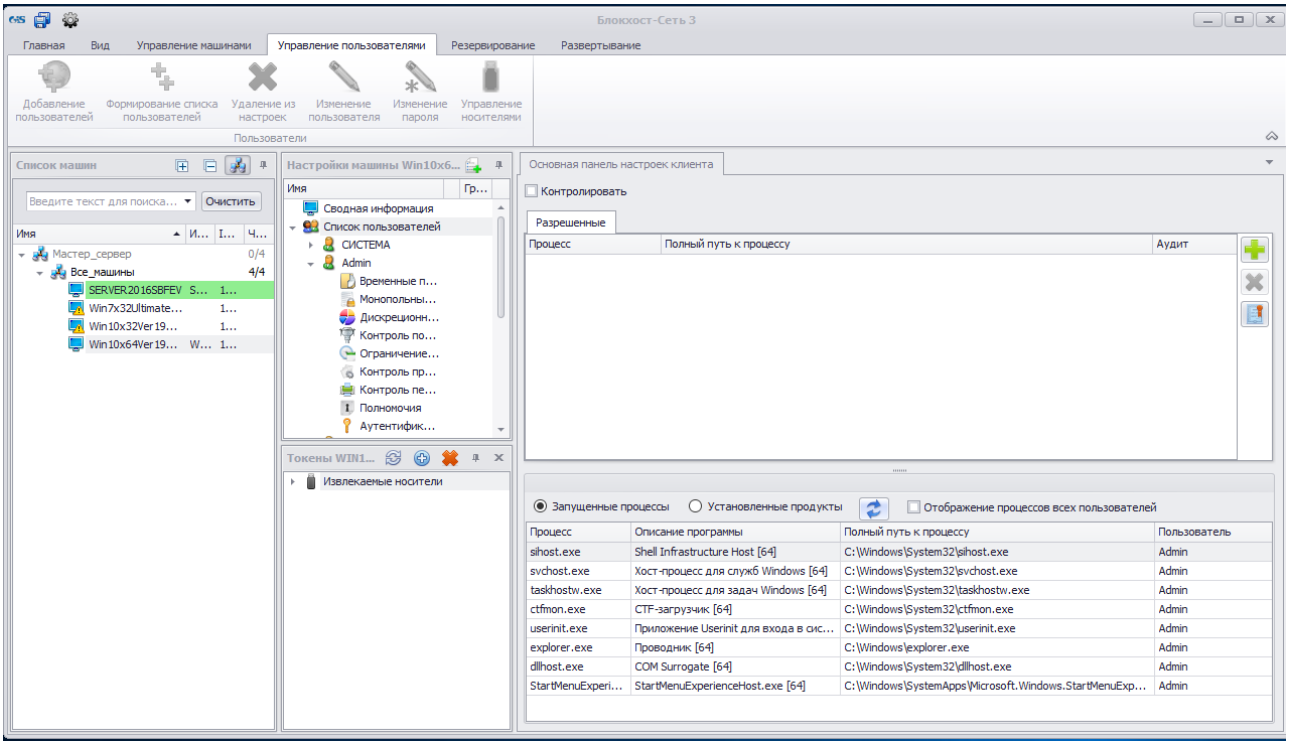


Рисунок 6.8 – Выбор механизма «Контроль процессов»

3) 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 (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить несколько процессов):

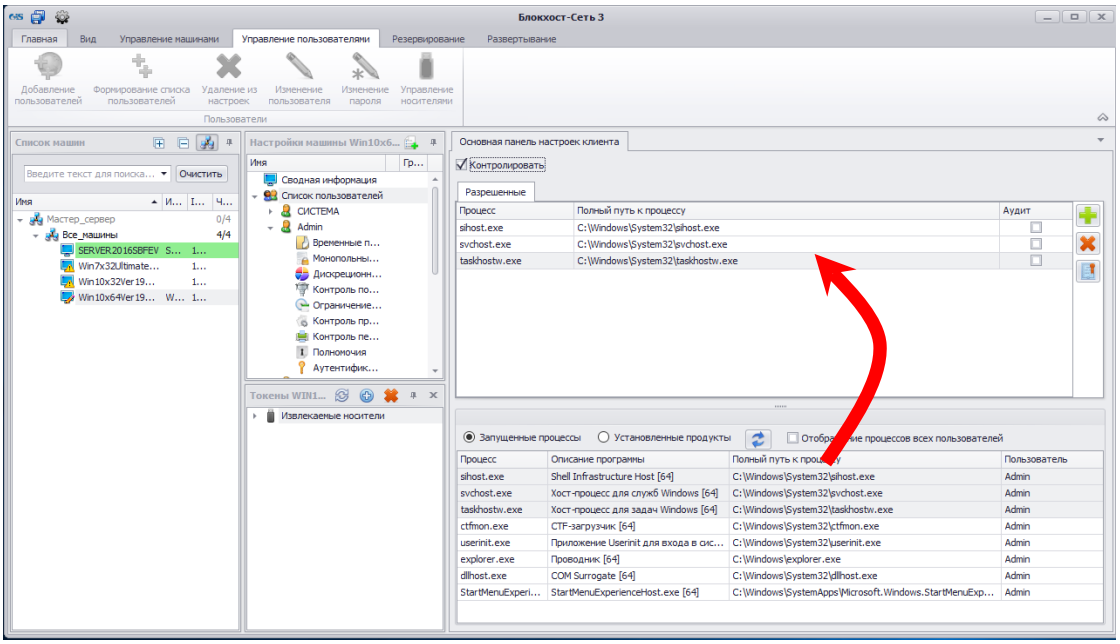


Рисунок 6.9 – Добавление разрешенных процессов в список

- нажать кнопку ***Добавить***  , и в открывшемся окне «**Выбор**» (см. пример на рис. 6.3) выбрать нужный процесс и нажать кнопку ***Добавить***.

Переключатель ***Запущенные процессы↔Установленные продукты*** в области *Запущенные процессы* (см. рис. 6.9) позволяет отображать либо список запущенных на рабочей станции процессов (переключатель установлен в положение ***Запущенные процессы***), либо список всех исполняемых файлов из перечня, установленного на рабочей станции ПО (переключатель установлен в положение ***Установленные 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 ***Запущенные процессы↔Установленные продукты*** установлен в положение ***Запущенные процессы***). Для отображения списка всех запущенных на рабочей станции процессов необходимо установить параметр ***Отображение процессов всех пользователей***.

Разрешенные для запуска процессы появятся в области настроек (рис. 6.10);

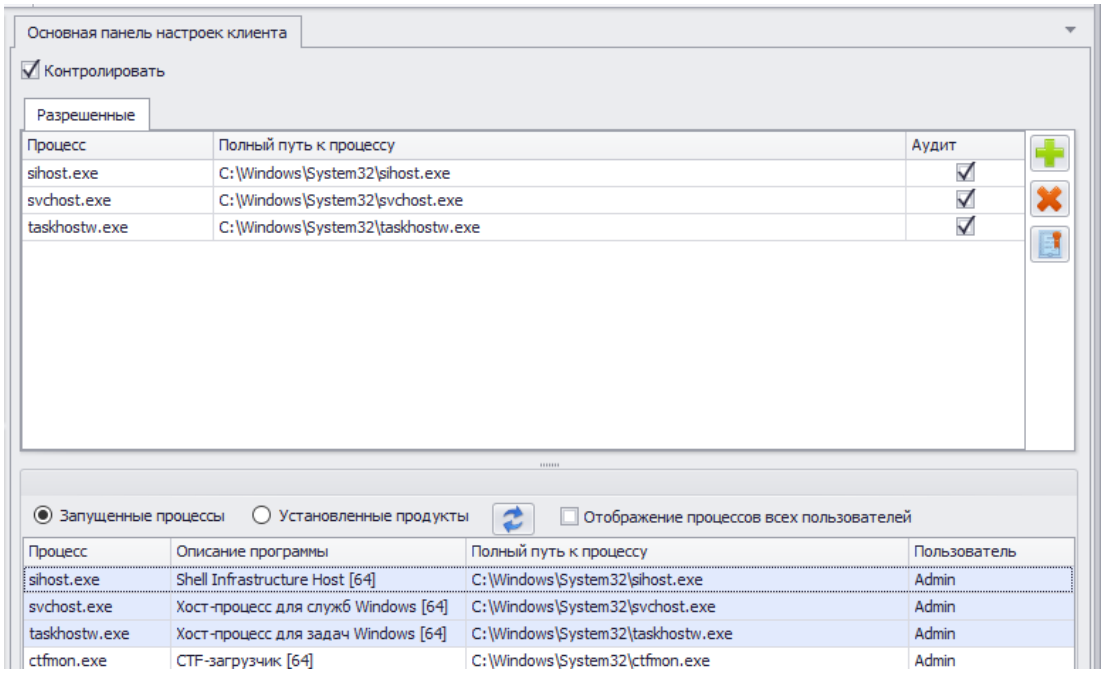


Рисунок 6.10 – Отображение добавленного процесса

4) 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. 6.11);

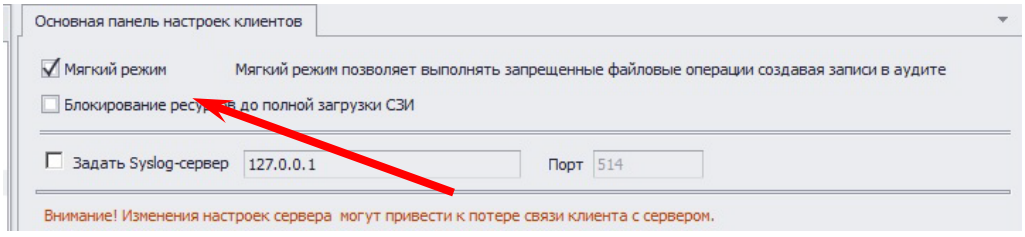


Рисунок 6.11 – Включение «Мягкого режима»

- сохранить настройки выбрав пункт меню ***Главная→ Сохранить все,*** 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 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. пример на рис. 6.10);
- начнется процесс загрузки сообщений аудита, который в зависимости от количества событий может занять некоторое время (рис. 6.12);

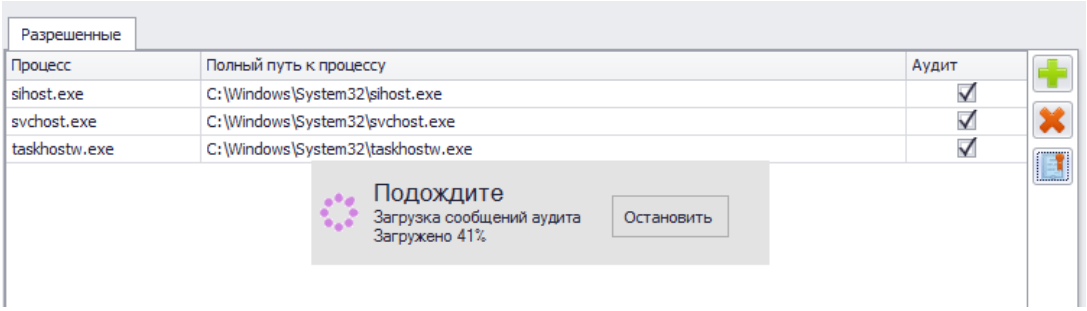


Рисунок 6.12 – Процесс загрузки сообщений аудита при формировании замкнутой среды

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

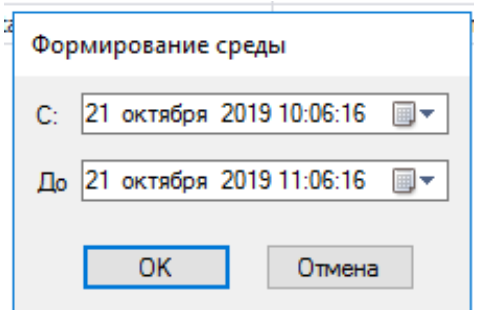


Рисунок 6.13 – Окно «Формирование среды»

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

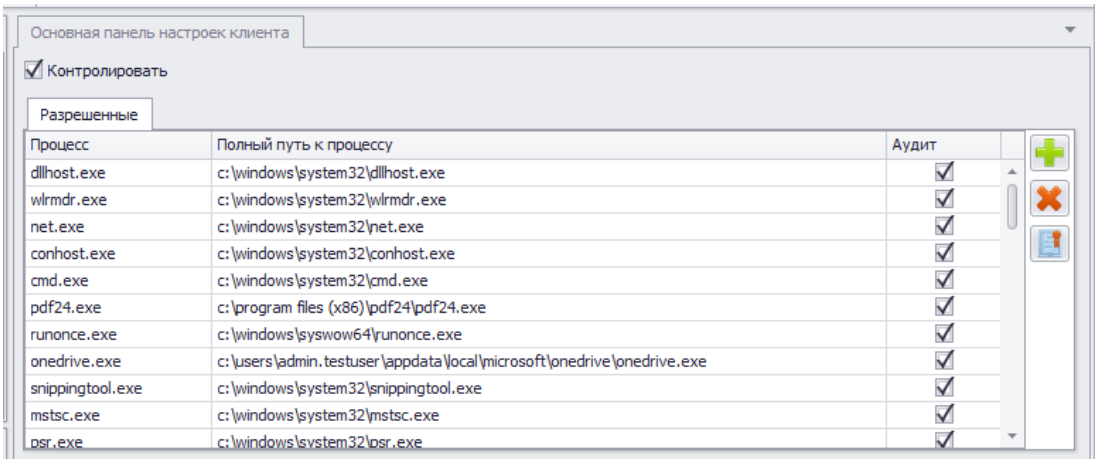


Рисунок 6.14 – Список процессов, разрешенных к запуску пользователем

- при необходимости можно откорректировать список разрешенных к запуску процессов, удалив из него ненужные, 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 3», 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** (см. пример на рис. 6.11).

5) Для включения режима замкнутой среды необходимо установить опцию ***Контролировать***, расположенную в верхней части вкладки (рис. 6.14) и сохранить настройки, выбрав пункт меню ***Главная*** → ***Сохранить все***, 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.

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

6.1.4 Разграничение времени доступа пользователей в систему

Механизм разграничения времени доступа пользователей 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 пользователей 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»** консоли администрирования СЗИ, 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. 6.15, а). В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.15, б).

3) В **Основной панели настроек клиентов** установить параметр ***Включить временные ограничения*** (рис. 6.15, 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.

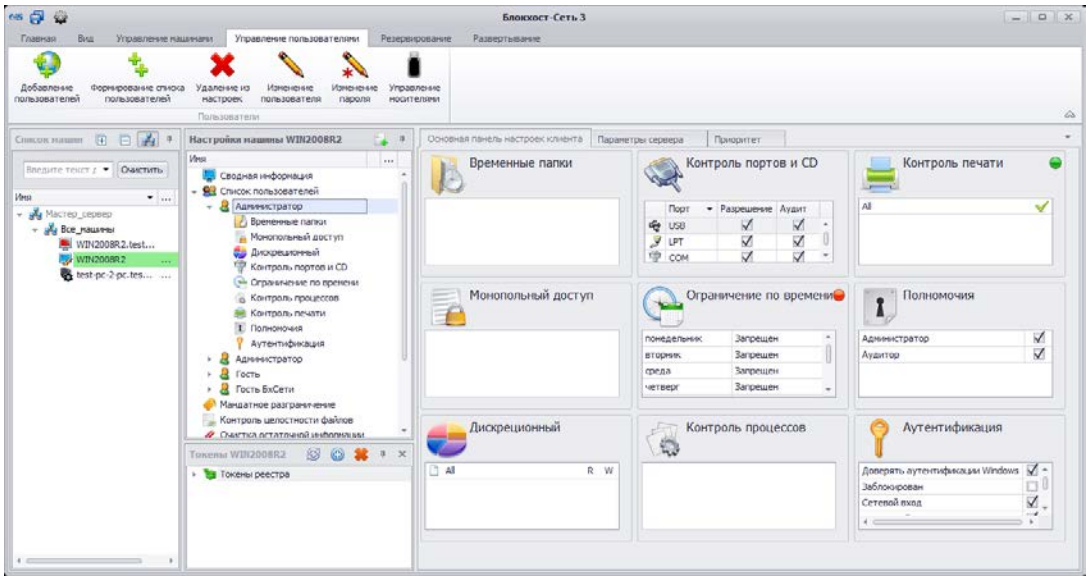
4) Установить время, в которое работа на рабочей станции пользователю будет запрещена. Для этого левой кнопкой мыши отметить соответствующие временные интервалы для каждого из дней недели. Красным цветом отмечаются промежутки времени, в которые работа запрещена, зеленым – разрешена (рис. 6.15, в).

При настройке механизма разграничения времени работы пользователей в 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.

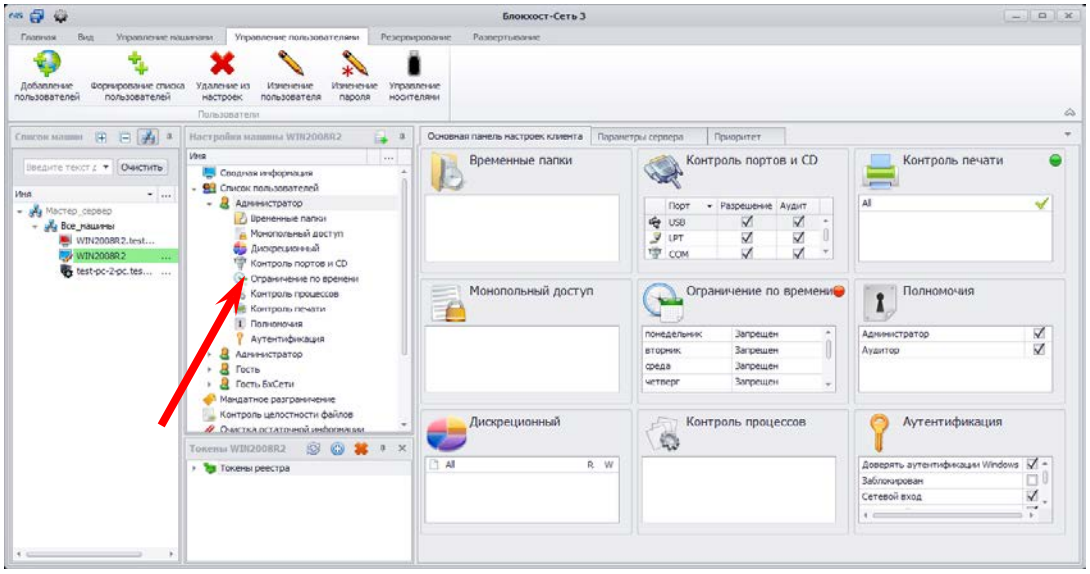
5) При необходимости можно разрешить фиксацию попыток входа пользователей в систему в несанкционированное время. Для этого в области настроек необходимо выбрать пункт ***Вести аудит временных ограничений***.

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

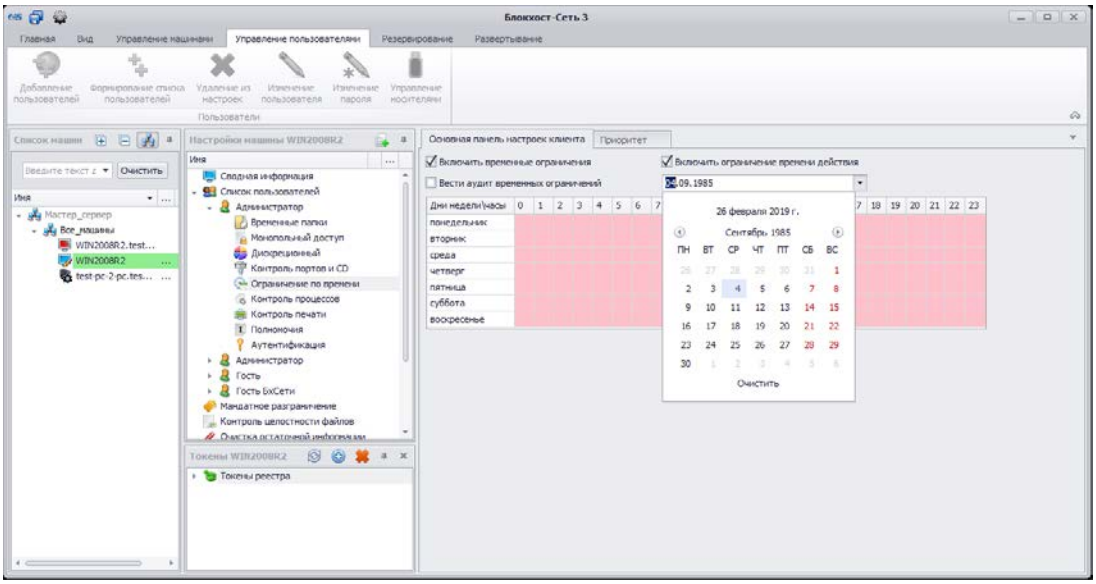
При настройке механизма разграничения времени работы пользователя на контролируемой рабочей станции администратор безопасности должен учесть, что для одного и того же дня недели время начала работы не может превышать время окончания работы.


Блокхост-Сеть 3
Временные папки
Контроль портов и CD
Контроль печати
Монопольный доступ
Ограничение по времени
Полномочия
Дискреционный
Контроль процессов
Аутентификация

а)


Блокхост-Сеть 3
Временные папки
Контроль портов и CD
Контроль печати
Монопольный доступ
Ограничение по времени
Полномочия
Дискреционный
Контроль процессов
Аутентификация

б)



в)

Рисунок 6.15 – Настройка временных ограничений

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. 6.16) о принудительном завершении работы ОС. Для исключения случайной потери данных пользователь должен сохранить все несохраненные данные и осуществить выход из системы.

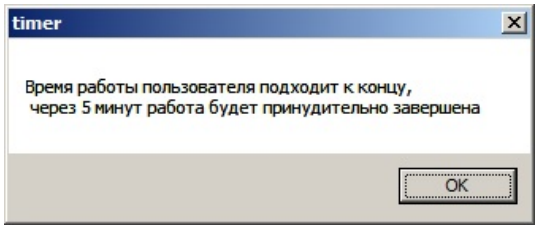


Рисунок 6.16 – Предупреждение об окончании времени работы пользователя в ОС

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.

6.1.4.2 Ограничение доступа пользователя

В СЗИ «Блокхост-Сеть 3» существует возможность ограничить доступ учетной записи пользователя в ОС контролируемой рабочей станции в установленное время. Для этого необходимо отметить параметр ***Включить ограничение времени действия*** (см. пример на рис. 6.15, в) и указать дату, после окончания которой (в 23 часа 59 минут указанной даты) учетной записи будет отказано во входе до момента окончания действия ограничения. В результате пользователь не сможет войти в систему после указанной даты независимо от установленных настроек механизма разграничения доступа пользователя в ОС по времени.

На пользователя, аутентификация которого осуществляется стандартными средствами ОС Windows (подробнее см. п. «5.2.1 Изменение общих параметров учетных записей пользователей» настоящего руководства), автоматическая блокировка, установленная средствами СЗИ, не распространяется. Для блокировки такого пользователя необходимо воспользоваться средствами ОС Windows или Active Directory (если пользователь доменный).

6.1.5 Настройки мандатного механизма разграничения доступа

В СЗИ «Блокхост-Сеть 3» реализован механизм мандатного (полномочного) разграничения доступа. Реализация мандатного механизма заключается в возможности присвоения администратором безопасности субъектам (пользователям) и объектам (ресурсам) классификационных уровней, отражающих их место в иерархии системы разграничения доступа. Классификационный уровень субъектов и объектов доступа является комбинацией назначенных им иерархических меток и неиерархических категорий.

Классификационные метки (иерархическая категория) присваиваются субъектам/объектам из диапазона чисел 1-255 и соответствуют их месту (уровню) иерархии в пределах иерархической категории. Иерархическая категория определяет уровень конфиденциальности защищаемой информации (чем метка больше, тем выше степень конфиденциальности). Иерархическая метка субъекта определяет права доступа к соответствующей иерархической категории. Неиерархические категории выступают в качестве ограничений по доступу субъектов к объектам, соответствующих неиерархических категорий.

Общий принцип работы мандатного механизма основан на взаимосвязи субъектов доступа (пользователей), объектов доступа (объектов файловой системы) и классификационных уровней (значений мандатных меток и категорий). Доступ субъекта к объекту санкционируется лишь в том случае, если выполняется ряд условий. Условия доступа субъектов к объектам для СЗИ «Блокхост-Сеть 3» приведены в таблице 6.2.

При 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 иерархических меток мандатного механизма определяются администратором безопасности исходя из требований политики безопасности. Мандатная иерархическая 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 3» субъекты могут осуществлять следующие виды доступа к объектам:

- доступ на *чтение*. Субъект может читать информацию из объекта, если его иерархическая метка не меньше, чем иерархическая метка объекта, к которому выполняется попытка доступа, и неиерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта. Субъект может осуществлять копирование объекта при условии строгого равенства классификационного уровня субъекта, классификационного уровня копируемого объекта и классификационного уровня объекта файловой системы, в который производится копирование;
- доступ на *запись*. Пользователь может осуществлять запись в объект, только если значение классификационного уровня пользователя равно значению классификационного уровня объекта.

Таблица 6.2 – Условия доступа субъектов к объектам при мандатном механизме разграничения доступа СЗИ «Блокхост-Сеть 3»

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

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

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

Порядок создания иерархической мандатных меток и неиерархических категорий, их сопоставление ресурсам рабочей станции описаны в пункте 6.2.2 настоящего документа.

6.1.5.1 Изменение мандатных меток и категорий пользователей

Для работы с конфиденциальными ресурсами пользователи должны иметь соответствующий уровень доступа, задаваемый категорией и числовым значением мандатной метки. Присвоение пользователю классификационного уровня доступа выполняется в следующей последовательности:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, для пользователя которой будет производиться изменение классификационного уровня доступа.

2) В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, классификационный уровень доступа которого будет изменяться, и затем выбрать пункт ***Аутентификация*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Аутентификация***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.17).

3) В области *Мандатное разграничение доступа* **Основной панели настроек клиентов** (рис. 6.17):

- для корректировки назначенной пользователю иерархической мандатной метки в поле ***Мандатная метка*** установить требуемое значение метки;
- для корректировки списка назначенных пользователю категорий нажать кнопку ***Изменить категории*** и в открывшемся окне **«Список существующих категорий»** (см. пример на рис. 5.11) выделить необходимую категорию (с помощью клавиш **<Ctrl>** или **<Shift>** можно выделить несколько категорий) и нажать кнопку ***Применить***;

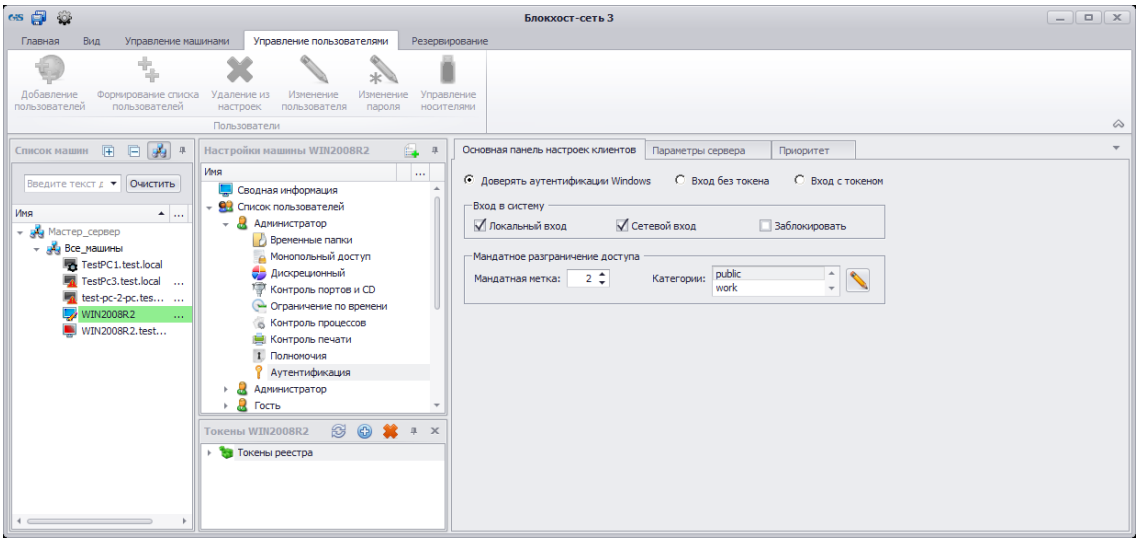


Рисунок 6.17 – Изменение классификационного уровня доступа пользователей

4) Изменить значение иерархической 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 (рис. 6.18).

5) Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить все***, 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*** без назначенных неиерархических категорий.

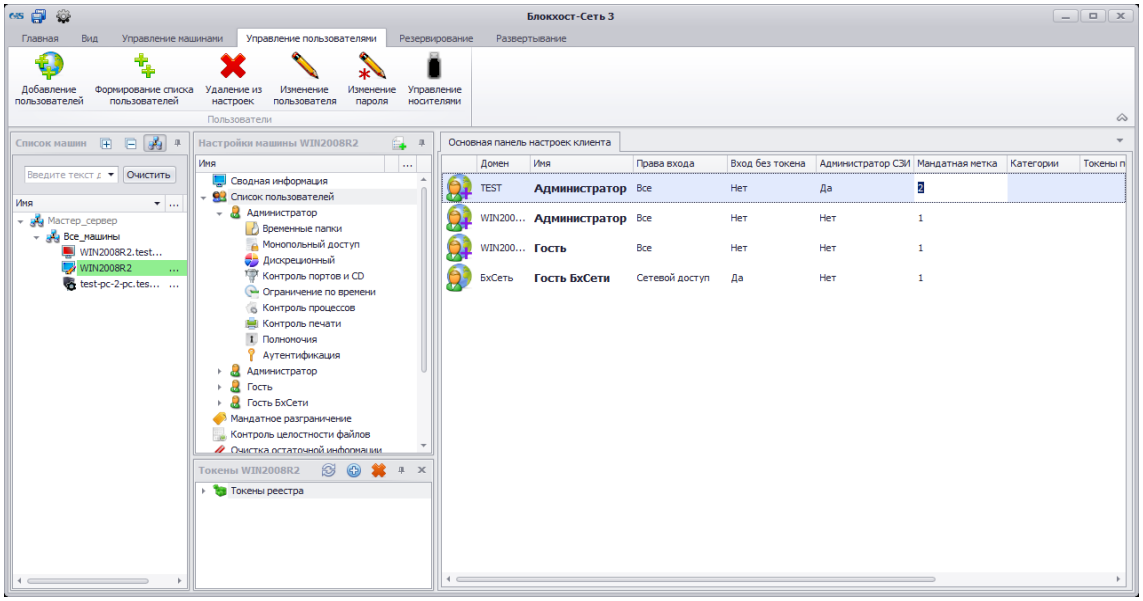


Рисунок 6.18 – Изменение мандатной метки пользователя

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 уровень доступа вошедшего пользователя и уровень конфиденциальности каталога, в котором приложения создают временные файлы, будут отличаться, такие приложения не смогут полноценно работать.

В СЗИ «Блокхост-Сеть 3» существует возможность назначения **динамического уровня конфиденциальности**, равного уровню доступа вошедшего пользователя, объектам файловой системы, определенным в СЗИ как ***Временные папки***. В результате такого назначения уровня конфиденциальности приложения получат полный доступ к этим папкам, независимо от уровня конфиденциальности родительского ресурса.

Следует иметь в виду, что содержимое каталогов, определенных как ***Временные папки***, затирается СЗИ «Блокхост-Сеть 3» по завершению сеанса работы пользователя. Необходимо быть внимательным при настройке этого механизма, чтобы в процессе работы СЗИ не была удалена нужная информация и не нарушилась работа установленных в системе приложений.

Настройка механизма ***Временных папок*** осуществляется индивидуально для каждого пользователя и выполняется в следующем порядке:

1) В окне **«Список машин»** консоли администрирования СЗИ, 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***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.19).

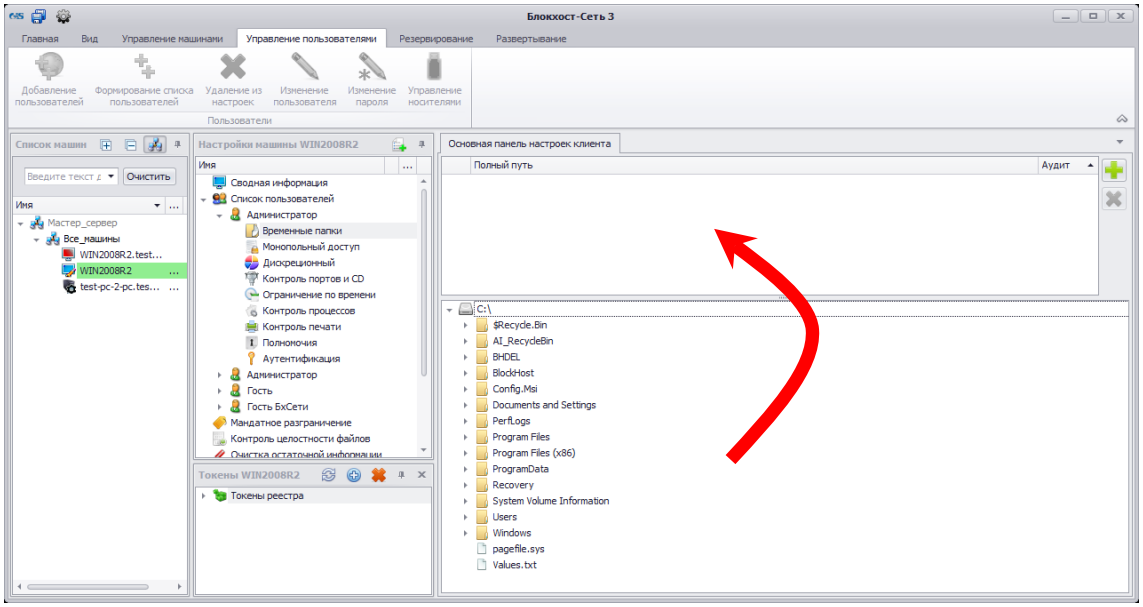


Рисунок 6.19 – Настройка механизма временных папок

3) В **Основной панели настроек клиентов** добавить ресурсы на контроль одним из перечисленных ниже способов:

- захватить и перетащить мышью необходимые объекты из дерева ресурсов в область настроек (рис. 6.19);
- нажать кнопку ***Добавить***  , в открывшемся окне «**Выбор**» (см. пример на рис. 6.3) выделить нужный каталог и нажать кнопку ***Добавить***.

4) Также можно настроить фиксацию событий доступа приложений к

контролируемым объектам в журнал событий СЗИ «Блокхост-Сеть 3», отметив параметр ***Аудит***, расположенный справа от выбранного каталога.

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.

При постановке на контроль механизма ***Временные папки*** каталогов, содержимое которых не может быть полностью удалено (например, файл открыт в приложении, которое препятствует его удалению), у пользователя, для которого выполнялась такая настройка, возникнет ошибка входа в систему (рис. 6.20). При возникновении такой ошибки администратору безопасности необходимо удалить из механизма ***Временные папки*** каталоги, содержимое которых не может быть очищено средствами СЗИ.

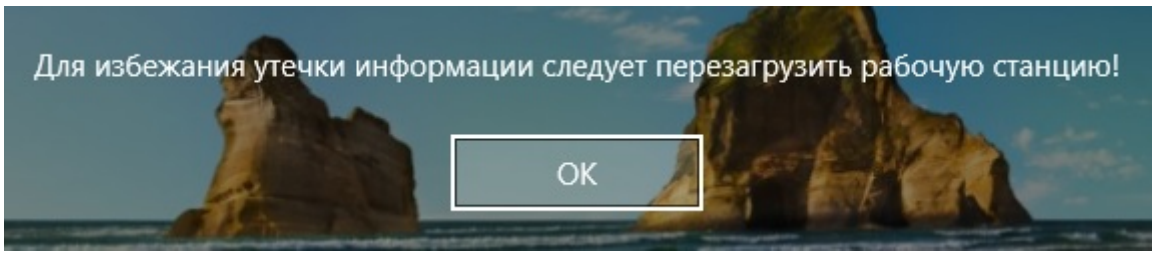


Рисунок 6.20 – Ошибка входа пользователя в ОС

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 3» 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.

Например, в ОС Windows 7 у приложения MS Word, из пакета Microsoft Office, такими файлами являются:
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) В консоли администрирования СЗИ включить механизм ***Мягкий режим*** (подробнее см. пункт 6.2.4 «Механизм мягкого режима» настоящего документа).

2) На 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 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***:

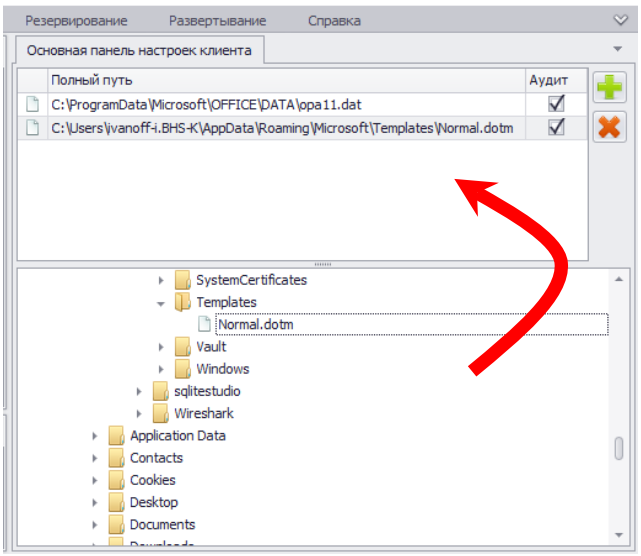


Рисунок 6.21 – Выбор файлов для монопольного доступа

7) В **Основной панели настроек клиентов** добавить ресурсы на контроль одним из перечисленных ниже способов:

- захватить и перетащить мышью необходимые объекты из дерева ресурсов в область настроек (рис. 6.21);
- нажать кнопку ***Добавить***  , в открывшемся окне «**Выбор**» (см. пример на рис. 6.3) выделить нужный файл и нажать кнопку ***Добавить***.

8) Также можно настроить фиксацию событий доступа приложений к контролируемым объектам в журнал событий СЗИ «Блокхост-Сеть 3», отметив параметр ***Аудит***, расположенный справа от выбранного файла.

9) Выключить «**Мягкий режим**».

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

6.1.8 Разграничение доступа к администрированию СЗИ «Блокхост-Сеть 3»

Для разделения функциональных обязанностей администратор безопасности может санкционировать администрирование СЗИ назначенными пользователями в полном объеме (в серверной или локальной консолях). Для этого необходимо воспользоваться механизмом разграничения доступа к администрированию СЗИ «Блокхост-Сеть 3».

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 3»

Для предоставления доступа пользователей к администрированию СЗИ «Блокхост-Сеть 3» администратору безопасности необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка разграничения доступа пользователей к администрированию СЗИ.

2) В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Полномочия*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Полномочия***. В обоих случаях в ***Основной панели настроек клиентов*** откроются настройки выбранного механизма (рис. 6.22).

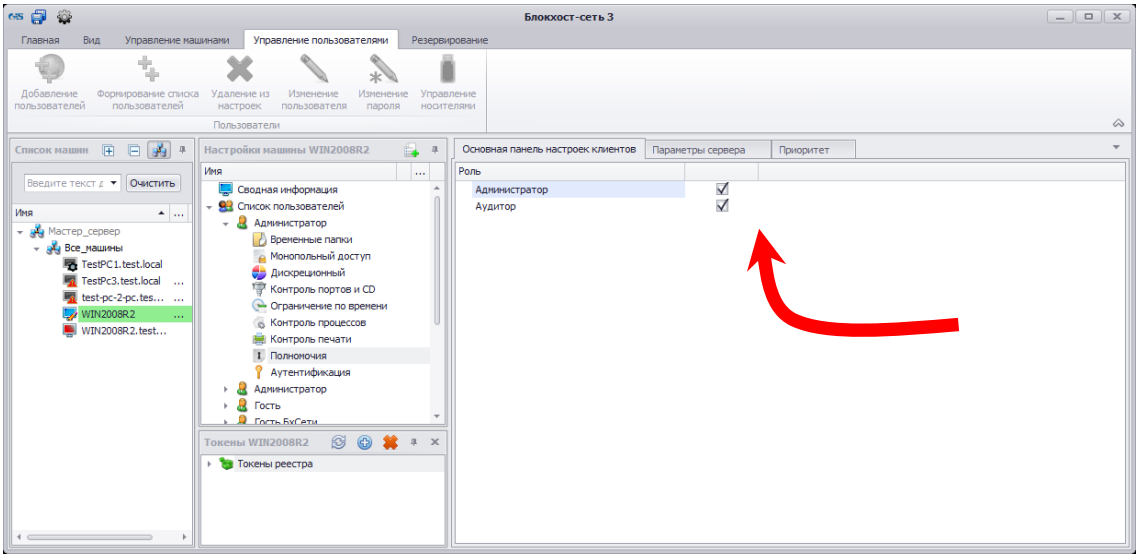


Рисунок 6.22 – Настройка полномочий администратора СЗИ

3) В **Основной панели настроек клиентов** установить параметр напротив необходимой роли.

4) Сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***

все, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

В зависимости от предоставляемых прав, пользователю могут быть присвоены роли:

- ***Администратора*** – предоставление пользователю прав администратора, полный доступ к функционалу СЗИ.
- ***Аудитора*** – предоставление пользователю прав аудитора. Пользователь имеет доступ только к просмотру настроек СЗИ, без внесения каких-либо изменений.

Права администратора предоставляются пользователю при установке флага ***Администратор*** или флагов ***Администратор*** и ***Аудитор.*** Права аудитора предоставляются пользователю при установке флага ***Аудитор.***

Распределение по ролям для ограничения полномочий пользователей подробно описано в подразделе 2.1 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

6.1.9 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 3».

Механизм контроля печати СЗИ «Блокхост-Сеть 3» поддерживает три режима работы:

1) **Режим базового аудита печати** – осуществляется регистрация событий 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 Полного аудита –** осуществляется регистрация всех событий печати.

3) **Режим аудита и разграничения доступа к приложениям** – осуществляется регистрация событий 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.

В СЗИ «Блокхост-Сеть 3» предусмотрена **маркировка** выводимых на печать конфиденциальных документов. Маркированные документы имеют специальный штамп в колонтитуле на страницах печатаемых документов. При маркировке происходит регистрация событий 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.

6.1.9.1 Режим базового аудита печати

6.1.9.1.1 Ограничения использования режима базового аудита печати

СЗИ «Блокхост-Сеть 3» при работе механизма контроля печати в режиме базового аудита печати имеет следующие ограничения: не ведется аудит событий печати на принтерах общего доступа (локальных принтерах рабочих станций, доступ к которым предоставлен пользователям сети).

6.1.9.1.2 Настройка СЗИ в режиме базового аудита печати

В настройках механизма контроля печати СЗИ «Блокхост-Сеть 3» 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»** консоли администрирования СЗИ, 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***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.23).

3) В **Основной панели настроек клиентов** включить механизм контроля печати, выбрав пункт ***Включить контроль печати*** и отметить параметр ***Только базовый аудит*** (рис. 6.23).

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.

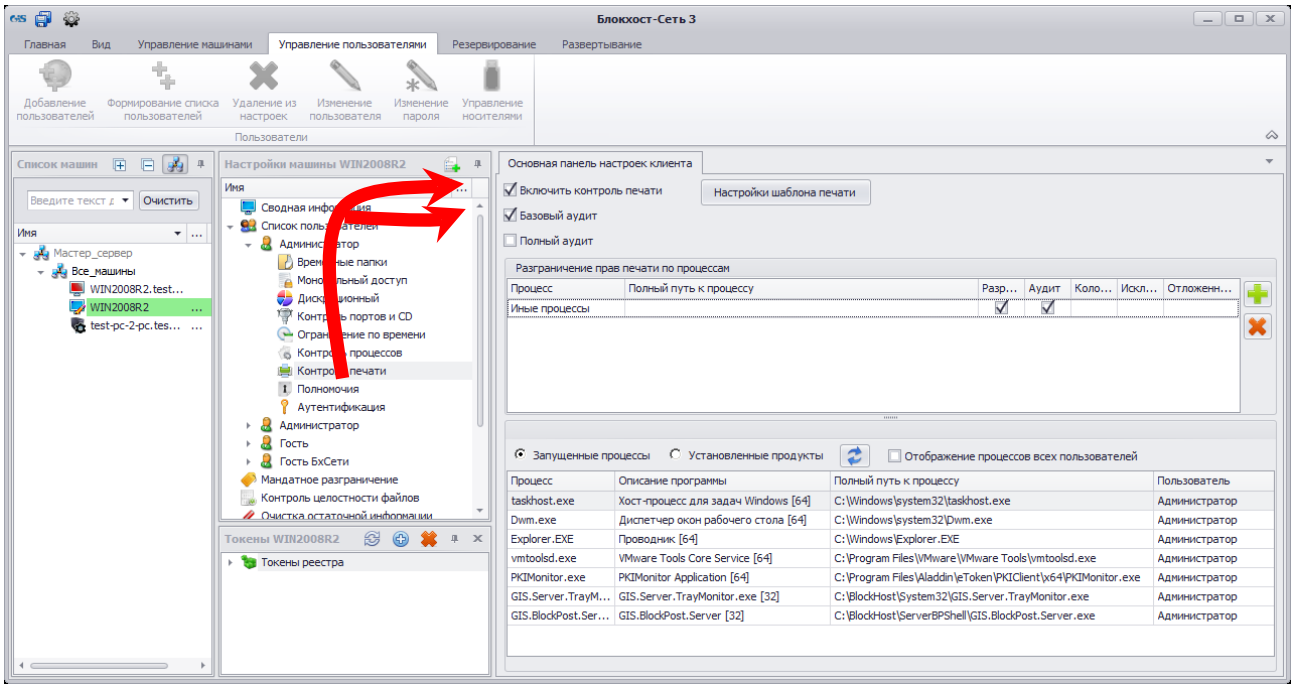


Рисунок 6.23 – Включение режима базового аудита печати

Для включения режима полного аудита необходимо выбрать параметр **Полный аудит** (рис. 6.23). В этом случае будут регистрироваться все события печати.

При включении параметра ***Только базовый аудит*** никакие настройки, кроме настройки шаблона печати, будут недоступны для редактирования (см. рис. 6.23). 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 6.1.9.2.2 настоящего документа.

6.1.9.1.3 Особенности работы СЗИ в режиме базового аудита печати

1) Если в окне **«Редактирование настроек шаблона печати»** (рис. 6.26) включены какие-либо опции, они будут применены ко всем распечатываемым документам из любых приложений (Подробнее о настройке механизма маркировки документов см. п. 6.1.9.3.2 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.

6.1.9.2 Режим аудита печати и разграничения доступа к приложениям

6.1.9.2.1 Ограничения использования режима аудита печати и разграничения доступа к приложениям

СЗИ «Блокхост-Сеть 3» 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 8.1 не поддерживается работа с приложениями, использующими metro-интерфейс.

6.1.9.2.2 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:

1) В окне **«Список машин»** консоли администрирования СЗИ, 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***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.23).

3) В **Основной панели настроек клиентов** включить механизм контроля печати, выбрав пункт ***Включить контроль печати*** (рис. 6.24).

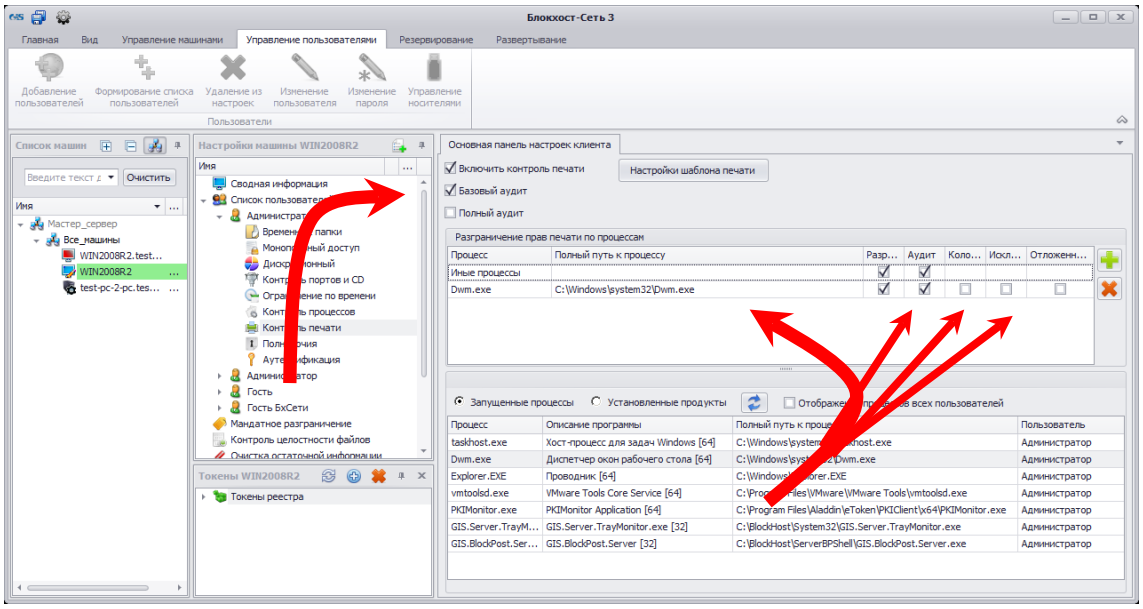


Рисунок 6.24 – Настройка механизма контроля печати

4) Добавить контролируемые процессы в область настроек одним из способов:

- захватить и перетащить мышью необходимые объекты из дерева ресурсов (с помощью клавиш <**Ctrl**> или <**Shift**> можно выделить несколько процессов) (рис. 6.24);
- нажать кнопку ***Добавить*** , и в открывшемся окне «**Выбор**» (см. пример на рис. 6.3) выбрать нужный процесс и нажать кнопку ***Добавить***.

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 ***Запущенные процессы↔Установленные продукты*** позволяет отображать в области *Запущенные процессы* либо список запущенных на рабочей станции процессов (переключатель установлен в положение ***Запущенные процессы***), либо список всех исполняемых файлов из перечня, установленного на рабочей станции ПО, которое поддерживается механизмом контроля печати (переключатель установлен в положение ***Установленные 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 ***Запущенные процессы↔Установленные продукты*** установлен в положение ***Запущенные процессы***). Для отображения списка всех запущенных процессов необходимо установить параметр ***Отображение процессов всех пользователей***.

5) 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.

6) Для сохранения событий печати из контролируемого приложения в журнал СЗИ «Блокхост-Сеть 3» необходимо в области *Разграничение прав печати по процессам* отметить поле ***Аудит***, расположенное справа от выбранного объекта (см. пример на рис. 6.24).

7) 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).

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

6.1.9.2.3 Особенности настройки СЗИ в режиме аудита печати и разграничения доступа к приложениям

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 на рабочей станции, с которой предоставляется общий доступ к принтеру (принт-сервере), СЗИ не установлено.

В остальных случаях распечатать документ на принтере общего доступа будет невозможно.

6.1.9.3 Режим маркировки документов при печати

При работе механизма контроля печати СЗИ в режиме маркировки документов осуществляются все функциональные возможности **Режима аудита и разграничения доступа к приложениям** (см. п. 6.1.9.2 настоящего документа), а также осуществляется

автоматическая маркировка каждого листа (страницы) документа при его печати.

6.1.9.3.1 Ограничения использования режима маркировки документов при печати

СЗИ «Блокхост-Сеть 3» 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. 6.1.9.2.1 настоящего документа);

2) печать цветного текста и/или изображения происходит в черно-белом варианте;

3) блокируется возможность печати из браузера Mozilla Firefox.

6.1.9.3.2 Настройка маркировки документов

В СЗИ «Блокхост-Сеть 3» 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 консоли администрирования СЗИ:

1) Последовательно выполнить пункты 1 – 6 пункта 6.1.9.2.2 настоящего документа.

2) Для отображения колонтитулов на документе, распечатываемом из контролируемого приложения, необходимо отметить поле ***Колонтитулы***, расположенное справа от выбранного приложения (см. рис. 6.24).

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**» следует выбрать необходимые маркеры (отметив соответствующие поля) и определить их содержание. Список маркеров и их описание указан ниже.

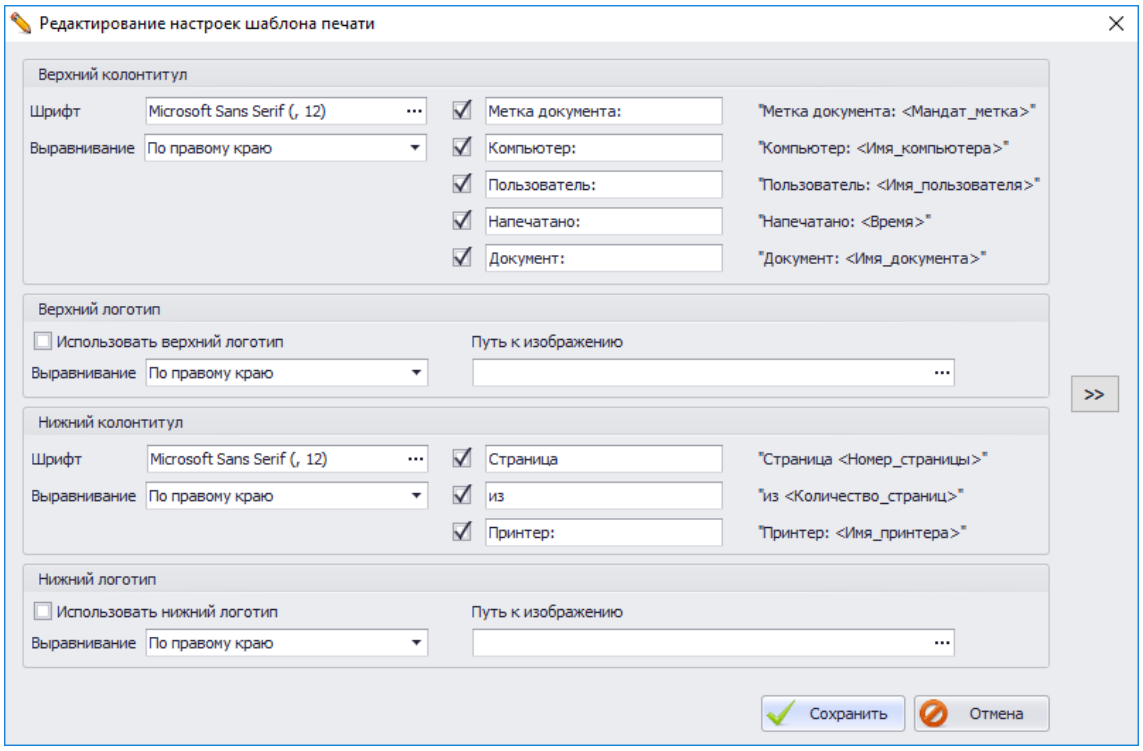


Рисунок 6.25 – Настройки шаблона печати

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. 6.26).

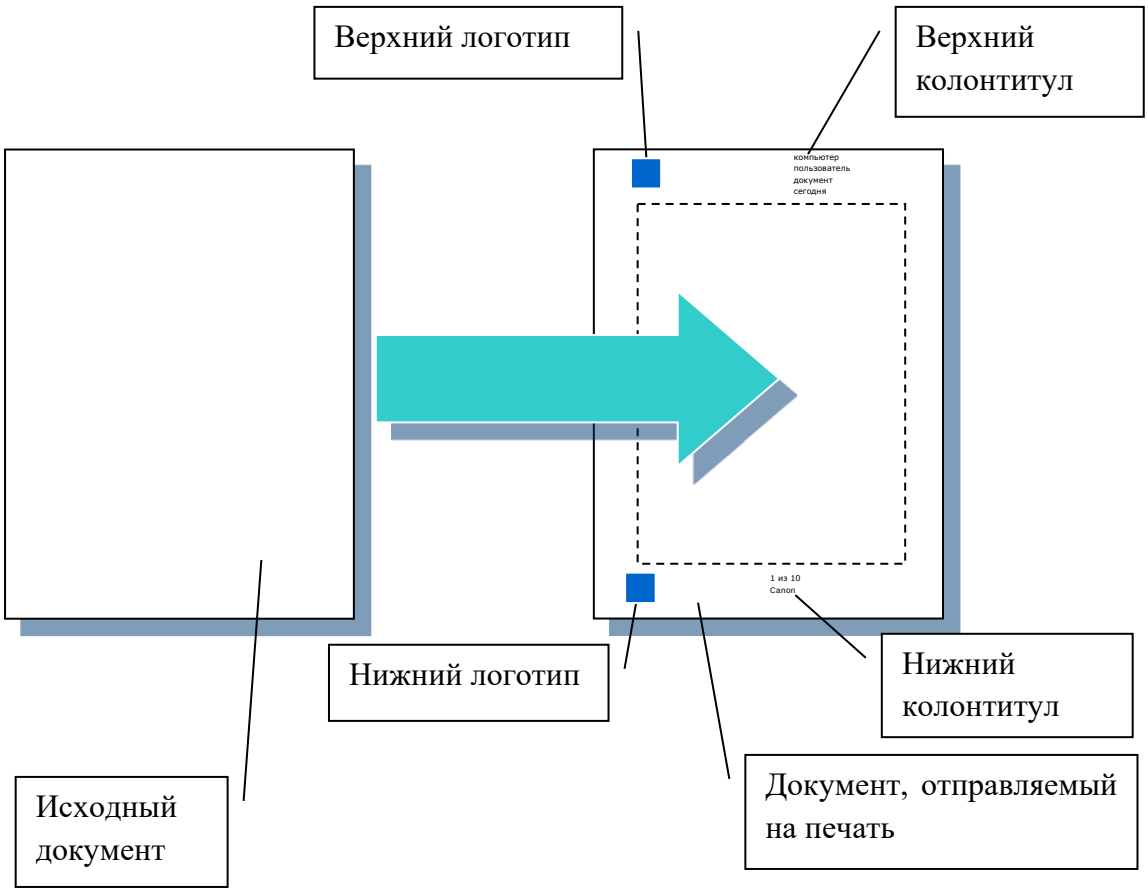


Рисунок 6.26 – Результат применения шаблона печати

Список маркеров шаблона печати и их описание:

1) **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”***.

2) **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 открывшемся окне **«Выбор»** (см. пример на рис. 6.3) 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***.

3) **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”***.

4) **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 открывшемся окне **«Выбор»** (см. пример на рис. 6.3) 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***.

Особенности настройки СЗИ в режиме маркировки документов при печати описаны в Приложении 3 к настоящему документу.

6.1.9.4 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.

6.1.9.4.1 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. 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.

Для включения отдельного режима обработки заданий на печать необходимо выполнить следующие действия в консоли администрирования СЗИ:

1) В настройках механизма контроля печати пользователя 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. 6.27).

3) При необходимости отметить параметры ***Аудит*** и ***Колонтитулы***.

4) Сохранить произведенные настройки механизма контроля печати выбрав пункт меню ***Главная→ Сохранить все,*** или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

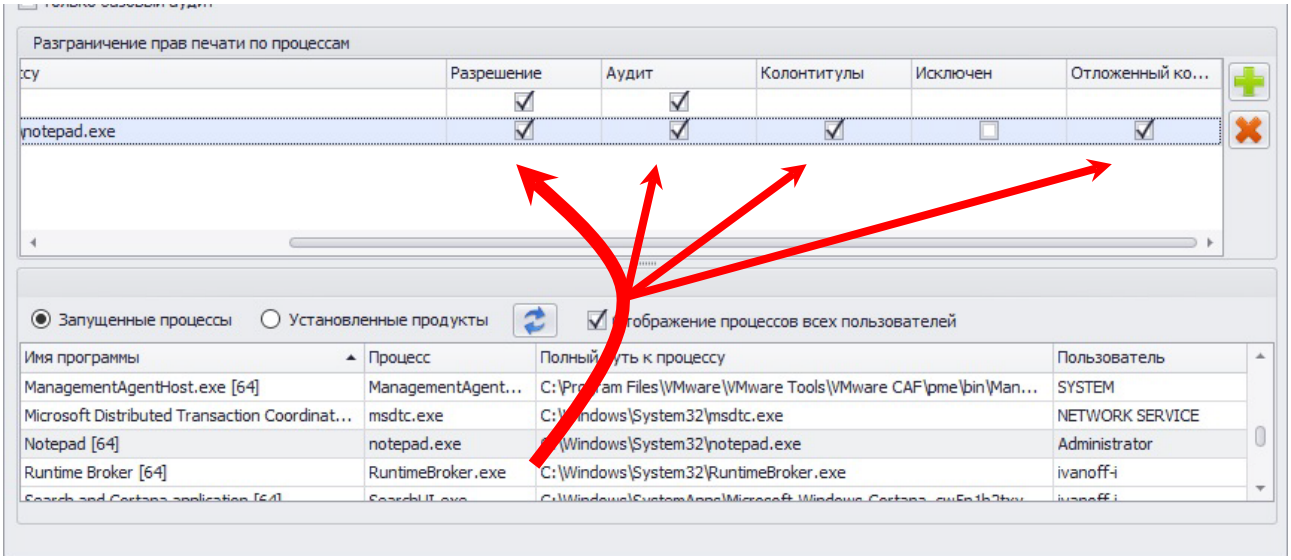


Рисунок 6.27 – Приложения с отдельным режимом обработки заданий на печать

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).

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. 6.28).

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.

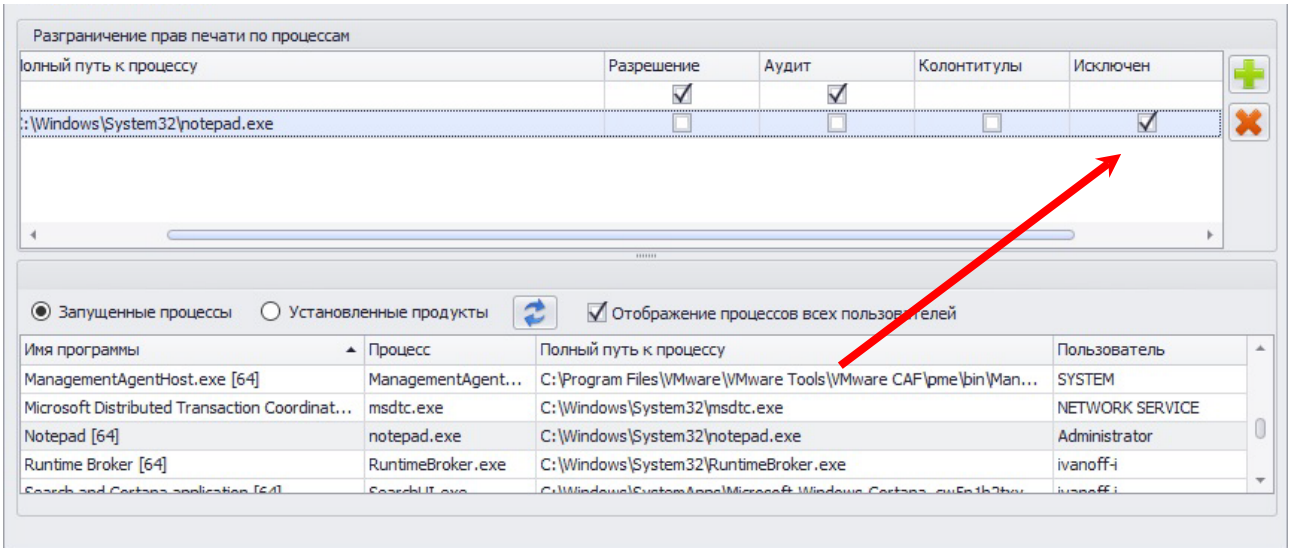


Рисунок 6.28 – Приложения, добавленные в исключения механизма контроля печати

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.

6.1.10 Репликация пользовательских механизмов разграничения доступа

В СЗИ «Блокхост-Сеть 3» существует возможность репликации (копирования) пользовательских механизмов разграничения доступа, настроенных для одного из пользователей, и на других пользователей, в том числе и на пользователей других рабочих станций (в серверной консоли администрирования СЗИ). Использование механизма копирования настроек СЗИ существенно облегчает задачу администратора безопасности по выполнению однотипных настроек пользовательских механизмов разграничения доступа для разных пользователей.

Для того, чтобы реплицировать настройки пользовательского механизма СЗИ администратору безопасности необходимо:

1) В окне «**Список машин**» консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, настройки пользовательского 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) 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.***

5) Выбрать пункт меню ***Главная→Вставить***. В результате у выбранных пользователей настройки скопированного механизма СЗИ будут идентичны.

6) При необходимости повторить операцию репликации выбранного механизма СЗИ и для других пользователей.

Для репликации следующего пользовательского механизма СЗИ следует повторно пройти шаги, описанные в п.п. 1 – 6.

6.2 Настройка механизмов защиты информации станции

Механизмы защиты информации станции являются механизмами, общими для всех пользователей на компьютере. В состав механизмов станции СЗИ входят: политика аутентификации, механизм мандатного разграничения доступа, механизм контроля целостности, механизм очистки памяти и механизм мягкого режима.

Произведенные настройки механизмов разграничения доступа станции 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 Политика аутентификации

Политика аутентификации СЗИ «Блокхост-Сеть 3» дополняет политики учетных записей пользователей, действующие в домене (в ОС Windows локальной рабочей станции), и параметры безопасности драйверов аппаратных идентификаторов, используемых в качестве персональных идентификаторов пользователей. Таким образом, параметры идентификации пользователя, для его корректного входа в ОС, должны удовлетворять всем политикам, действующим на рабочей станции.

Настройка параметров политики аутентификации пользователей в СЗИ заключается в установлении требований к:

- параметрам пароля пользователя;
- параметрам PIN-кода доступа к аппаратному идентификатору;
- параметрам блокировки пользователей при неудачных попытках авторизации в ОС Windows.

Для того чтобы перейти к настройке параметров политики аутентификации пользователей администратору безопасности следует:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию (или группу рабочих станций), для которой будет производиться настройка политики аутентификации.

2) В **Основной панели настроек клиентов** щелкнуть по названию ***Политика аутентификации*** или в окне «**Настройки машины**» выбрать пункт ***Политика аутентификации***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма (рис. 6.29).

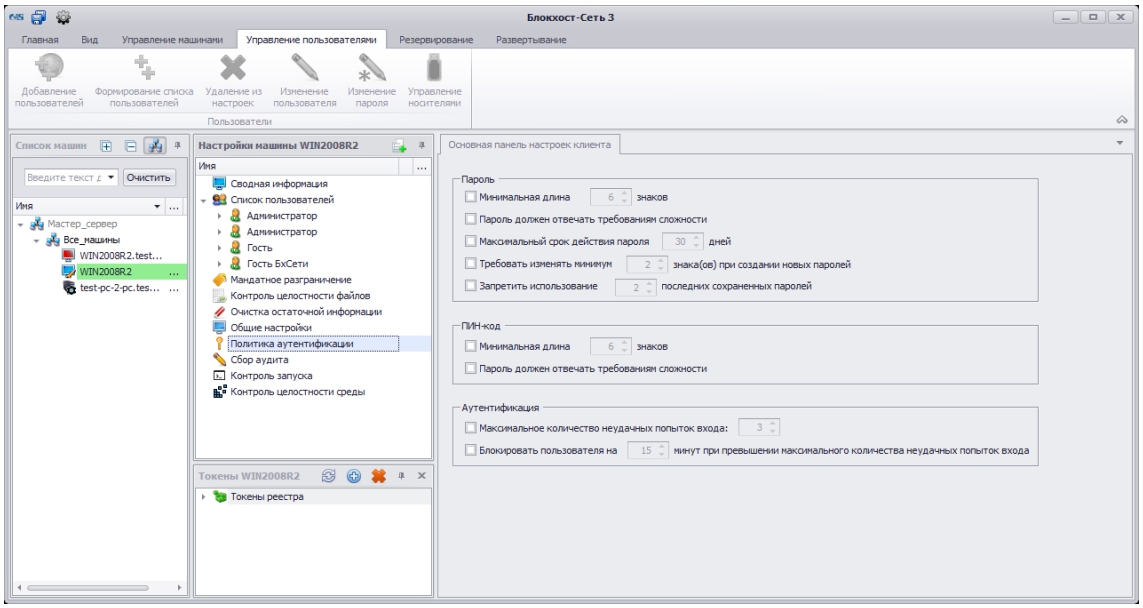


Рисунок 6.29 – Настройка политики аутентификации пользователей в СЗИ

3) В **Основной панели настроек клиентов** в области *Пароль* установить требуемые характеристики пароля пользователя (описание параметров приведено в табл. 6.3).

4) В **Основной панели настроек клиентов** в области *ПИН-код* установить требуемые характеристики PIN-кода доступа к аппаратному идентификатору, изменяемому средствами СЗИ (описание параметров приведено в табл. 6.3).

5) В **Основной панели настроек клиентов** в области *Аутентификация* установить требуемые параметры блокировки учетной записи пользователя при его неудачной авторизации в СЗИ (описание параметров приведено в табл. 6.3).

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

Таблица 6.3 – Параметры политики аутентификации пользователей

Наименование параметра	Описание	Возможные значения
Пароль		
Минимальная длина	Устанавливаются требования к минимальной длине пароля.	от 6 символов.
Пароль должен отвечать требованиям сложности	Установка требования к сложности пароля	Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы
Максимальный срок действия пароля	Устанавливается максимальное время действия пароля пользователя.	от 1 дня.
Требовать изменять знаки при создании новых паролей	Требование к изменению состава при создании нового пароля пользователя.	от 1 знака.
Запретить использование последних паролей	Устанавливается запрет на использование предыдущих паролей пользователя.	от 1 до 24 паролей
ПИН-код		
Минимальная длина	Устанавливаются требования к минимальной длине PIN-кода доступа к аппаратному идентификатору.	от 6 символов.
ПИН-код должен отвечать требованиям сложности	Установка требования к сложности PIN-кода	PIN-код должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы
Аутентификация		
Максимальное количество неудачных попыток входа	Устанавливается значение максимального количества неудачных попыток входа пользователя в ОС до его автоматической блокировки.	от 1 попытки.
Блокировать пользователя	Устанавливается время (в минутах) блокировки возможности входа пользователя в ОС рабочей станции после превышения им максимального количества неудачных попыток входа в ОС.	от 1 мин

Если при настройке параметров аутентификации рабочей станции были установлены параметры ***Минимальная длина пароля*** (***PIN-кода***), ***Пароль*** (***PIN-код***) ***должен отвечать требованиям сложности*** и ***Максимальный срок действия пароля***, а действующий пароль (PIN-код) нарушает установленные в СЗИ параметры, то при входе пользователя в ОС возникнет ошибка, после ознакомления с которой откроется диалог изменения пароля (PIN-кода).

В случае, если при загрузке ОС произошла ошибка запуска какой-либо службы СЗИ, или произошла ошибка чтения установленных в СЗИ параметров политики аутентификации, для параметров политики аутентификации ***Максимальное количество неудачных попыток входа*** и ***Блокировать пользователя*** устанавливаются значения по умолчанию: **3** неудачные попытки аутентификации и блокировка пользователя на **15** минут.

6.2.2 Мандатное разграничение доступа

Настройка мандатного механизма разграничения доступа в СЗИ «Блокхост-Сеть 3» заключается в сопоставлении списка защищаемых ресурсов (объектов файловой системы) значениям созданных иерархических мандатных меток и неиерархических категорий.

Для того чтобы перейти к настройке мандатного механизма разграничения доступа АБ следует:

1) В окне **«Список машин»** консоли администрирования СЗИ, 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 *Мандатное разграничение* или в окне «Настройки машины» выбрать пункт *Мандатное разграничение*. В обоих случаях в Основной панели настроек клиентов откроются настройки выбранного механизма (рис. 6.30).

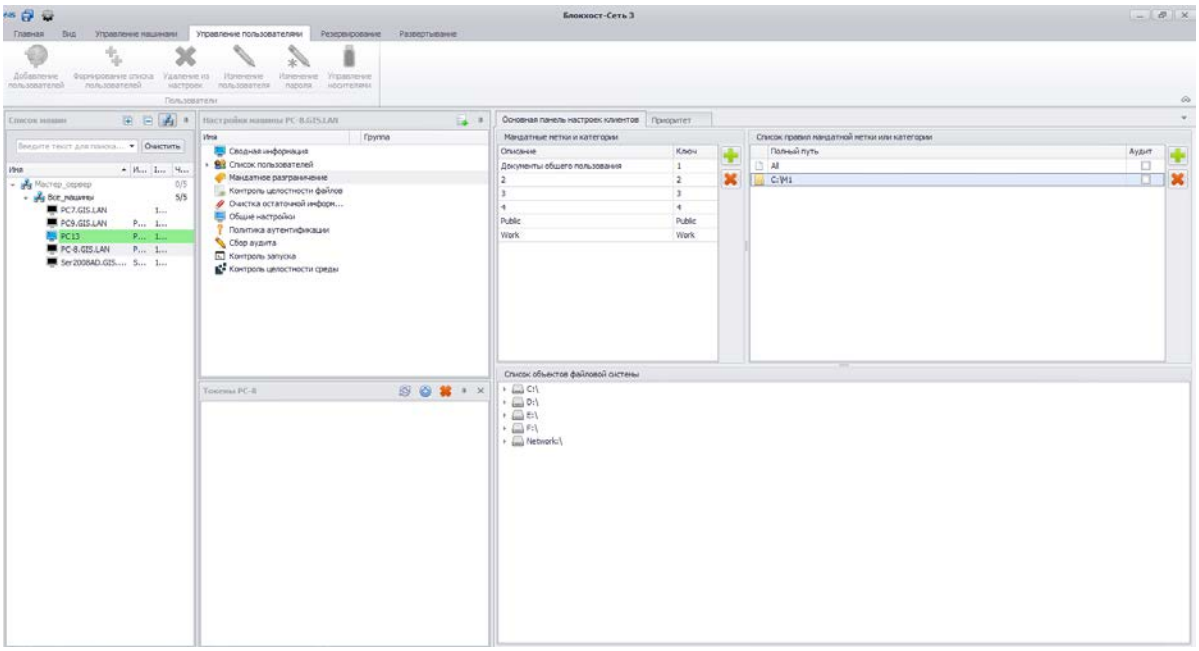


Рисунок 6.30 – Настройка мандатного механизма в консоли администрирования СЗИ

Все дальнейшие действия по созданию, изменению или удалению мандатных меток и категорий происходят во вкладке **Основная панель настроек клиентов** редактируемой

рабочей станции.

6.2.2.1 Создание иерархических мандатных меток

В процессе инсталляции СЗИ «Блокхост-Сеть 3» в настройках мандатного механизма 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 3» администратору безопасности необходимо:

1) В **Основной панели настроек клиентов** в области *Мандатные метки и категории* нажать кнопку ***Добавить***.

2) В открывшемся окне **«Добавление мандатной метки или категории»** (рис. 6.31) отметить параметр ***Метка*** и в соответствующих полях указать числовое значение (ключ) и описание мандатной метки.

При создании метки в поле ***Ключ*** возможен ввод только цифр. При вводе в поле ***Ключ*** числа, равного или больше 256 рядом с полем появится пиктограмма ошибки. В этом случае при наведении курсора на пиктограмму появится всплывающее описание ошибки – *Номер мандатной метки должен быть меньше 256*.

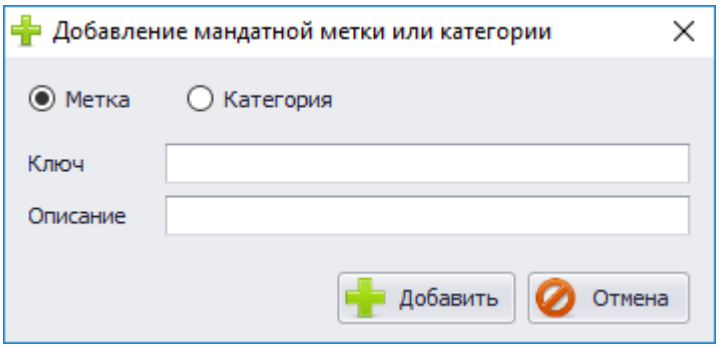


Рисунок 6.31 – Окно создания мандатной метки (категории)

3) В окне **«Добавление мандатной метки или категории»** нажать кнопку ***Добавить***. Добавленная метка отобразится в области *Мандатные метки и категории* (см. рис. 6.33). Нажатие кнопки ***Отмена*** в окне **«Добавление мандатной метки или категории»** 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 или категории»** появится пиктограмма ошибки, при наведении курсора на которую отобразится текст ошибки (на рис. 6.32 приведен пример создания иерархической мандатной метки с существующим номером).

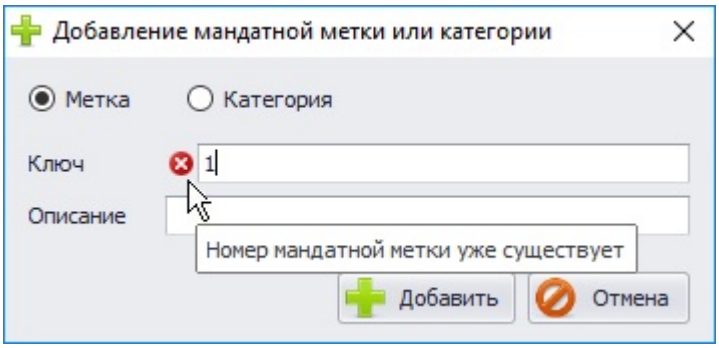


Рисунок 6.32 – Сообщение об ошибке создания мандатной метки

6.2.2.2 Создание неиерархических категорий

Для создания неиерархической категории в СЗИ «Блокхост-Сеть 3» администратору безопасности необходимо:

1) В **Основной панели настроек клиентов** в области *Мандатные метки и категории* нажать кнопку ***Добавить***.

2) В открывшемся окне **«Добавление мандатной метки или категории»** отметить параметр ***Категория*** и в соответствующих полях указать имя (ключ) и описание создаваемой категории.

3) В окне **«Добавление мандатной метки или категории»** нажать кнопку ***Добавить***. Добавленная категория отобразится в области *Мандатные метки и категории*. Нажатие кнопки ***Отмена*** в окне **«Добавление мандатной метки или категории»** позволит администратору выйти из окна без создания новой категории.

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

6.2.2.3 Сопоставление ресурсов меткам и категориям

По умолчанию в мандатном механизме СЗИ «Блокхост-Сеть 3» присутствует метка *Документы общего пользования* со значением ***1***, которой сопоставлен файловый объект (ресурс) ***All***. Объект ***All*** подразумевает под собой все логические и подключаемые съемные диски (USB-диски, флешки, CD-, DVD-приводы и т.п.) с расположенными на них объектами (файлами и каталогами), которые доступны пользователю при работе в операционной системе, но могут отсутствовать на рабочей станции в момент настройки администратором СЗИ мандатного механизма.

Уровень конфиденциальности (совокупность иерархической мандатной метки и

категорий), указанный для диска (каталога), автоматически распространяется и на вложенные в него объекты (файлы и каталоги). Для изменения уровня конфиденциальности вложенных объектов необходимо явно присвоить им необходимую иерархическую метку и категории.

В списке дерева ресурсов мандатного механизма СЗИ отсутствуют подключаемые USB-устройства, которые определяются ОС Windows как ***съемные устройства***. Файловым объектам таких устройств всегда будет соответствовать мандатная метка *Документы общего пользования* со значением ***1***.

Подключаемые USB-устройства, которые определяются ОС Windows как ***основной диск***, ***CD*** или ***DVD***, отображаются в списке дерева ресурсов мандатного механизма СЗИ. Уровень конфиденциальности файловых объектов таких устройств можно изменить.

Для определения классификационного уровня объектов файловой системы (сопоставления ресурсов контролируемой рабочей станции мандатным меткам и категориям) администратору безопасности необходимо выполнить следующие действия:

1) В **Основной панели настроек клиентов** в области *Мандатные метки и категории* выделить из списка мандатных меток (категорий) ту метку (категорию), 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 или категории* (рис. 6.33).

Для сопоставления файловых объектов выделенной мандатной метке (категории) можно также воспользоваться кнопкой ***Добавить***  , после нажатия на которую откроется окно **«Выбор»** (см. пример на рис. 6.3). В окне **«Выбор»** необходимо раскрыть структуру каталогов контролируемого компьютера, выбрать необходимый ресурс (файл или каталог) и нажать кнопку ***Добавить***.

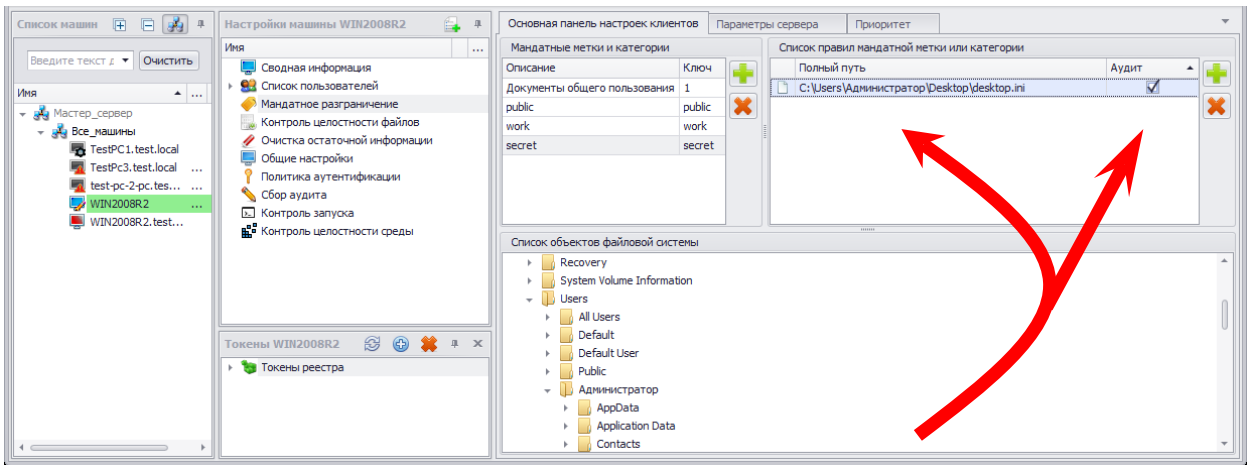


Рисунок 6.33 – Добавление ресурса

3) Для удаления ресурсов из списка сопоставленных метке (категории) достаточно выделить в области *Список правил мандатной метки или категории* 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 3». Для этого в области *Список правил мандатной метки* необходимо установить отметку в поле ***Аудит***, расположенное справа от выбранного объекта файловой системы (рис. 6.33).

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

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. 6.34). При необходимости переназначения мандатной метки (категории) такого ресурса следует нажать кнопку ***Да***. Нажатие кнопки ***Отмена*** в окне **«Добавление мандатного доступа»** оставит метку добавляемого файлового ресурса без изменений.

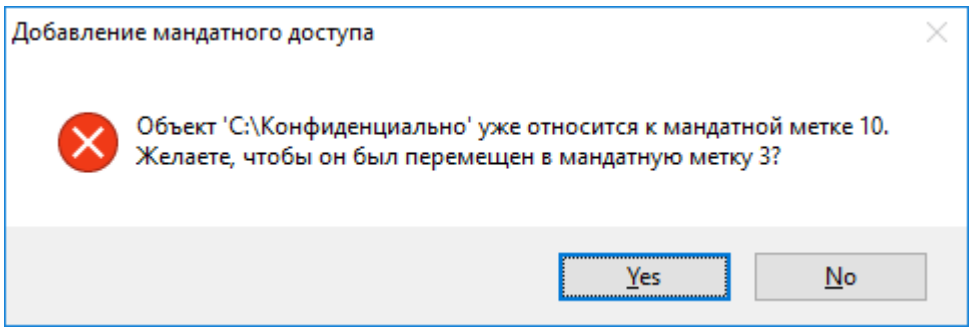


Рисунок 6.34 – Переназначение мандатной метки файлового ресурса

По умолчанию в СЗИ «Блокхост-Сеть 3» отсутствуют неиерархические категории. При сопоставлении файловых ресурсов, созданным на рабочей станции неиерархическим категориям, один и тот же файловый ресурс можно отнести сразу к нескольким категориям.

Особенности работы с жесткими и символьными ссылками при настройке мандатного механизма разграничения доступа описаны в Приложении 2 к настоящему документу.

6.2.2.4 Разграничение доступа субъектов к объектам через помеченный канал связи

СЗИ «Блокхост-Сеть 3» позволяет при помощи мандатного механизма установить

разграничение доступа между защищаемым объектом, помеченным каналом связи и субъектом доступа.

Назначение мандатной метки/категории каналу связи (сетевой карте) осуществляется аналогично сопоставлению мандатных меток/категорий объектам файловой системы и описано в п.6.2.2.3. При этом канал связи в качестве объекта доступа может быть сопоставлен только одной мандатной метке и нескольким категориям.

Разграничение доступа субъектов к объектам через помеченный канал связи можно представить, как последовательность действий сетевого взаимодействия, при выполнении которой субъект (пользователь) обращается к защищаемому объекту (файлу, директории) по каналу связи.

СЗИ «Блокхост-Сеть 3» разрешает операции вывода (ввода) защищаемого объекта при условии:

- равенства мандатных меток субъекта и объекта меткам канала связи;
- превосходства мандатных меток канала связи над метками субъекта и объекта.

СЗИ «Блокхост-Сеть 3» запрещает операции вывода (ввода) защищаемого объекта при условии:

- превосходства мандатных меток субъекта и объекта над метками канала связи.

Разграничение доступа субъектов к объектам через помеченный канал связи представлено в таблице 6.4.

Таблица 6.4 – Соотношение доступа субъекта к объекту через помеченный канал связи

Операции вывода (ввода) защищаемого объекта	**Соотношение доступа субъекта (МС) к объекту (МО) через помеченный канал связи (МК)**
Запрещены	**МС, МО > МК**
Разрешены	**МК > МО, МС**
Разрешены	**МС = МО = МК**

6.2.2.5 Изменение мандатных меток и категорий

Администратор безопасности может при необходимости изменять следующие параметры мандатной метки (категории): ее название (описание) и ключевое значение. Данные параметры изменяются без ущерба для списка сопоставленных метке (категории) ресурсов.

Для изменения параметров существующей мандатной метки (категории) администратор безопасности должен:

1) В **Основной панели настроек клиентов** в области *Мандатные метки и категории* щелкнуть два раза левой кнопкой мыши по имени той метки (категории), параметры которой будут изменяться.

2) В открывшемся окне **«Изменение мандатной метки или категории»** (рис. 6.35) изменить требуемые параметры мандатной метки (категории):

- ключевое значение мандатной метки (категории) – поле ***Ключ***;
- название метки (категории) – поле ***Описание***.

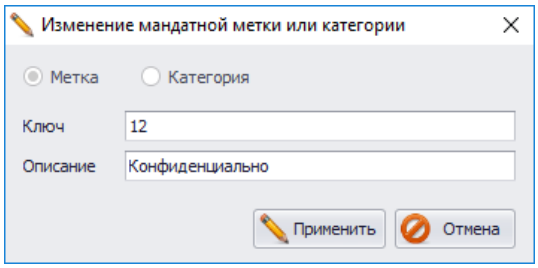


Рисунок 6.35 – Диалоговое окно изменения мандатной метки

3) После корректировки параметров мандатной метки (категории), для присвоения ей новых значений необходимо нажать кнопку ***Применить***. Список объектов, ранее сопоставленных данной метке (категории), останется без изменений. Нажатие кнопки ***Отмена*** вместо кнопки ***Применить*** в окне **«Изменение мандатной метки или категории»** 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 (категории) позволяет существенно упростить процедуру корректировки классификационного уровня для группы объектов файловой системы. Администратору безопасности вместо удаления одной метки (категории), создания другой и сопоставления с ней группы объектов достаточно изменить ключевое значение выбранной метки (категории).

6.2.2.6 Удаление мандатных меток и категорий

Для удаления мандатной метки (категории) администратору безопасности необходимо:

1) В **Основной панели настроек клиентов** в разделе *Мандатные метки и категории* (рис. 6.33) выбрать необходимую мандатную метку (категорию) и нажать кнопку ***Удалить*** (либо воспользоваться клавишей **<Del>**). Выбранная мандатная метка (категория) 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 или категории (т.е. имеющие классификационный уровень, равный значению данной метки или категории), 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** и ему назначена неиерархическая категория, 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 классификационного уровня по умолчанию (мандатная метка равна **1**, отсутствует сопоставление с неиерархическими категориями), то классификационный уровень высвободившегося ресурса будет равен **1** (высвободившийся ресурс автоматически будет сопоставлен метке по умолчанию *Документы общего доступа* и не сопоставлен неиерархическим категориям).

Мандатную метку *Документы общего доступа* удалить нельзя. При попытке удаления этой метки откроется окно с сообщением об ошибке удаления метки со значением **1**.

6.2.3 Контроль целостности файлов

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 запуске СЗИ. Целостность поставленных на контроль файлов обеспечивается путем 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 СЗИ, при установленном параметре восстановления контролируемых файлов, файлы заменяются их исходными версиями из резервной папки.

Не рекомендуется ставить на контроль целостности файлы большого объема (>500 Mb) – при осуществлении периодической проверки вычисленных контрольных сумм файлов, в зависимости от используемого аппаратного обеспечения, возможно снижение производительности системы вплоть до некоторого «зависания» компьютера.

6.2.3.1 Настройка механизма контроля целостности файлов

Для настройки механизма контроля целостности администратор безопасности должен:

1) В окне **«Список машин»** консоли администрирования СЗИ, 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 файлов** (рис. 6.36).

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.

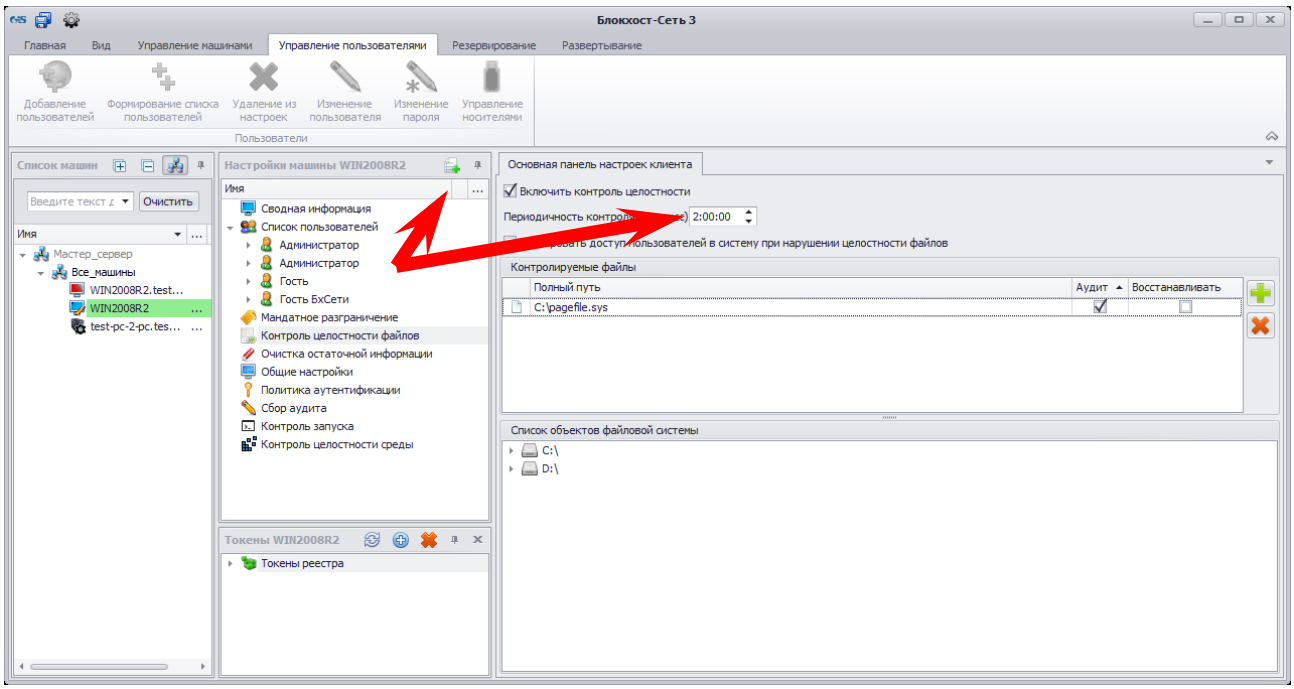


Рисунок 6.36 – Настройка механизма контроля целостности

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. 6.3). 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 3». Для этого в области *Контролируемые файлы* необходимо оставить отмеченным переключатель параметра ***Аудит***, расположенный справа от выбранного объекта:

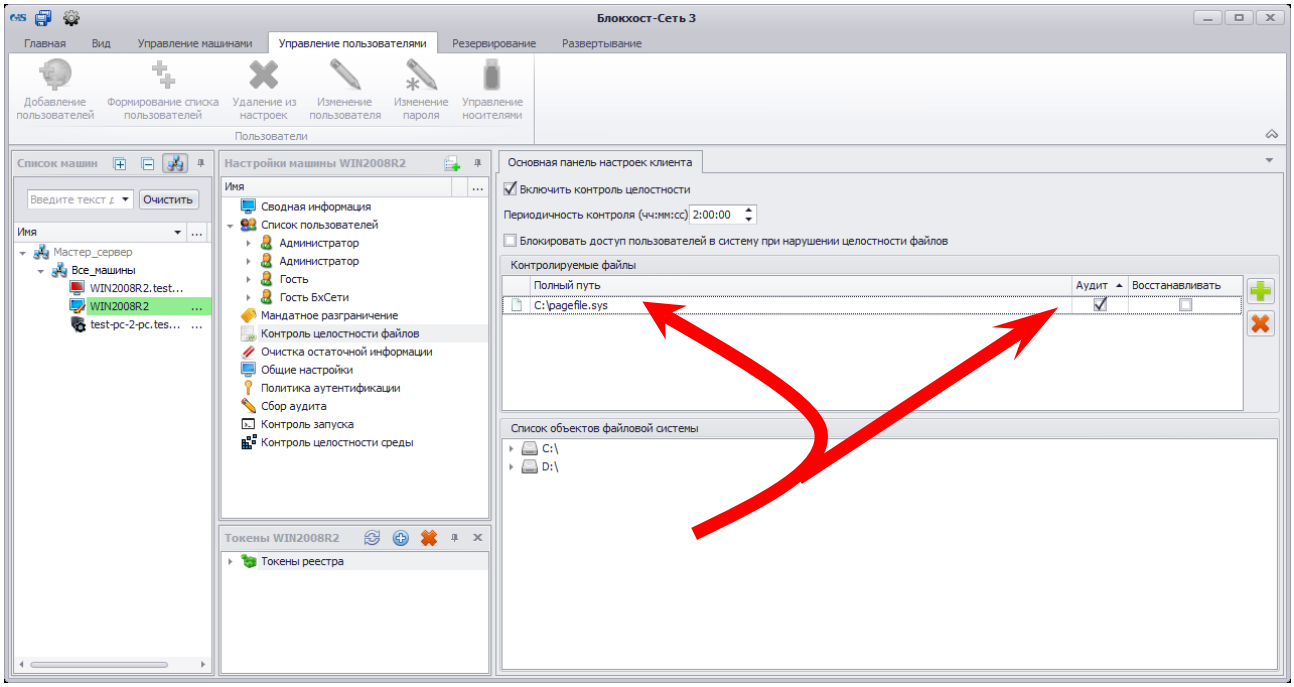


Рисунок 6.37 – Добавление ресурсов на контроль целостности

7) При необходимости администратор безопасности может разрешить восстановление измененных или удаленных файлов, которые были поставлены на контроль. Для этого в области *Контролируемые файлы* необходимо оставить отмеченным переключатель параметра ***Восстанавливать***, расположенный справа от выбранного объекта.

8) 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).

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

Измененные в СЗИ настройки механизма контроля целостности вступят в силу только после перезагрузки рабочей станции.

Следует иметь в виду, что в СЗИ «Блокхост-Сеть 3» 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>*.

6.2.4 Механизм очистки остаточной информации

Механизм очистки остаточной информации объединяет в себе механизм очистки памяти и механизм гарантированного удаления.

В СЗИ «Блокхост-Сеть 3» 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 3».

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.

Гарантированное удаление выполняется модулем диспетчера доступа СЗИ. При попытке удаления поставленного на контроль файла диспетчер доступа запрещает удаление средствами ОС и запускает механизм гарантированного удаления. Поставленные на контроль файлы удаляются путем трехкратного затирания их содержимого по специальному алгоритму, который исключает считывание остаточной информации на диске после удаления.

6.2.4.1 Настройка механизма очистки памяти

Для настройки механизма очистки памяти АБ необходимо осуществить следующие действия:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыть пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля целостности.

2) В **Основной панели настроек клиентов** щелкнуть по названию ***Очистка остаточной информации*** (рис. 6.38).

3) В **Основной панели настроек клиентов** включить механизм очистки памяти, отметив пункт **«Включить очистку памяти»** (рис. 6.38).

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. 6.38). 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. 6.3). В окне **«Выбор»** следует раскрыть структуру каталогов удаленного компьютера, выбрать необходимый исполняемый файл и нажать кнопку ***Добавить***.

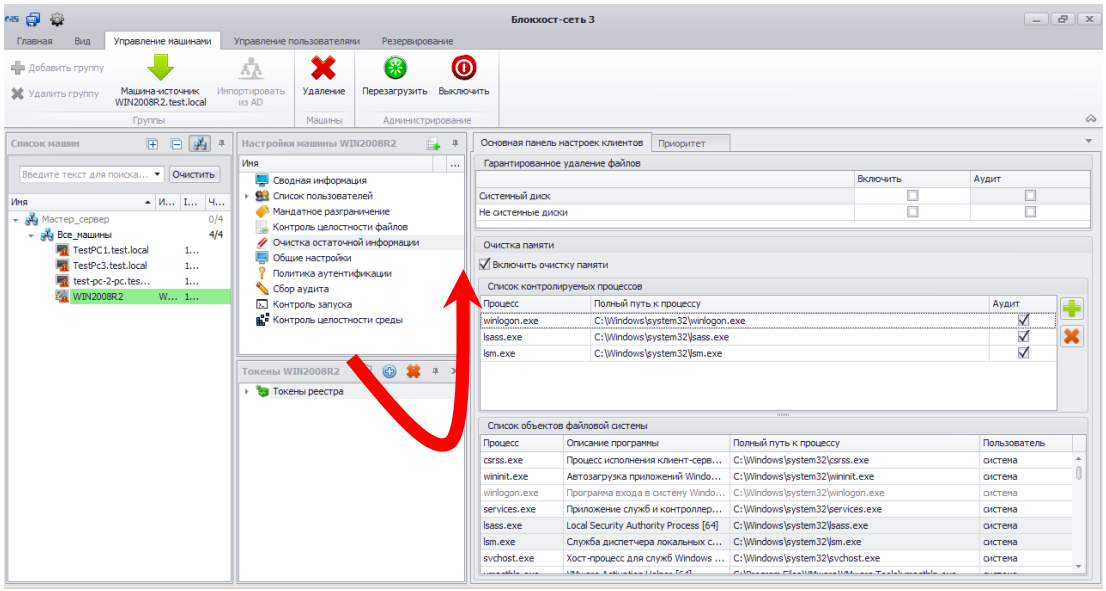


Рисунок 6.38 – Включение механизма очистки памяти

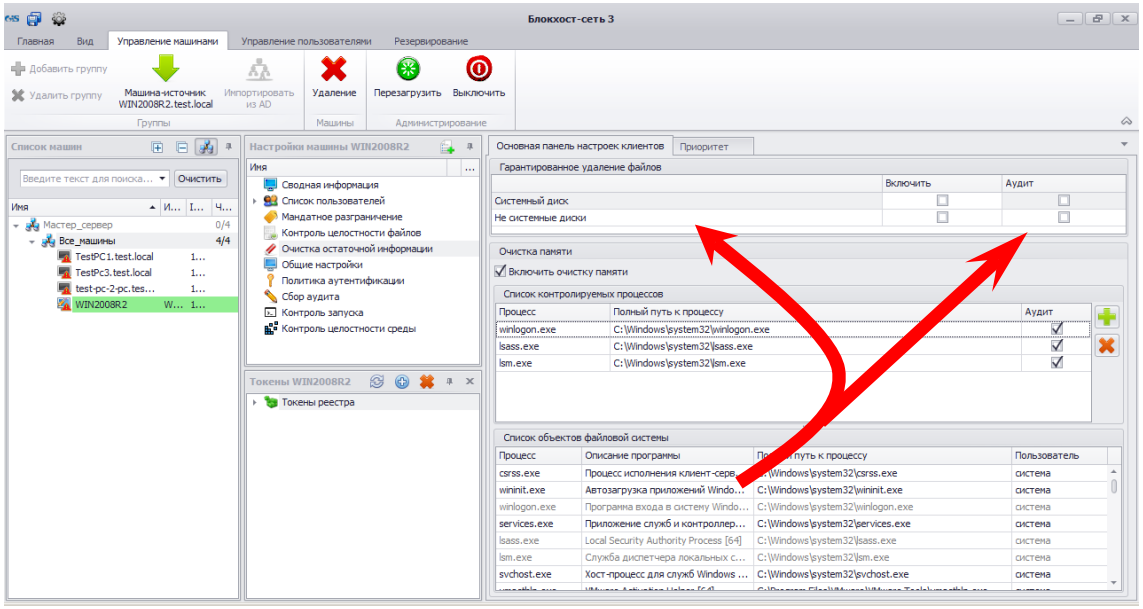


Рисунок 6.39 – Добавление ресурсов для механизма очистки памяти

5) При необходимости администратор безопасности может разрешить фиксацию событий, связанных с безопасностью информации, содержащейся в контролируемом

объекте, в журнал СЗИ «Блокхост-Сеть 3». 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 все***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

Измененные в СЗИ настройки механизма очистки памяти вступят в силу только после перезагрузки рабочей станции.

6.2.4.2 Настройка механизма гарантированного удаления файла

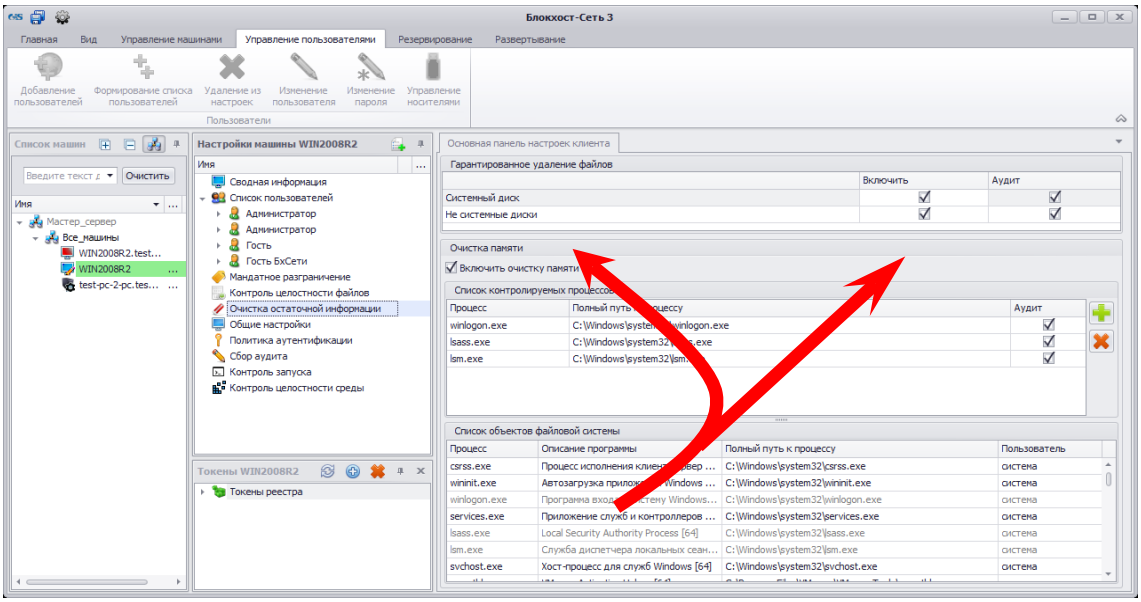
Для настройки механизма **гарантированного удаления,** администратору безопасности необходимо осуществить следующие действия:

1) В окне «Список машин» консоли администрирования СЗИ, раскрыть пункт **Все машины**, выбрать рабочую станцию, для которой будет производиться настройка механизма гарантированного удаления.

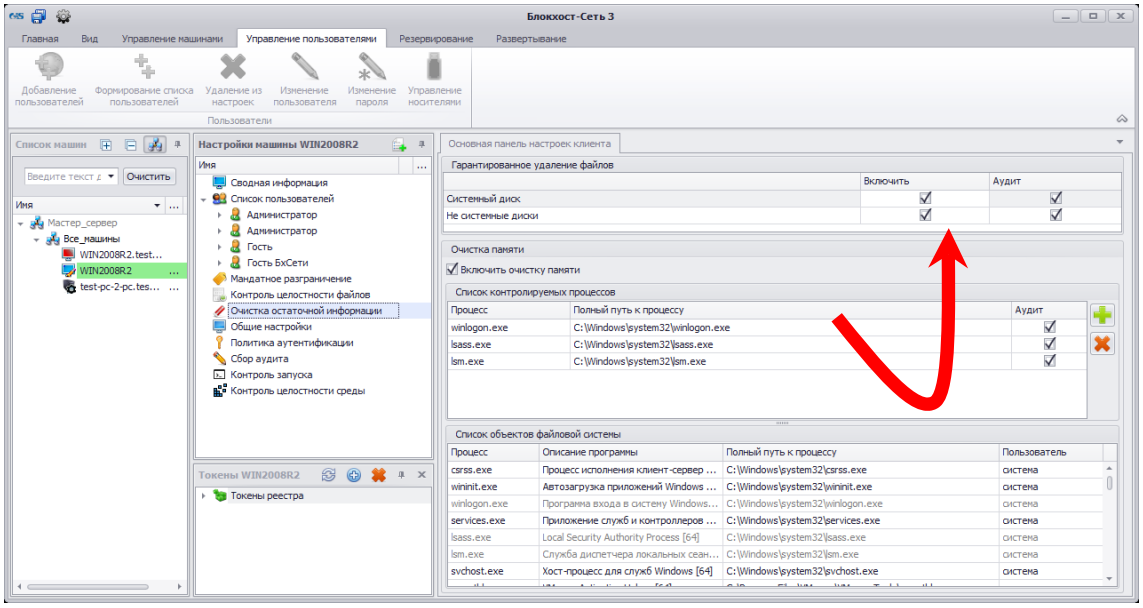
2) В Основной панели настроек клиентов щелкнуть по названию **Очистка остаточной информации**.

3) В Основной панели настроек клиентов включить механизм гарантированного удаления, отметив пункт «Включить» в области **Гарантированное удаление файлов** (рис. 6.40, а) напротив необходимого типа диска.

4) При необходимости регистрации событий гарантированного удаления файлов, необходимо отметить пункт **Аудит**, напротив необходимого типа диска (рис. 6.40, б).



а)



б)

Рисунок 6.40 – Включение механизма гарантированного удаления файлов.

6.2.5 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.

6.2.5.1 Порядок использования механизма мягкого режима

Для включения (отключения) механизма мягкого режима администратор безопасности должен выполнить следующие действия:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма мягкого режима.

2) В **Основной панели настроек клиентов** щелкнуть по названию ***Сводная информация*** или в окне «**Настройки машины**» выбрать пункт ***Общие настройки***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма.

3) В **Основной панели настроек клиентов** включить (отключить) механизм мягкого режима, выбрав пункт ***Мягкий режим*** (рис. 6.41).

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 3» при включенном механизме мягкого режима после входа пользователя в ОС приведена в таблице 6.5.

Таблица 6.5 – Работоспособность компонентов СЗИ «Блокхост-Сеть 3» при включенном механизме мягкого режима

Наименование компонента	Мягкий режим (обычный пользователь)
Дискреционный доступ	не активен
Контроль портов	не активен
Контроль процессов	не активен
Ограничения по времени	не активен
Контроль печати	не активен
Мандатное разграничение	не активен
Контроль целостности файлов	не активен
Очистка остаточной информации	не активен
Политика аутентификации	не активен

Наименование компонента	Мягкий режим (обычный пользователь)
Сбор аудит	активен
Контроль запуска	не активен
Контроль целостности среды	не активен

Необходимо обратить внимание, что при неактивных в мягком режиме компонентах СЗИ пользователи смогут получать доступ к защищаемым ресурсам, а при нарушении заданных правил разграничения доступа защищаемая информация может быть утрачена.

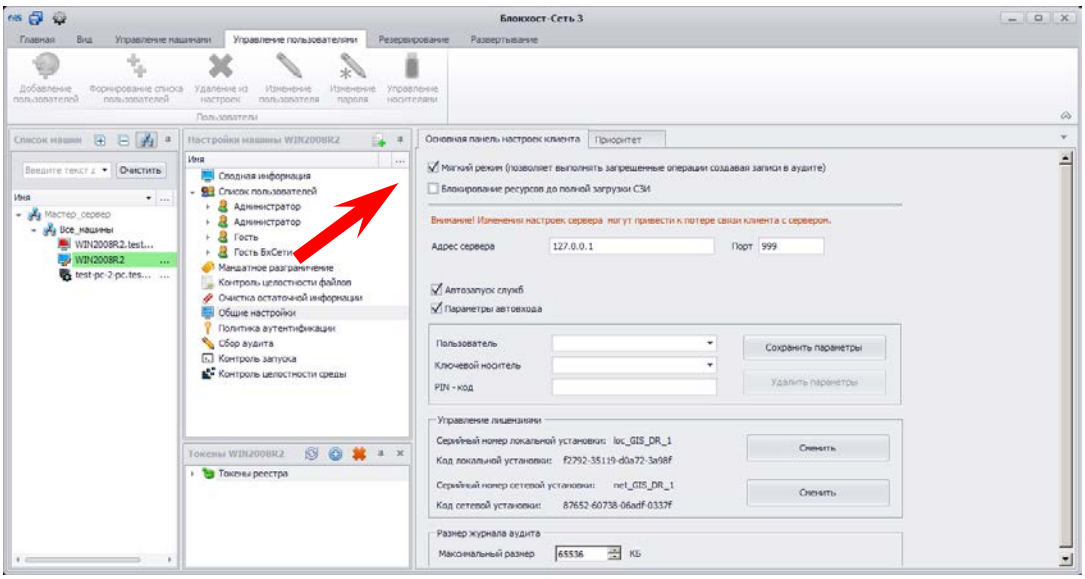


Рисунок 6.41 – Включение «Мягкого режима»

6.2.6 Механизм идентификаторов входа

Задача встроенного в 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 3».

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 локальной БД СЗИ каждой рабочей станции.

Администратор СЗИ имеет возможность редактировать любой носитель, даже если он не присвоен пользователям на данной рабочей станции, в специальном разделе, где будут отображаться пользователи, ассоциированные с данным идентификатором, и

рабочие станции, с которыми ассоциируется носитель.

В серверной консоли администрирования СЗИ отображение доступных идентификаторов входа осуществляется в окне **«Токены сервера»** или **«Токены <имя_рабочей_станции>»**. В окне **«Токены сервера»** отображаются персональные идентификаторы, подключенные к серверу СЗИ. Данное окно отображается, если в окне **«Список машин»** выделена какая-либо группа.

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.

В локальной консоли администрирования СЗИ, вне зависимости от того, что выделено в окне **«Список машин»**, всегда отображается окно **«Токены»**.

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 персональный 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 или окне **«Токены»** локальной 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***.

Если введен корректный PIN-код, то откроется вкладка **Настройки токена**. 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. 6.42). 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.

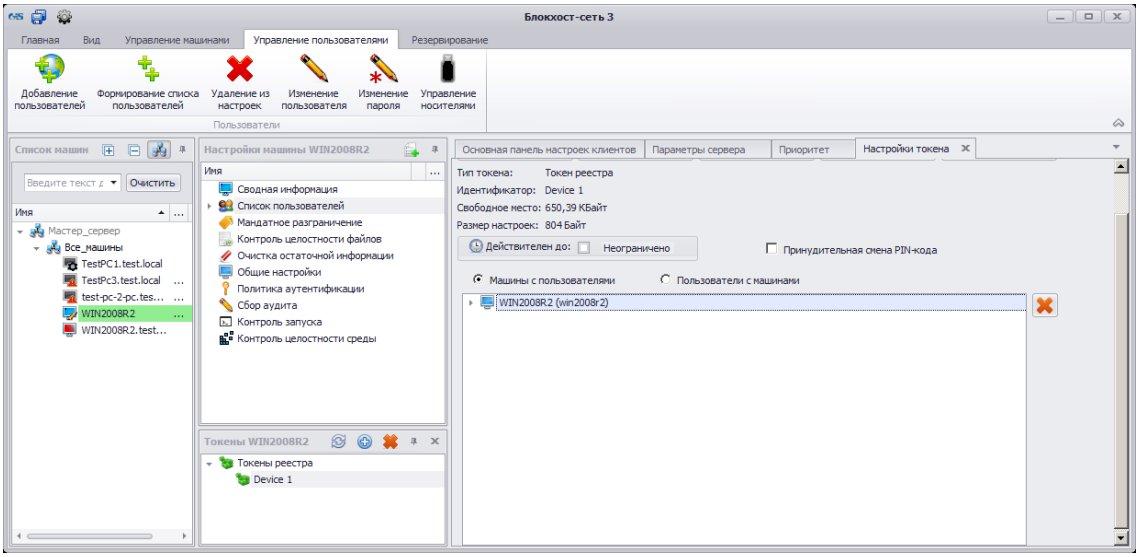


Рисунок 6.42 – Окно настроек идентификатора входа

6.2.6.1 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. 6.43) 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.

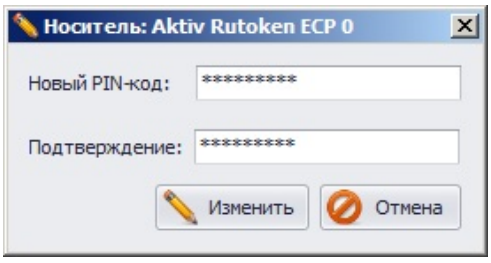


Рисунок 6.43 – Изменение PIN-кода ключевого носителя

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.

После смены PIN-кода доступа к редактируемому ключевому носителю из консоли

администрирования СЗИ администратор безопасности может указать требование смены PIN-кода доступа к этому токену пользователем при его первом использовании. Для этого следует отметить параметр ***Принудительная смена PIN-кода*** во вкладке **Настройки токена**.

6.2.6.2 Сохранение настроек СЗИ ключевого носителя в файл

Для сохранения настроек СЗИ ключевого носителя в файл администратору безопасности необходимо:

1) Во вкладке **Настройки токена** нажать кнопку ***Сохранить в файл***;

2) В открывшемся окне **«Сохранение настроек токена»** (рис. 6.44):

- ввести пароль, с применением которого будет зашифрован файл настроек СЗИ токена;
- нажать кнопку ***Выбор пути***, в открывшемся стандартном окне Windows **«Сохранить как»** выбрать каталог размещения и ввести имя файла, в котором будут сохранены настройки СЗИ редактируемого ключевого носителя;
- нажать кнопку ***Сохранить***.

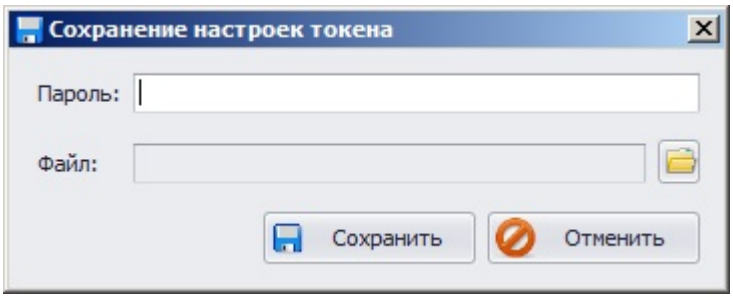


Рисунок 6.44 – Окно сохранения настроек ключевого носителя

В результате в выбранном каталоге будет сохранен файл с указанным именем, в котором в зашифрованном виде содержится информация о настройках СЗИ ключевого носителя.

Процедура сохранения настроек СЗИ ключевого носителя в файл может понадобиться, например, для резервирования настроек СЗИ ключевого носителя администратора безопасности. В случае неисправности действующего носителя администратора безопасности для его восстановления необходимо будет загрузить сохраненный файл настроек СЗИ этого ключевого носителя на новый носитель такого же типа.

6.2.6.3 Восстановление настроек СЗИ на ключевой носитель из файла

Для восстановления настроек СЗИ ключевого носителя администратору безопасности необходимо:

1) Во вкладке **Настройки токена** нажать кнопку ***Загрузить из файла***.

2) В открывшемся окне «**Восстановление настроек токена**» (рис. 6.45):

- ввести пароль, с применением которого был зашифрован файл настроек;
- указать каталог размещения и имя файла, в котором были зарезервированы настройки СЗИ ключевого носителя. Полный путь к файлу настроек СЗИ ключевого носителя можно ввести вручную в поле ***Файл*** или, воспользовавшись кнопкой ***Выбор пути***, указать необходимые данные в стандартном окне Windows **«Открыть»**;
- нажать кнопку ***Восстановить***.

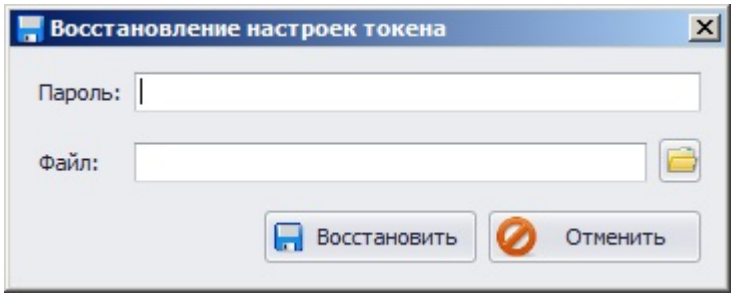


Рисунок 6.45 – Окно восстановления настроек ключевого носителя

В результате на ключевой носитель будут загружены настройки СЗИ, содержавшиеся на ключевом носителе, с которого они были скопированы в файл.

Возможность загрузки на ключевой носитель настроек СЗИ из файла существует только для ключевых носителей одного типа.

6.2.6.4 Инициализация ключевого носителя

Кнопка ***Инициализировать***, расположенная во вкладке **Настройки токена**, служит для очистки области памяти персонального идентификатора, в которой расположены настройки СЗИ «Блокхост-Сеть 3». 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 (флеш-накопителей, дискет и пр.) или закрытые ключи сертификатов) не удаляется. Также при операции инициализации из вкладки **Настройки токена** не изменяется PIN-код и имя ключевого носителя.

6.2.6.5 Ограничение времени действия ключевого носителя

Параметр ***Действителен до*** вкладки **Настройка токена** 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 6.48), который появляется после нажатия на кнопку раскрытия списка поля даты.

По умолчанию срок действия персонального идентификатора пользователя не ограничен.

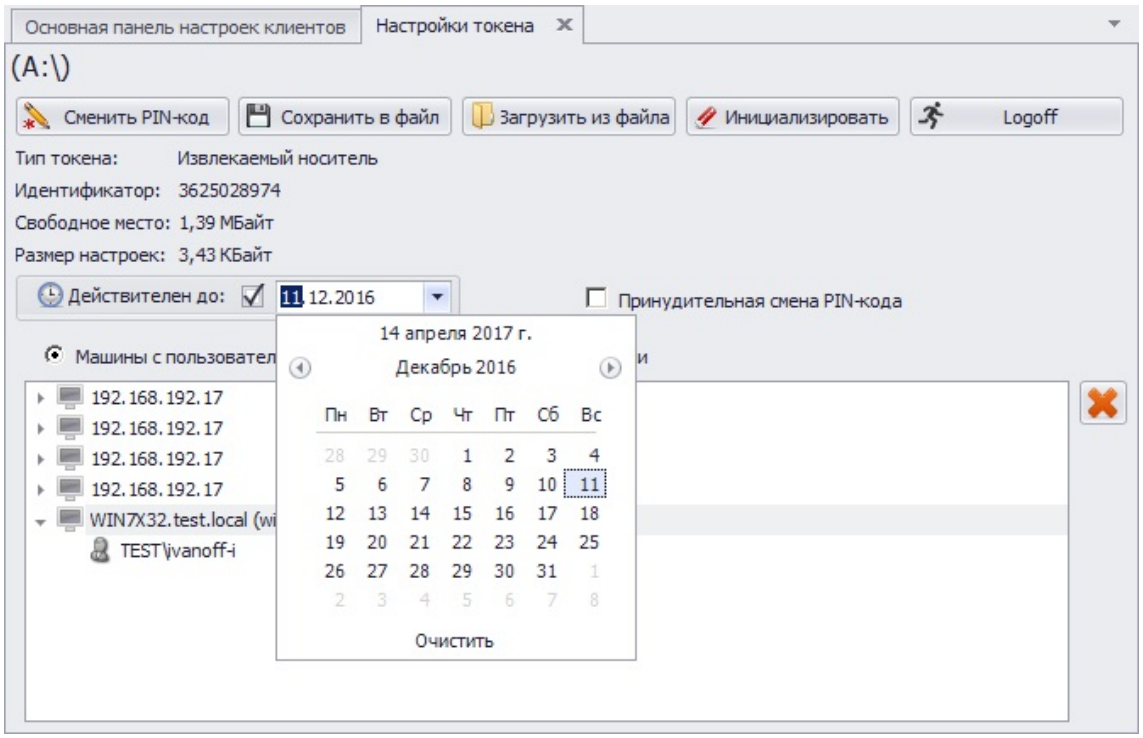


Рисунок 6.46 – Время жизни носителя

6.2.6.6 Редактирование списка пользователей, привязанных к ключевому носителю

Для удаления пользователя из списка привязанных к выбранному ключевому носителю необходимо во вкладке **Настройки токена** 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** 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. 6.49). Затем необходимо выбрать удаляемую рабочую станцию и нажать кнопку ***Отвязать***  , находящуюся справа от списка машин или воспользоваться клавишей **<DEL>**.

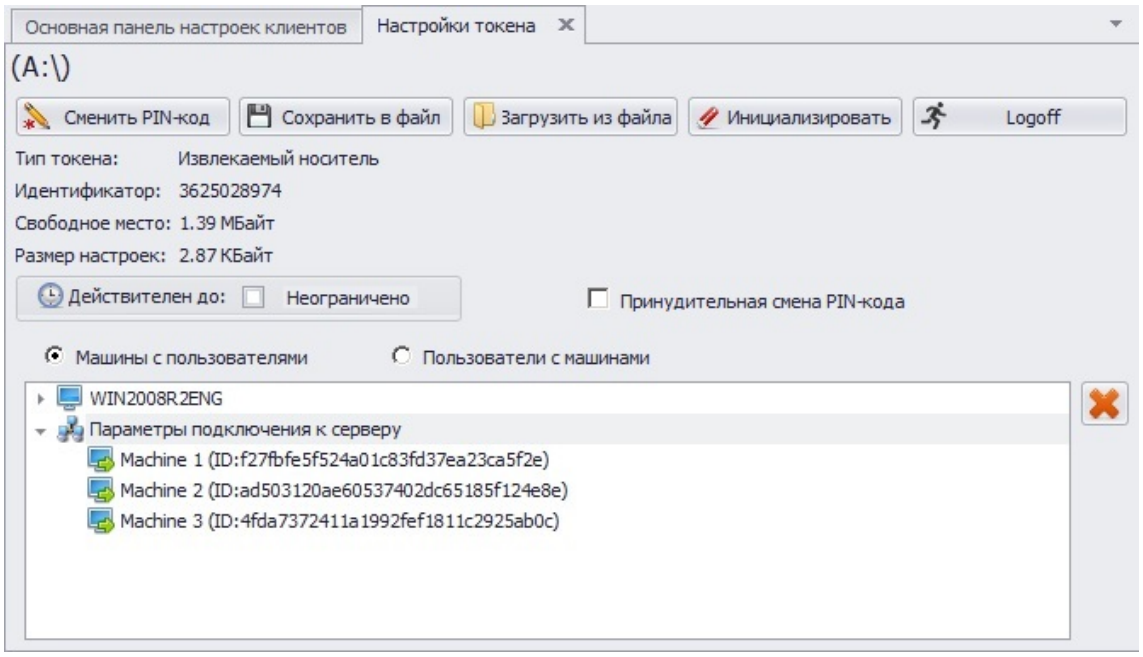


Рисунок 6.47 – Список сгенерированных на сервере СЗИ рабочих станций

6.2.6.7 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**» 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***:

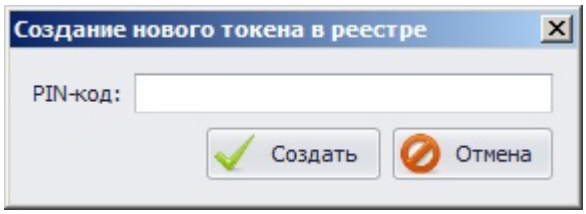


Рисунок 6.48 – Окно создания персонального идентификатора в реестре

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 <№>*:

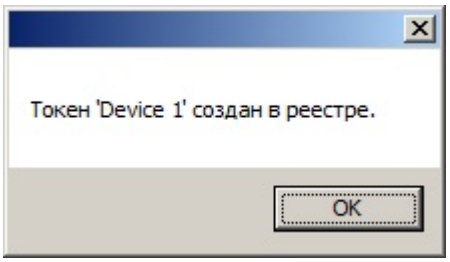


Рисунок 6.49 – Информационное окно об успешном создании идентификатора в реестре

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»**, 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.

6.2.6.8 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**» 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***:

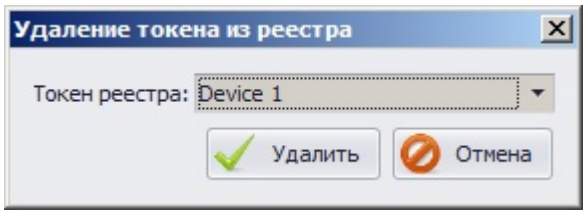


Рисунок 6.50 – Окно удаления персонального идентификатора в реестре ОС Windows

4) В результате из реестра редактируемой рабочей станции будет удален выбранный персональный идентификатор в реестре ОС Windows:

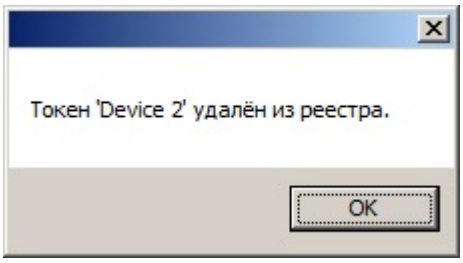


Рисунок 6.51 – Информационное окно об успешном удалении идентификатора из реестра

6.2.7 Блокировка сетевых ресурсов рабочей станции

В СЗИ «Блокхост-Сеть 3» реализована возможность блокировки сетевых ресурсов контролируемой рабочей станции до входа пользователей в ОС. 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 интерактивного входа в операционную систему авторизованного пользователя, администратору безопасности необходимо в 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. 6.52) или в окне **«Настройки машины»** выбрать пункт ***Параметры***. В обоих случаях в **Основной панели настроек клиентов** откроются параметры редактируемой рабочей станции (рис. 6.52).

3) В **Основной панели настроек клиентов** (рис. 6.52) отметить параметр ***Блокирование ресурсов до полной загрузки СЗИ***.

4) В **Основной панели настроек клиентов** (см. рис. 6.52) снять отметку параметра ***Автозапуск служб***.

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.

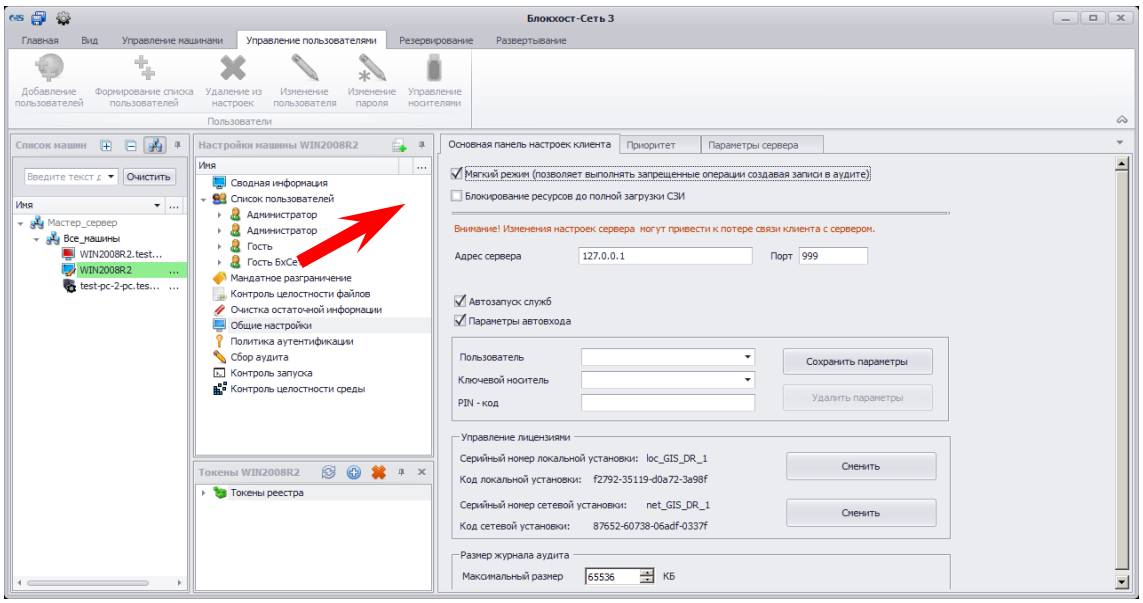


Рисунок 6.52 – Отображение вкладки «Параметры» контролируемой рабочей станции

Настройки блокировки сетевых ресурсов контролируемой рабочей станции до входа пользователей в ОС вступят в силу только после перезагрузки рабочей станции.

Доступ пользователей к сетевым ресурсам рабочей станции не блокируется, если был осуществлен интерактивный выход пользователя из ОС без ее перезагрузки.

6.2.8 Репликация механизмов защиты информации станции

В серверной консоли администрирования СЗИ «Блокхост-Сеть 3» существует возможность репликации (копирования путем замещения) механизмов защиты информации станции, настроенных на одной рабочей станции на другие, контролируемые на текущем сервере СЗИ. Использование репликации настроек защиты

информации станции позволит администратору безопасности существенно упростить процесс назначения однотипных политик на рабочие станции в сети.

Для того, чтобы реплицировать настройки механизмов станции СЗИ администратору безопасности необходимо:

1) В окне **«Список машин»** серверной консоли администрирования СЗИ, раскрыв пункт ***Все_машины***, выбрать рабочую станцию, настройки механизмов которой будут копироваться.

2) В окне «**Настройки машины**» выделить копируемый механизм (пункт ***Мандатное разграничение, Очистка памяти*** или ***Контроль целостности файлов***).

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 ***Сводная информация***.

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.

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

Для репликации следующего механизма СЗИ рабочей станции следует заново пройти шаги, описанные в п.п. 1 – 6.

Также в серверной консоли СЗИ «Блокхост-Сеть 3» можно скопировать установленные на одной из рабочих станций параметры использования ***Мягкого режима***, IP-адреса и номера портов Syslog-сервера и сервера СЗИ. Для копирования этих параметров администратору необходимо выполнить шаги, описанные выше для копирования механизмов станции СЗИ, но на втором шаге в окне **«Настройки машины»** выбрать пункт ***Параметры***.

Также из серверной консоли СЗИ «Блокхост-Сеть 3» можно синхронизировать настройки механизмов на рабочих станциях, входящих в одну группу на сервере СЗИ. Подробнее о таком способе репликации механизмов станции СЗИ см. п. 7.1 «Групповая репликация механизмов защиты информации станции» настоящего руководства.

6.2.9 Сбор аудита

Механизм регистрации событий и аудита предназначен для отслеживания событий и регистрации обращения к защищаемым ресурсам. а также при срабатывании всех механизмов защиты. Централизованный сбор и просмотр данных аудита, из настроенного АБ перечня, осуществляется в консоли системы развертывания и аудита Блокхост-Сеть.

Описание просмотра событий аудита приведено в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

Настройка сбора событий, собираемых с клиентских компьютеров и подчиненных серверов на родительский сервер, и отображаемых в консоли системы развертывания и аудита Блокхост-Сеть, осуществляется в консоли администрирования СЗИ.

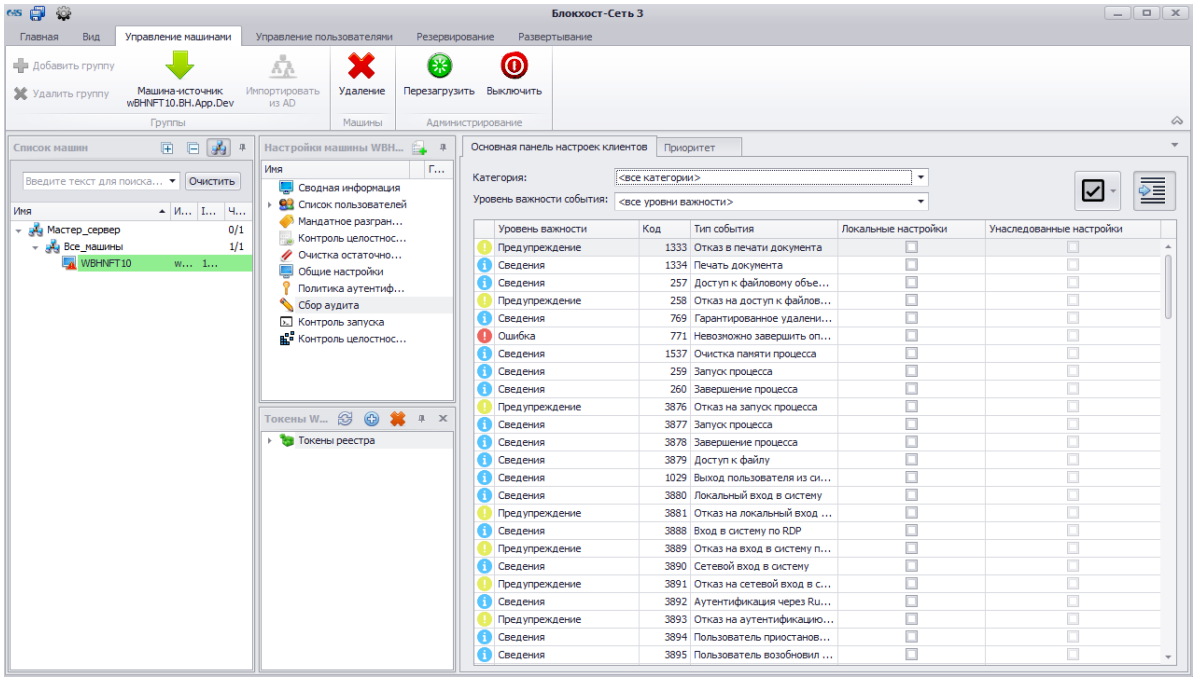


Рисунок 6.53 – Настройка сбора аудита

Для определения списка собираемых событий необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыть пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма сбора аудита (рисунок 6.53).

2) В **Основной панели настроек** машины выбрать ***Сбор аудита***.

3) В **Основной панели настроек клиентов** содержится полный список событий, регистрируемых на клиентах Блокхост-Сеть.

4) Для выбора собираемых событий необходимо для каждого, требуемого к сбору, события установить флаг ***Локальные настройки***. При этом все события с серверов и

клиентских компьютеров, подчиненных текущему серверу для которых установлен параметр ***Локальные настройки***, будут собираться локально на выбранном сервере.

В верхней части вкладки ***Основная панель настроек клиентов*** расположены кнопки:

- «  » - кнопка, позволяющая выделить все/сбросить все/сбросить к рекомендованным события в списке;
- «  » - кнопка, позволяющая объединять/разделять отображение в списке (в зависимости от вида) ***Локальных*** и ***Унаследованных настроек*** в ***Результирующие настройки***.
- кнопки выбора категории и уровня важности события, позволяющие отфильтровать список событий по заданному значению:
    - ***Категория*** - выборка событий, относящихся только к заданной категории (значение <все категории>, установленное по умолчанию, отфильтрует список событий по всем категориям).
    - ***Уровень важности события*** - выборка событий только с заданным уровнем важности (значение <все уровни важности>, установленное по умолчанию, отфильтрует список событий по всем уровням важности).

В параметре ***Унаследованные настройки*** отображаются все события, отобранные для сбора на головном/родительском сервере и наследуемые для выбранного сервера и всех подчиненных ему серверов. Параметр недоступен для редактирования.

6.2.10 Контроль запуска

В СЗИ «Блокхост-Сеть 3» реализован механизм, позволяющий администратору безопасности контролировать доступ к определённым типам файлов: аудио, видео и изображения, путем регистрации событий аудита.

Данный механизм позволяет осуществлять регистрацию событий аудита всех файлов, относящихся к типам аудио, видео и изображения, а также задавать аудит определенных типов файлов установкой маски имени исполняемого файла.

Для настройки механизма необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыть пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизм контроля запуска.

2) В **Основной панели настройки машины** щелкнуть по названию ***Контроль запуска*** (рис. 6.54).

3) В **Основной панели настроек клиентов** активировать напротив необходимого типа файла флаг **Аудит.**

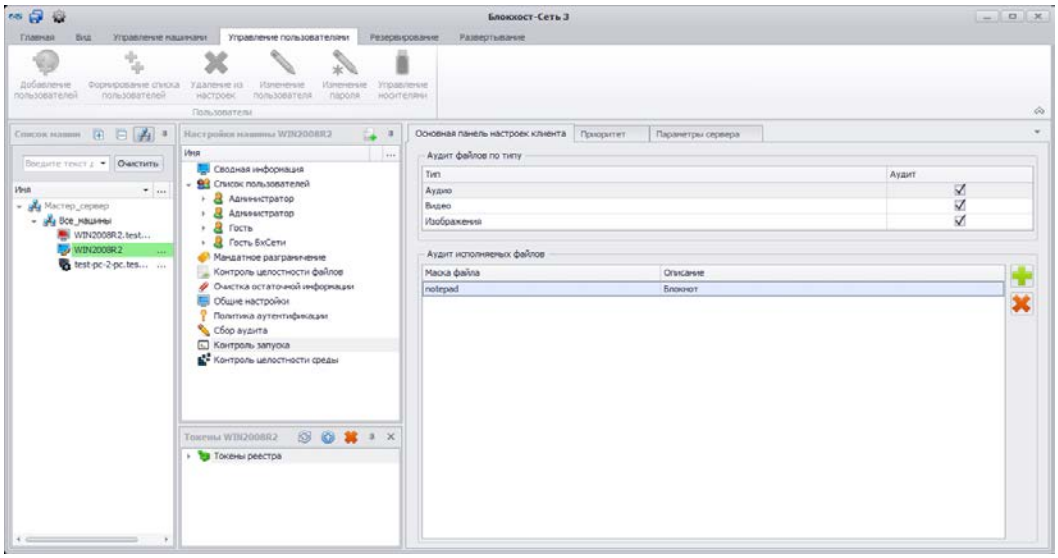


Рисунок 6.54 – Установка механизма контроля запуска

4) При необходимости установки маски файла, в области ***Аудит исполняемых файлов*** нажать на кнопку  , и в открывшемся окне (рис. 6.55) задать маску имени исполняемого файла и добавить его описание. После нажатия кнопки ***Добавить*** заданная маска появится в области аудита исполняемых файлов. При этом регистрация события аудита выбранного типа файла будет осуществляться только с учетом введенной маски.

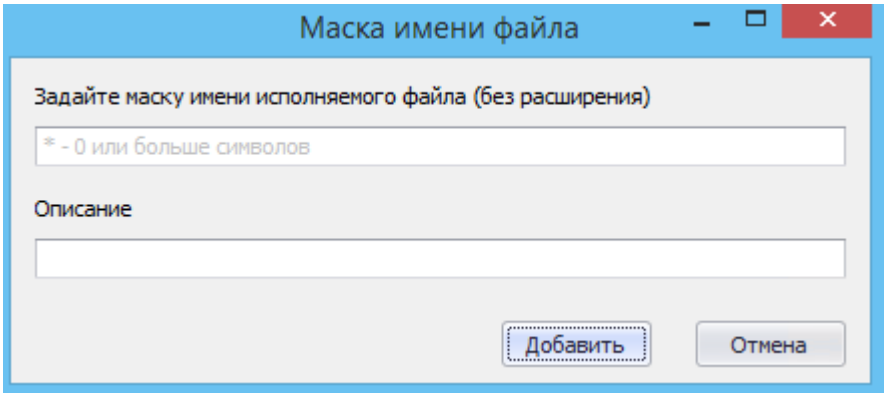


Рисунок 6.55 – Подтверждение добавления маски файла

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

6.2.11 Контроль целостности среды

Механизм контроля целостности среды предназначен для слежения за неизменностью контролируемых объектов с целью обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

Для настройки механизма контроля целостности среды необходимо:

1) В окне **«Список машин»** консоли администрирования СЗИ, раскрыть пункт ***Все_машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля целостности среды (рис. 6.56).

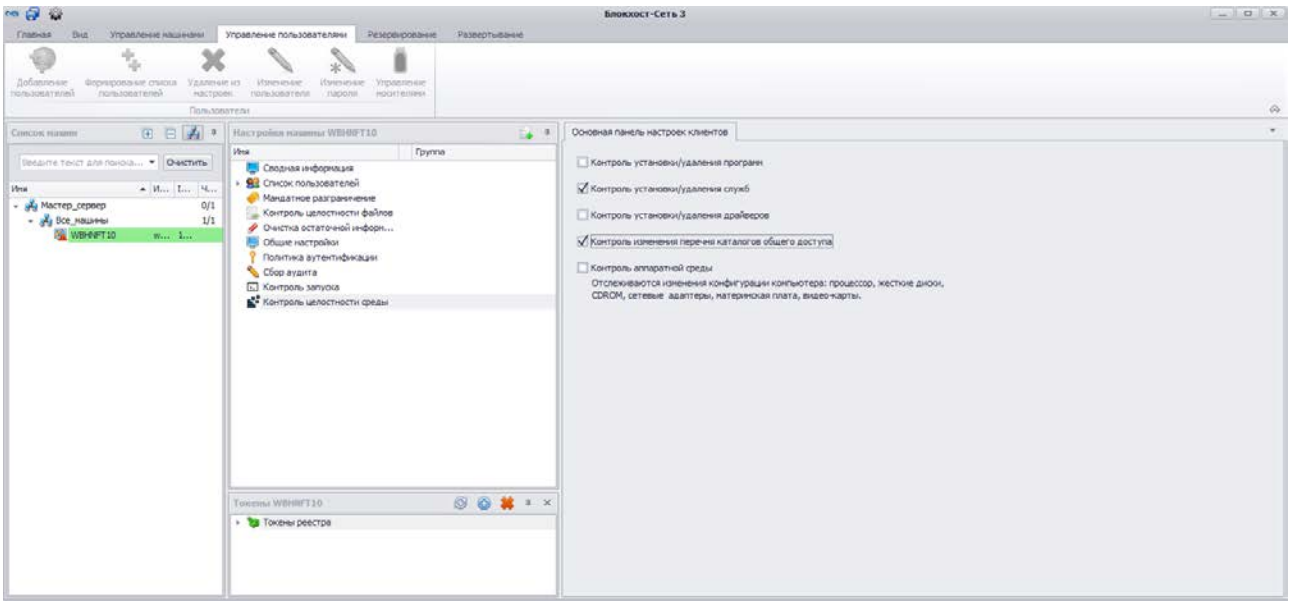


Рисунок 6.56 – Контроль целостности среды

2) В **Основной панели настроек машины** выбрать ***Контроль целостности среды.***

3) В **Основной панели настроек клиентов** (рис. 6.56) установить на контроль необходимые параметры:

- отслеживание изменений списка установленных программ;
- отслеживание изменений списка установленных служб/драйверов;
- отслеживание изменений перечня каталогов общего доступа;
- контроль аппаратной среды (отслеживает изменения конфигурации следующих устройств компьютера: процессор, жесткий диск, CDROM, сетевой адаптер. материнская плата, видеокарта).

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

7 Группирование рабочих станций

В серверной консоли администрирования СЗИ «Блокхост-Сеть 3» существует возможность группировки рабочих станций, подключенных к серверу СЗИ, по логическим группам (например, дирекция, бухгалтерия, группа проектирования и т.п.). Для рабочих станций, входящих в одну группу, можно установить единые настройки механизмов СЗИ (подробнее см. п. «7.1 Групповая настройка пользовательских механизмов защиты информации» и «7.2 Групповая настройка механизмов защиты информации станции» настоящего руководства).

Для активации меню создания групп администратору безопасности необходимо в окне **«Список машин»** серверной консоли администрирования СЗИ «Блокхост-Сеть 3» выделить группу ***Мастер_сервер*** и нажать кнопку ***Показывать группы***  , расположенную в заголовке окна. В результате, в пункте меню ***Управление машинами*** в разделе *Группы*: станет активным пункт ***Добавить группу***, а также в контекстном меню окна **«Список машин»** появятся пункты по работе с группами:

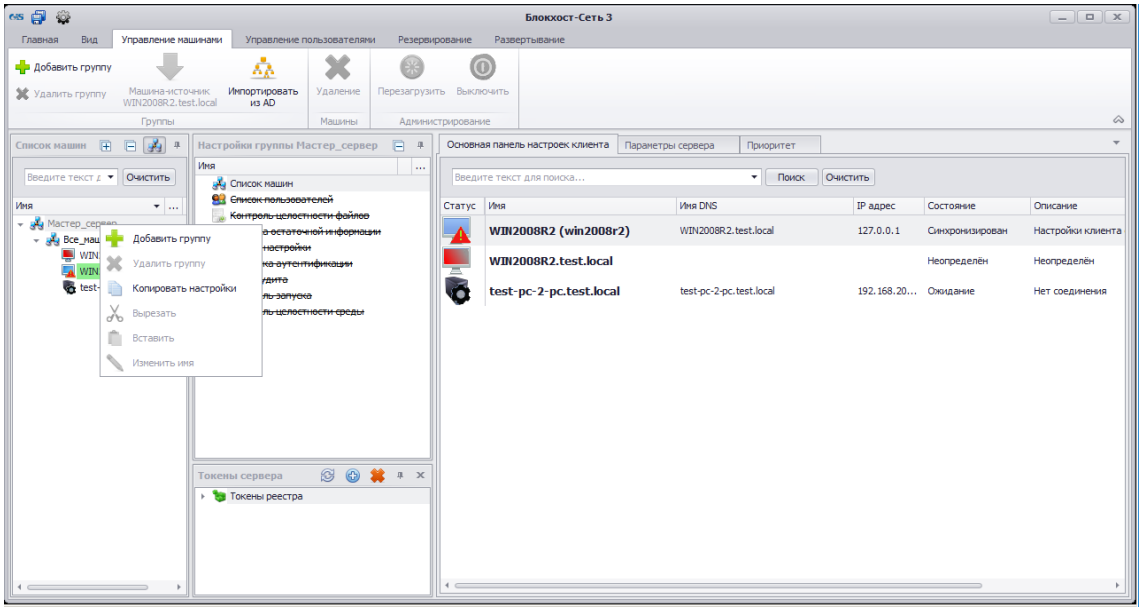


Рисунок 7.1 – Меню создания группы объектов

Для создания группы необходимо выделить в окне **«Список машин»** группу ***Мастер_Сервер*** (или любую другую, в которую будет добавляться новая группа, за исключением группы ***Все_машины***) и выбрать пункт меню ***Управление машинами*** →***Добавить группу***, или воспользоваться пунктом контекстного меню ***Добавить группу***, появляющегося при щелчке правой кнопкой мыши по имени группы 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>**.

Для всех созданных на сервере групп (за исключением группы по умолчанию ***Все_машины***) можно создавать вложенные группы – выделить в окне **«Список машин»** необходимую группу и выбрать пункт главного или контекстного меню ***Добавить группу***. В результате, созданная группа будет вложена в выделенную в окне **«Список машин»**.

Для добавления рабочей станции, уже контролируемой на сервере СЗИ, в группу необходимо захватить ее левой кнопкой мыши и, не отпуская кнопку, перетащить эту рабочую станцию на имя группы (рис. 7.2).

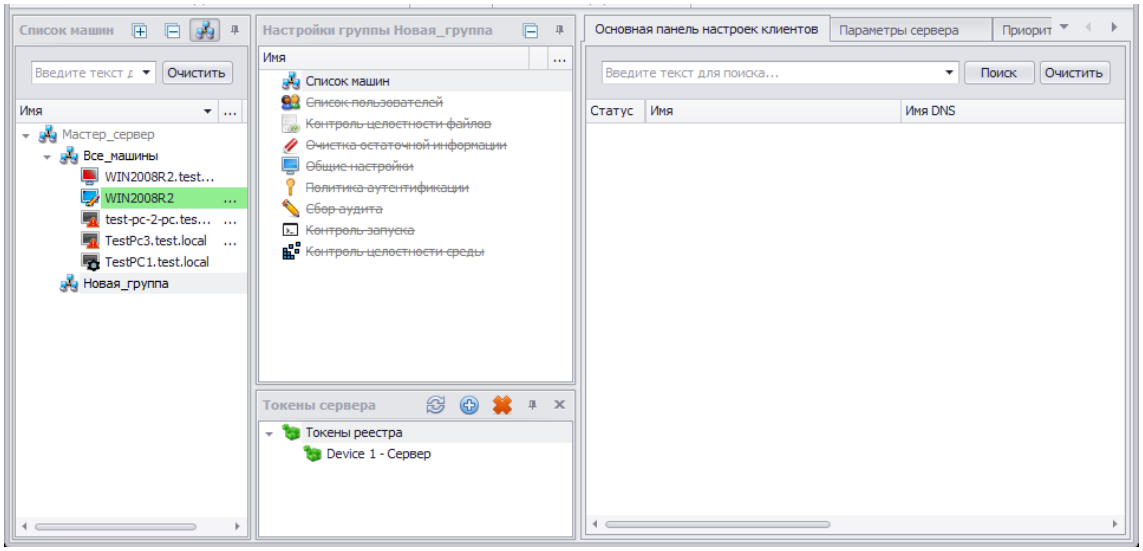


Рисунок 7.2 – Перемещение рабочей станции в группу

Также переместить рабочую станцию в группу можно при помощи меню:

1) Выделить переносимую рабочую станцию и выбрать пункт основного меню ***Управление машинами*** →***Вырезать*** (см. пример на рис. 7.1), или выбрать пункт контекстного меню выделенной рабочей станции ***Вырезать*** (рис. 7.3).

2) Выделить группу, в которую будет помещена рабочая станция и выбрать пункт основного меню ***Управление машинами*** →***Вставить***, или выбрать пункт контекстного меню выделенной группы ***Вставить*** (см. пример на рис. 7.1).

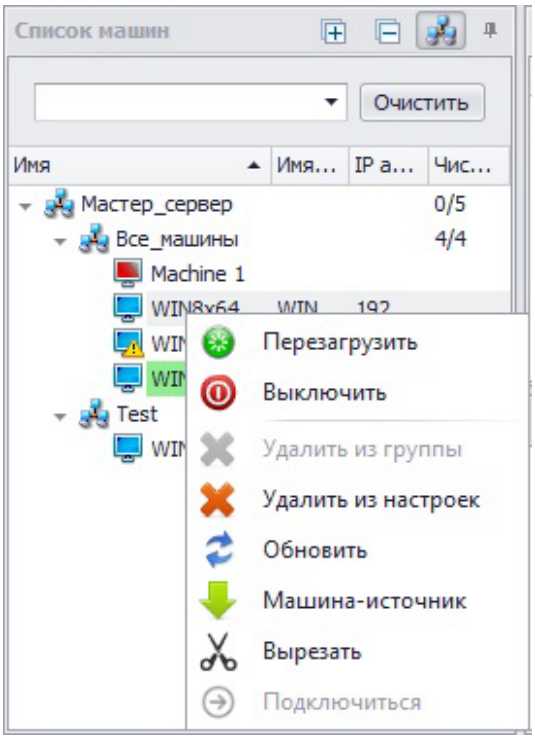


Рисунок 7.3 – Контекстное меню рабочей станции

Одну и ту же рабочую станцию можно добавить только в одну из созданных групп, при этом она пропадет из группы по умолчанию (***Все_машины***) окна **«Список машин»**, но останется в списке рабочих станций выделенной группы ***Мастер_сервер*** в **Основной консоли настроек клиентов**. Переместить рабочую станцию из созданной группы, в группу ***Мастер_сервер*** нельзя. Настройки СЗИ, ранее произведенные на контролируемых рабочих станциях, сохраняются и после перемещения рабочих станций в другие группы.

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 выбрать пункт контекстного меню ***Удалить из группы*** (рис. 7.3). В результате рабочая станция будет перемещена в группу по умолчанию (***Все_машины***). Рабочая станция, удаленная из вложенной группы, также сразу будет перемещена в группу ***Все_машины***, минуя родительскую группу.

Из группы по умолчанию (***Все_машины***) удалить рабочую станцию нельзя – в этом случае пункт контекстного меню рабочей станции ***Удалить из группы*** будет неактивен. Выбор пункта контекстного меню рабочей станции ***Удалить из настроек*** приведет к удалению ее из списка контролируемых текущим сервером СЗИ.

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. Удаление вложенной группы также приводит к тому, что все входившие в нее рабочие станции будут перемещены в группу ***Все_машины***, минуя родительскую группу. Группу ***Все_машины*** удалить нельзя.

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***.

7.1 Групповая настройка пользовательских механизмов защиты информации

В серверной консоли СЗИ «Блокхост-Сеть 3» существует возможность настройки (копирования путем замещения) пользовательских механизмов защиты информации на рабочих станциях, которые входят в одну группу на сервере СЗИ. Групповая настройка пользовательских механизмов СЗИ также распространяется и на группы, вложенные в выбранную группу. Использование групповой репликации пользовательских настроек защиты информации позволит АБ существенно упростить процесс назначения однотипных политик на контролируемые рабочие станции.

Групповая настройка пользовательских механизмов СЗИ включает в себя: монопольный доступ, дискреционный механизм, контроль портов, ограничения по времени, контроль процессов, контроль печати, полномочия администратора, аутентификация.

При репликации списка пользователей, который сформирован для группы, на рабочих станциях происходит добавление учетных записей, которые отсутствуют в списке СЗИ рабочей станции. При этом уже имеющиеся в СЗИ рабочей станции учетные записи, которые не входят в список СЗИ пользователей группы, не удаляются из списка СЗИ рабочей станции, настройки механизмов СЗИ этих учетных записей также не изменяются.

Группа пользователей AD с привязанным к ним настройками пользовательских механизмов БХС (политика групп пользователей) распространяются по всей иерархии серверов и групп, на любых уровнях. Политика групп пользователей (ПГП), определенная на уровне отдельной станции, не распространяется по иерархии и действует только на той станции, где она была создана. Настройки ПГП (если они определены) приоритетнее настроек пользователя, заведенного в консоли напрямую. Правила применения ПГП на конечных рабочих станциях группах и механизмах определения результирующих настроек для конечного пользователя, входящего в несколько или одну группу пользователей описаны в подпункте 7.1.2.3 «Управление политиками групп пользователей».

7.1.1 Особенности применения настроек пользовательских механизмов СЗИ

Порядок применения настроек пользовательских механизмов СЗИ для рабочей станции после их объединения с настройками группы осуществляется следующим образом:

1) Для пользователя устанавливаются настройки механизмов СЗИ учетной записи группы пользователей AD с наивысшим ***Приоритетом*** (наивысшее значение приоритета - 1), если они заданы в группе рабочих станций.

2) Для пользователя устанавливаются настройки механизмов СЗИ, определенные непосредственно для него, если его учетная запись не входит в группы пользователей AD, учетные записи которых добавлены в список пользователей СЗИ, или если для учетных записей групп пользователей AD, в которые входит пользователь, настройки пользовательских механизмов СЗИ не установлены.

Просмотреть список заданных пользовательских механизмов СЗИ группы можно во вкладке **Приоритет**, которая открывается при выборе в окне **«Настройки группы»** параметра ***Список пользователей***. Во вкладке **Приоритет** механизмы СЗИ отображены в виде иконок. При наведении указателя мышки на иконку механизма появляется всплывающая подсказка с именем механизма СЗИ.

Заданные пользовательские механизмы СЗИ группы пользователей отображаются:

- зеленой галочкой, если они установлены в редактируемой группе. При наведении на галочку указателя мышки отображается всплывающая подсказка *Задан в групп*е;
- серой галочкой, если они заданы в родительской группе. При наведении на галочку указателя мышки отображается всплывающая подсказка *Унаследован от <имя_группы>*.

Незаданные механизмы СЗИ группы пользователей содержат пустые ячейки в соответствующих столбцах.

7.1.2 Настройка пользовательских механизмов СЗИ для группы рабочих станций

По умолчанию в настройках группы рабочих станций все механизмы СЗИ запрещены к редактированию. Для возможности редактирования параметров СЗИ необходимо эту операцию явно разрешить: выбрать пункт ***Задать*** контекстного меню требуемого параметра СЗИ (рис. 7.4). Включение возможности редактирования пользовательских механизмов СЗИ в группе рабочих станций осуществляется с учетом иерархии параметра. Например, для включения возможности редактирования дискреционного механизма СЗИ пользователя (группы пользователей) необходимо сначала включить такую возможность для параметра ***Список пользователей***, затем добавить учетную запись пользователя (группы пользователей) в список пользователей СЗИ группы рабочих станций, и только потом появится возможность включения возможности редактирования параметра ***Дискреционный***.

Выбор пункта контекстного меню ***Отключить*** для учетной записи пользователя (группы пользователей) автоматически удаляет выбранную учетную запись пользователя (группы пользователей) из списка пользователей СЗИ.

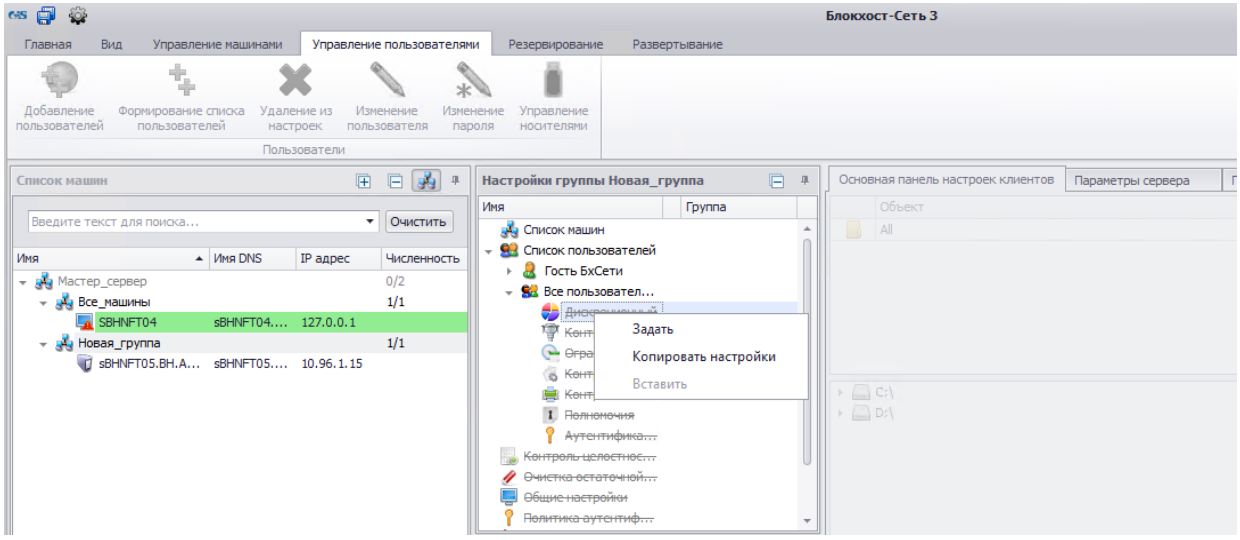


Рисунок 7.4 – Контекстное меню управления механизмами СЗИ группы рабочих станций

Любые «заданные» настройки можно переопределить на любом нижнем уровне иерархии, так как они будут открыты для редактирования. В случае, если у группы или сервера, где было выполнено переопределение, есть свои дочерние группы или сервера, то на них будут распространяться уже переопределенные настройки.

Если АБ хочет распространить по иерархии какие-либо настройки без возможности их переопределения на уровнях ниже, то следует использовать **режим запрета переопределения («замок»)**, доступный в контекстном меню механизма или ПГП (рисунок 7.5). Режим «замок» означает, что настройка или ПГП не может переопределена на нижних уровнях иерархии, по которой она распространяется.

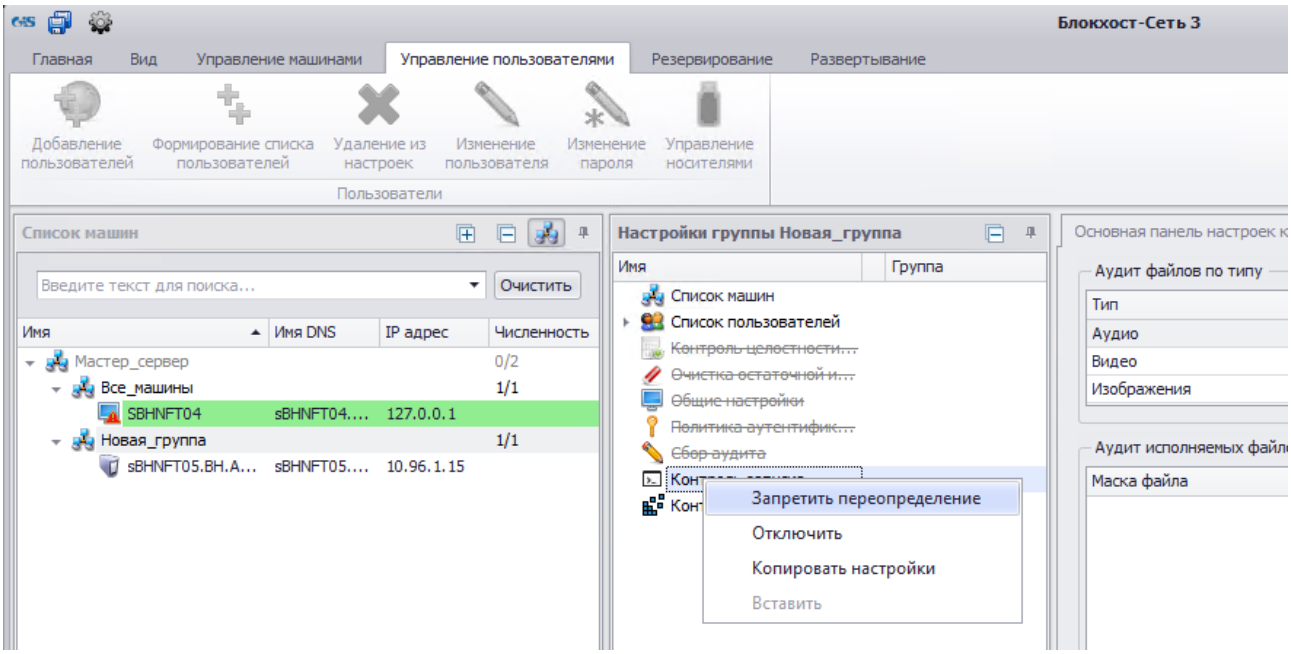


Рисунок 7.5 – Запрет переопределения на нижних уровнях иерархии

Процесс настройки пользовательских механизмов СЗИ списка пользователей группы рабочих станций, полностью совпадает с порядком настройки этих механизмов для пользователей рабочих станций и описан в подразделе 6.1 «6.1 Настройка пользовательских механизмов разграничения доступа» настоящего руководства.

7.1.2.1 Формирование списка пользователей в группе

Для возможности настройки пользовательских механизмов СЗИ группы рабочих станций с целью их последующей синхронизации на рабочих станциях, входящих в группу, необходимо сформировать список пользователей СЗИ в настройках выбранной группы. Для добавления учетных записей пользователей (групп пользователей) в список группы администратор должен выполнить следующие действия в серверной консоли администрирования СЗИ:

1) В окне **«Список машин»** выделить группу, для которой будет формироваться список пользователей.

2) В окне **«Настройки группы»** щелкнуть правой кнопкой мыши по параметру ***Список пользователей*** и выбрать пункт контекстного меню ***Задать*** (см. пример на рис. 7.4).

3) В окне **«Настройки группы»** выделить параметр ***Список пользователей*** и, выбрав пункт меню ***Управление пользователями →Добавление пользователей***, сформировать список учетных записей пользователей (групп пользователей) СЗИ группы.

Процесс формирования списка пользователей СЗИ для группы полностью совпадает с процессом формирования списка пользователей в СЗИ рабочих станций и подробно описан в подразделе 5.1 «Добавление пользователей в СЗИ «Блокхост-Сеть 3»

настоящего руководства.

4) Сохранить произведенные настройки группы, для чего выбрать пункт меню ***Главная*** → ***Сохранить все***, или нажать кнопку ***Сохранить все***  , расположенную в левом верхнем углу консоли администрирования СЗИ.

В результате во всех вложенных в редактируемую группу группах рабочих станций (если они есть) также появится сформированный в родительской группе список пользователей СЗИ.

Для возможности редактирования пользовательских механизмов СЗИ для этих учетных записей необходимо эту операцию явно разрешить: выбрать пункт ***Задать*** контекстного меню требуемого механизма СЗИ для учетной записи пользователя (группы пользователей) – см. пример на рис. 7.4).

Нельзя изменить параметры учетной записи пользователя, добавленной в список пользователей группы рабочих станций: имя (логин), пароль и назначить аппаратный идентификатор.

7.1.2.2 Изменение приоритета учетных записей групп пользователей

Добавленным в список пользователей СЗИ группы рабочих станций учетным записям групп пользователей Active Directory присваивается ***Приоритет***. Параметр ***Приоритет*** учетной записи группы пользователей учитывается в случае применения заданных в настройках группы рабочих станций параметров механизмов СЗИ к пользователю, учетная запись которого присутствует в составе нескольких учетных записей групп пользователей AD, добавленных в список пользователей СЗИ. Для такого пользователя будут использоваться настройки механизмов СЗИ, которые заданы для учетной записи группы пользователей AD имеющей наибольшее значение параметра ***Приоритет*** (значение 1) на рабочей станции.

Порядок изменения значения параметра ***Приоритет*** учетных записей групп пользователей AD для выбранной группы рабочих станций полностью совпадает с процессом изменения значения параметра ***Приоритет*** учетных записей групп пользователей в списке СЗИ рабочей станции.

Значение параметра ***Приоритет*** учетных записей групп пользователей AD, добавленных в список пользователей СЗИ группы рабочих станций, автоматически распространяется и на все вложенные в эту группу группы рабочих станций.

По умолчанию приоритет учетных записей групп пользователей AD в списке пользователей СЗИ рабочей станции устанавливается по мере формирования этого списка – наивысший приоритет (значение 1) имеет учетная запись группы пользователей, которая была добавлена в список пользователей в СЗИ раньше. Администратор безопасности может изменить приоритет учетных записей групп пользователей AD, которые присутствуют в списке пользователей в СЗИ. Для изменения приоритета учетной записи группы пользователей AD в списке пользователей в СЗИ

рабочей станции необходимо выполнить следующие действия:

1) В окне **«Список машин»** консоли администрирования СЗИ раскрыв пункт ***Все_машины***, выделить рабочую станцию, список пользователей которой будет редактироваться.

2) В окне «**Настройки машины**» выделить пункт ***Список пользователей*** – рядом с **Основной панелью настроек клиентов** откроется вкладка **Приоритет**:

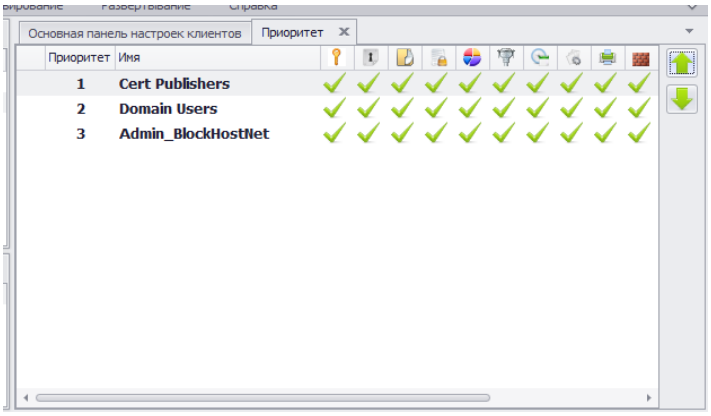


Рисунок 7.6 – Редактирование значения приоритета группы пользователей

3) Во вкладке **Приоритет** выделить учетную запись группы пользователей и с помощью стрелок ***Повысить приоритет*** и ***Понизить приоритет***, расположенных в правой части вкладки, установить необходимое значение приоритета этой учетной записи.

4) Сохранить внесенные изменения, выбрав пункт меню ***Главная→ Сохранить все***, или нажав кнопку ***Сохранить все***  , расположенную в левом верхнем углу консоли администрирования СЗИ.

В списке пользователей СЗИ группы рабочих станций существует возможность заблокировать изменение значения параметра ***Приоритет*** для одной или нескольких учетных записей групп пользователей AD. Для блокировки значения параметра ***Приоритет*** группы пользователей администратору безопасности необходимо выполнить следующие действия:

1) В окне **«Список машин»** выделить группу рабочих станций, в которой будут редактироваться параметры учетных записей из списка пользователей СЗИ.

2) В окне **«Настройки группы»** выделить параметр ***Список пользователей*** и перейти в открывшуюся вкладку **Приоритет**.

3) Во вкладке **Приоритет** щелкнуть правой кнопкой мыши на строке с именем учетной записи группы пользователей и выбрать пункт контекстного меню ***Заблокировать приоритет*** (рис. 7.7).

4) Сохранить произведенные в группе рабочих станций настройки, для чего выбрать пункт меню ***Главная→ Сохранить все***, или нажать кнопку ***Сохранить все***  ,

расположенную в левом верхнем углу консоли администрирования СЗИ.

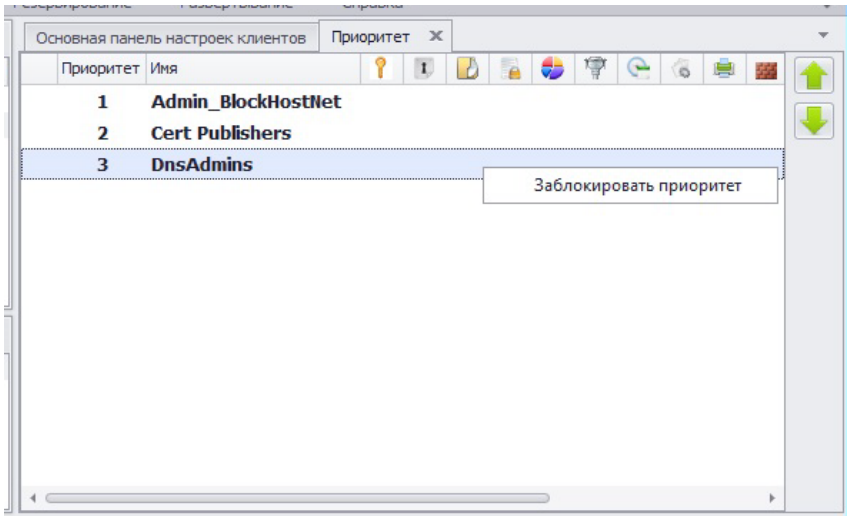


Рисунок 7.7 – Блокировка приоритета группы пользователей

В результате во всех вложенных группах рабочих станций (если они есть у редактируемой группы) с разрешенным к редактированию параметром ***Список пользователей*** появится дополнительная учетная запись группы пользователей, в имени которой содержится имя группы рабочих станций на сервере СЗИ.

7.1.2.3 Управление политиками групп пользователей

Политики групп пользователей основаны на доменных группах безопасности. Количество ПГП для группы машин или станции может быть неограниченно. Один и тот же пользователь может входить в несколько групп пользователей, и на него будет распространятся действия нескольких ПГП. Кроме того, в различных ПГП для пользователя могут быть определены различные механизмы безопасности, причем в каждой ПГП такой набор механизмов будет уникальным.

Для понимания механизма определения настроек конечного пользователя в этом случае рассмотрим пример:

Пользователь входит в доменные группы: группа 1, группа 2 и группа 3. На основе этих групп созданы одноименные ПГП, механизмы в них определены согласно таблице 1. Значение от set1 до set 9 – уникальные настройки механизмов ПГП, заданные АБ.

Таблица 7.1 – Настройки ПГП

Наименование ПГП	***Приоритет***	***Дискре-ционный механизм***	***Контроль портов***	***Контроль печати***	***Контроль процессов***	***Аутенти-фикация***
Группа 1	1	Set1	Не задано	Set2	Set3	Не задано
Группа 2	2	Не задано	Set4	Не задано	Set5	Не задано
Группа 3	3	Set6	Set7	Set8	Не задано	Set9

Если пользователь входит во все три группы одновременно, то заданные настройки (у нас они обозначены термином set) буду браться из группы, обладающей наибольшим приоритетом (максимальным приоритетом в таблице обладает группа 1 с приоритетом 1, минимальным приоритетом: группа 3 с приоритетом 3).

Если настройки в самой приоритетной группе не заданы, берутся заданные настройки из ПГП со следующим по значению приоритетом.

Если настройки механизма не заданы ни в одной из ПГП, присваиваются настройки по умолчанию или те, которые были заданы пользователю вручную. Таким образом, пользователь, входящий во все три ПГП, получит следующий набор настроек:

Таблица 7.2 – Результирующие настройки пользователя

Дискреционный механизм	***Контроль портов***	***Контроль печати***	***Контроль процессов***	***Аутентификация***
Set1	Set4	Set2	Set3	Set9

Дискреционный механизм, контроль печати и контроль процессов заданы в группе 1, которая является наиболее приоритетной (значение приоритета 1), поэтому пользователь получит настройки этих механизмов из группы 1. Контроль портов пользователь получит из группы 2, так как в группе 1 механизм не задан, а значение приоритета группы 2 меньше, чем группы 3. Значение аутентификации пользователь получит из группы 3, так как в других группах этот параметр не задан.

Приоритет ПГП может быть изменен АБ вручную на любом уровне иерархии с помощью окна управления приоритетом. Для запрета изменения приоритета АБ может использовать режим «замок» на приоритете любой ПГП (п. 7.1.2. «Настройка пользовательских механизмов СЗИ для группы рабочих станций»).

Установка режима «замок» на список пользователей может привезти к невозможности входа пользователей на рабочие станции и отказам, связанным с изменением настроек станций и с удалением из списка пользователей учетной записи «**Гость БхСети**». Что приведет к невозможности работы таких учетных записей на станции, и может привести к отказу в работе приложений и служб, и к отказу в доступе к станции.
При использовании списка пользователей в режиме «замок» рекомендуется вручную добавлять на рабочие станции учетную запись «**Гость БхСети**».

7.2 Групповая настройка механизмов защиты информации станции

В серверной консоли СЗИ «Блокхост-Сеть 3» существует возможность настройки механизмов защиты информации на рабочих станциях, которые входят в одну группу на сервере СЗИ. Использование групповых настроек защиты информации станции позволит администратору безопасности существенно упростить процесс назначения однотипных политик на рабочие станции, входящих в одну группу.

Для групповой настройки механизмов станции доступны все механизмы станции СЗИ (мандатный, контроль целостности, очистка памяти, политика аутентификации, включение или отключение мягкого режима), а также общие параметры работы клиента СЗИ.

В процессе репликации механизмов станции СЗИ происходит замещение настроек механизмов СЗИ, которые установлены на рабочих станциях, на настройки механизмов СЗИ, которые установлены в группе рабочих станций, находящихся ниже по иерархии.

Определенные на верхней группе настройки действуют для всей иерархии, но могут быть переопределены на уровне нижних групп иерархии. Настройки будут применятся ко всем пользователям станций иерархии, независимо от других политик безопасности.

Если рабочая станция в момент запуска процесса синхронизации находится в выключенном состоянии, то настройки механизмов СЗИ, предназначенные для нее, будут записаны в базу данных СЗИ, которая расположена на сервере СЗИ. После включения рабочей станции, в момент ее соединения с сервером СЗИ, настройки механизмов СЗИ этой рабочей станции будут заменены на настройки механизмов СЗИ, которые хранятся в базе данных СЗИ.

Для того чтобы синхронизировать настройки механизмов станции СЗИ на рабочие станции, входящие в одну группу на сервере СЗИ, администратору безопасности необходимо:

1) Сделать одну из рабочих станций на сервере СЗИ источником файловой системы, необходимой для настройки механизмов группы станции:

- выделить рабочую станцию в окне **«Список машин»**;
- выбрать пункт меню ***Управление машинами →Машина-источник*** (рис. 7.8), или выбрать аналогичный пункт в контекстном меню рабочей станции (см. пример на рис. 7.3).

Не рекомендуется устанавливать в качестве источника файловой системы для настройки механизмов станции группы рабочую станцию, настройки которой еще не были загружены в серверную консоль администрирования СЗИ – список доступных объектов в **Основной панели настроек клиентов** будет пустой.

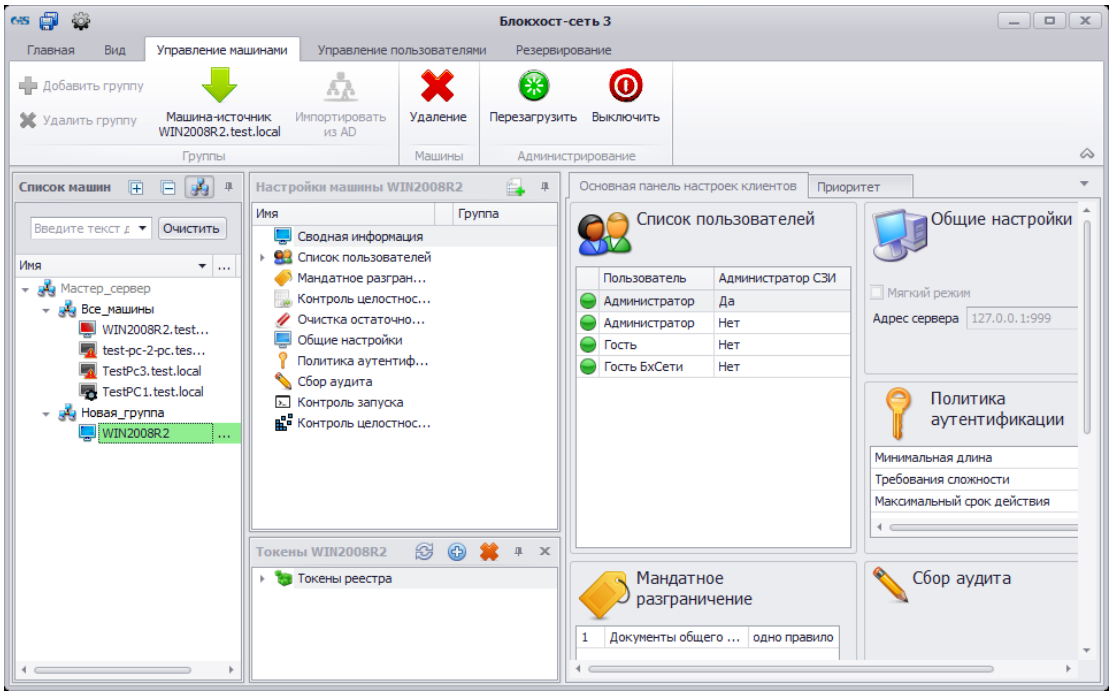


Рисунок 7.8 – Меню управления группами рабочих станций

2) Разрешить синхронизацию механизма станции СЗИ в группе, который будет синхронизирован на входящие в группу рабочие станции, для чего выделить в окне **«Список машин»** группу, а в окне **«Настройки группы»** щелкнуть правой кнопкой мыши по названию требуемого механизма СЗИ и выбрать пункт контекстного меню ***Задать*** (см. пример на рис. 7.4).

3) Произвести настройку механизмов станции СЗИ группы, которые будут синхронизироваться (подробнее о настройке механизмов станции СЗИ см. п. 6.2 «Настройка механизмов защиты информации станции» настоящего руководства).

4) Сохранить внесенные изменения в параметры настроек механизмов станции СЗИ группы, для чего выбрать пункт меню ***Главная→ Сохранить все***, или нажать кнопку ***Сохранить все***  , расположенную в левом верхнем углу консоли администрирования СЗИ.

5) При необходимости повторить действия пунктов 1 – 4 по настройке и синхронизации механизмов станции СЗИ для других групп и рабочих станций, имеющихся на сервере СЗИ.

После того, как будет нажата кнопка **Сохранить все**  , все измененные параметры будут синхронизированы между сервером и подчиненными серверами и клиентами.

8 Регистрация событий, связанных с безопасностью защищаемой информации

Механизм регистрации событий и аудита предназначен для отслеживания событий и регистрации обращения к защищаемым ресурсам. а также при срабатывании всех механизмов защиты.

Сформированные события содержат следующую информацию:

- дата и время;
- источник записи;
- категория доступа;
- тип сообщения (успешное или неуспешное);
- код (ID);
- пользователь;
- имя компьютера;
- имя пользователя;
- метка пользователя;
- имя объекта;
- метка объекта;
- тип доступа;
- привилегии.

Кроме того, сформированные события могут содержать дополнительную информацию, характерную для каждого модуля СЗИ «Блокхост-Сеть 3». Список событий, регистрируемых механизмом регистрации событий СЗИ «Блокхост-Сеть 3», и их описание приведен в Приложении 5 к настоящему документу.

В консоли системы развертывания и аудита Блокхост-Сеть АБ доступен следующий функционал для работы с событиями аудита:

- формирование сводного отчета с информацией о состоянии клиентов, подключенных к серверам иерархии;
- сбор событий аудита с клиентов на сервер СЗИ;
- просмотр и фильтрация событий аудита, собранных с клиентских компьютеров на сервер;
- просмотр и фильтрация событий аудита напрямую из журнала клиентского компьютера;
- передача событий аудита вверх по иерархии серверов вплоть до головного сервера с последующей передачей в SIEM-систему.

Настройка перечня собираемых событий осуществляется АБ в консоли администрирования СЗИ (п. 6.2.9 «Сбор аудита»).

Централизованный сбор и просмотр данных аудита, из настроенного АБ перечня, осуществляется в консоли системы развертывания и аудита Блокхост-Сеть. Описание работы с событиями приведено в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

8.1 Просмотр событий аудита

Просмотр событий аудита, собираемых механизмом регистрации событий и аудита СЗИ «Блокхост-Сеть 3», осуществляется администратором безопасности с помощью:

- программы просмотра событий операционной системы – консоли MMC;
- консоли «Системы развертывания и аудита» (просмотр событий аудита с помощью консоли подробно рассмотрен в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности»).

Просмотр событий с помощью средств консоли MMC позволяет осуществлять просмотр всех событий системы. Просмотр событий с помощью средств консоли «Системы развертывания и аудита» позволяет осуществлять только просмотр событий, зафиксированных СЗИ «Блокхост-Сеть 3».

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*** (рисунок 8.1).

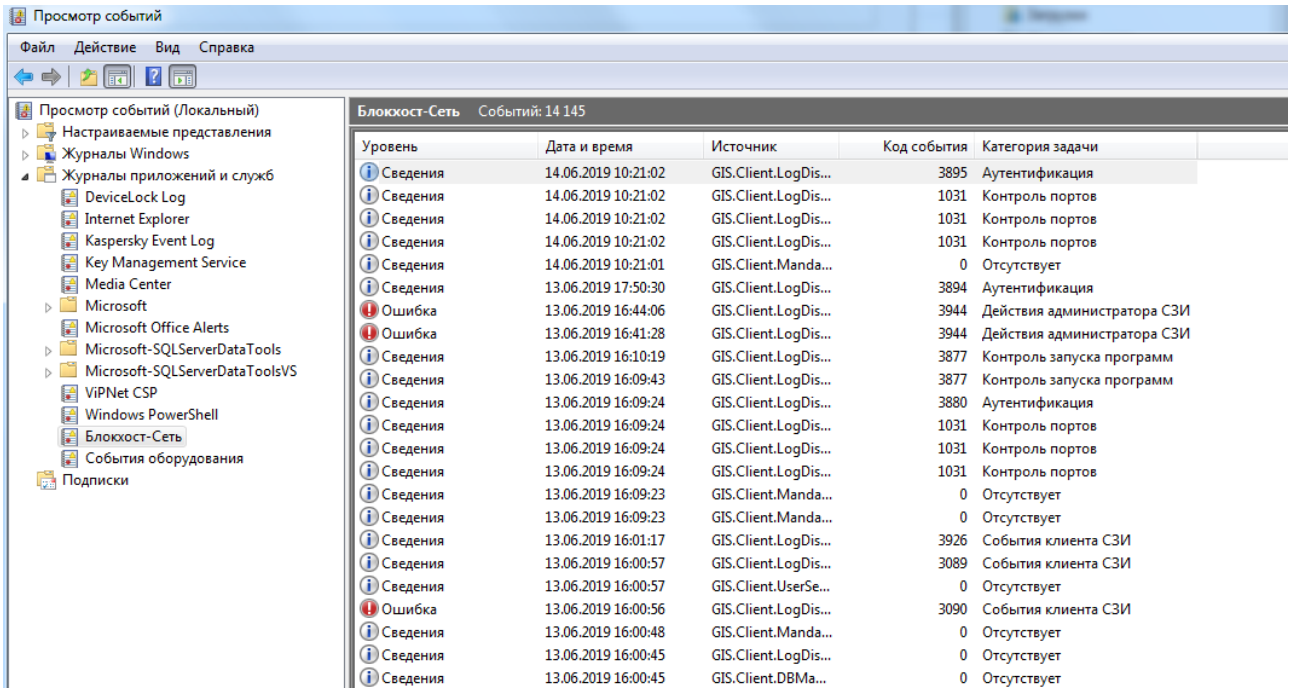


Рисунок 8.1 – Окно просмотра аудита с помощью консоли MMC

После двойного щелчка на выбранном событии станет доступным его подробное описание (рисунок 8.2).

Для пользователя, не имеющего соответствующих полномочий, можно ограничить просмотр событий аудита. Для этого необходимо запретить соответствующему пользователю запуск процесса *Просмотр событий* ОС Windows (т.е. запретить запуск MMC-консоли). Запретить запуск *Просмотр событий* можно также, 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 *Просмотр событий*) будут запрещены для запуска. Подробное описание данного механизма приведено в пункте 6.1.3 «Разграничение доступа к запуску процессов» настоящего руководства.

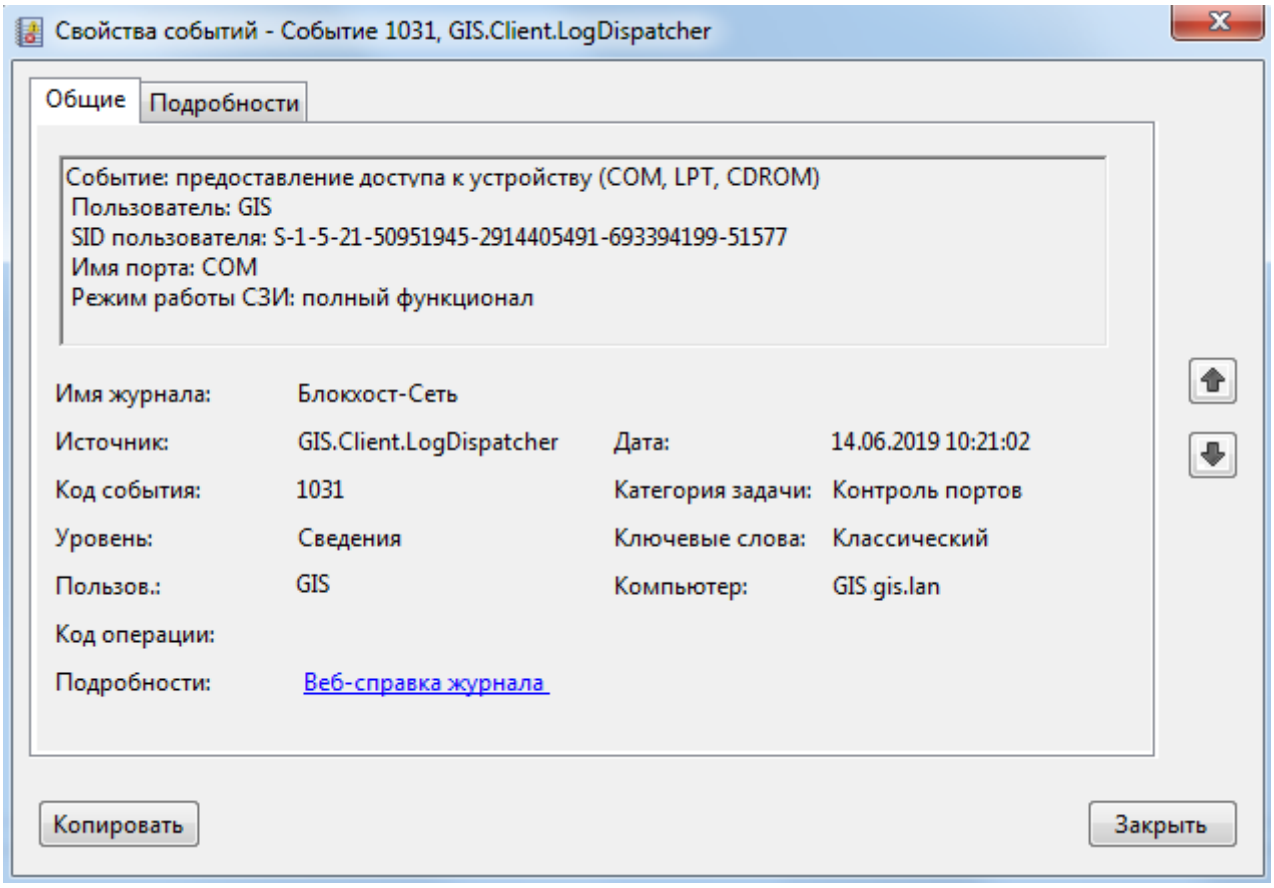


Рисунок 8.2 – Окно описания события

Приложение 1

(рекомендуемое)

Сбор диагностической информации

В СЗИ «Блокхост-Сеть 3» 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 консоли администрирования СЗИ имеется возможность контролировать информационные сообщения СЗИ. Для этого необходимо на ярлыке вызова приложения вызвать его свойства (пункт контекстного меню ярлыка ***Свойства***) и в открывшемся окне свойств на вкладке **Ярлык** в текстовое поле ***Объект*** добавить к команде вызова приложения параметр ***-trace*** таким образом, чтобы получилась команда: *C:\BlockHost\ServerBPShell\GIS.BlockPost.Server.exe –trace* (для серверной консоли) или *C:\BlockHost\BPShell\GIS.BlockPost.Client.exe –trace* (для локальной консоли).

После включения этой опции в окне **«Лог»** будут отображаться все события, связанные с работой консоли администрирования СЗИ. А в каталоге *%LOCALAPPDATA%\BlockPost\Log* профиля пользователя, запустившего консоль, 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 *%LOCALAPPDATA%\BlockPost\Log* профиля пользователя, запустившего консоль администрирования СЗИ.

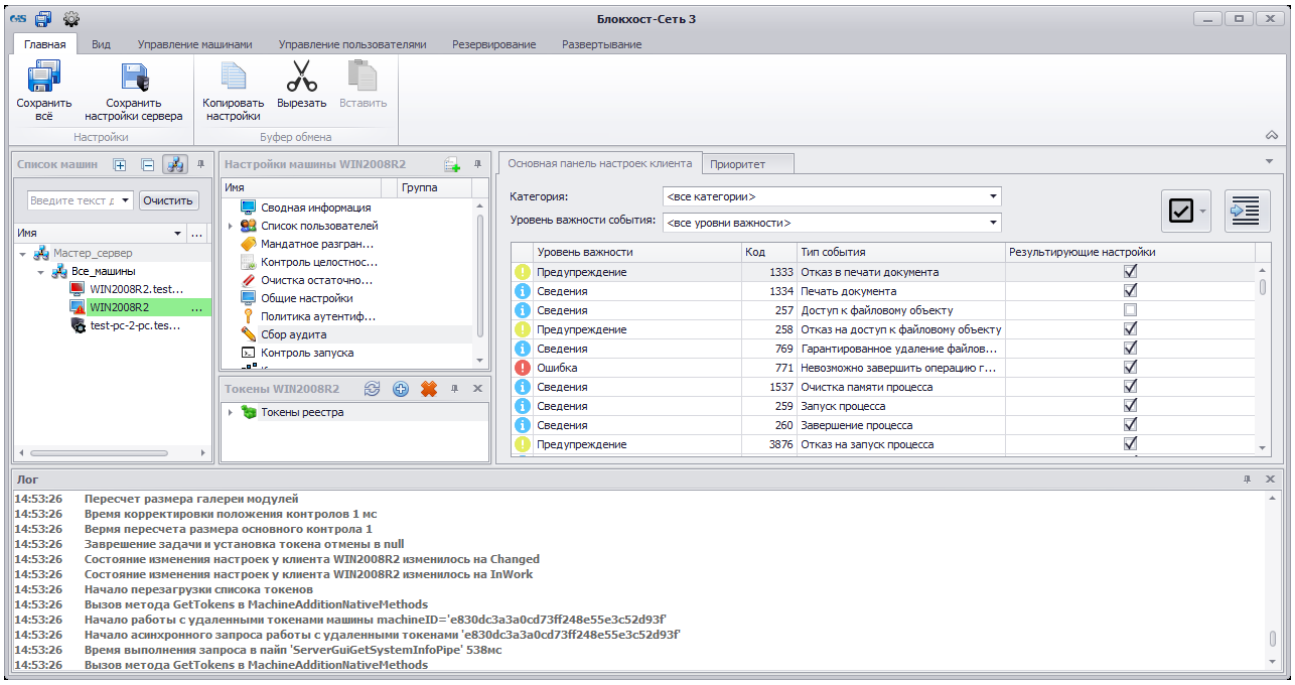


Рисунок П1.1 – Отображение информационных сообщений СЗИ в окне «Лог» серверной консоли

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 подсистемы аутентификации СЗИ. 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.