ViPNet SafePoint

Руководство администратора по локальному администрированию

infotecs

ФРКЕ.00240-01 32 01

Версия продукта 1.0.0

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

АННОТАЦИЯ

В документе приводится руководство администратора безопасности (локальное администрирование) к системе защиты информации «ViPNet SafePoint» для ОС Microsoft Windows (далее СЗИ «ViPNet SafePoint»). В первых четырех частях документа представлены общие сведения об интерфейсе СЗИ «ViPNet SafePoint», процедуры инсталляции, деинсталляции и запуска программного комплекса. В частях 5-15 документа приведены описания действий администратора по настройке механизмов защиты, содержание сообщений, выдаваемых администратору СЗИ «ViPNet SafePoint», описание действий, которые должен предпринять администратор, получив данные сообщения. Данные материалы сгруппированы в отдельных частях документа по функциональному назначению механизмов защиты СЗИ «ViPNet SafePoint».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. НАЗНАЧЕНИЕ

Система защиты информации «ViPNet SafePoint» для ОС Microsoft Windows (СЗИ «ViPNet SafePoint») предназначена для защиты от несанкционированного доступа к информации.

СЗИ «ViPNet SafePoint» – это система защиты уровня ядра ОС. Эффективная защита на уровне ядра ОС является основой безопасности любой информационной системы. Только реализовав эффективную защиту на этом уровне, уже имеет смысл реализовывать дополнительную защиту различными прикладными средствами, в том числе, решающими различные задачи детектирования.

СЗИ «ViPNet SafePoint» позволяет в комплексе решать актуальные задачи защиты информации от внешних и от внутренних угроз.

1. Защита от внутренних угроз (от инсайдерских атак):

- от атак со стороны интерактивных пользователей, санкционированно обрабатывающих данные в информационной системе;
- от атак со стороны привилегированных пользователей (администраторов), решающих те или иные задачи администрирования в информационной системе.

2. Защита от внешних угроз (хакерских атак), в том числе, эффективная защита от целевых (таргетированных) атак.

СЗИ «ViPNet SafePoint» может использоваться для защиты рабочих станций, серверов, терминальных серверов, средств виртуализации Hyper-V, включая защиту и гостевых машин, и гипервизора.

1.2. СОСТАВ СЗИ «VIPNET SAFEPOINT», ЗАДАЧИ КОМПОНЕНТОВ

СЗИ «ViPNet SafePoint» состоит из следующих отдельно устанавливаемых программных средств:

1. Клиентская часть.
2. Сервер безопасности.
3. Сервер аудита.
4. Программа тиражирования настроек.

Клиентская часть СЗИ «ViPNet SafePoint» предназначена для непосредственной защиты информации – в ней реализуются все механизмы защиты, как для защиты компьютеров в составе локальной вычислительной сети (ЛВС) предприятия с выделенным рабочим местом администратора безопасности ЛВС, так и для защиты автономных компьютеров. Устанавливается на защищаемые объекты информатизации: рабочие станции и серверы.

Сервер безопасности СЗИ «ViPNet SafePoint» предназначен для удаленного управления клиентскими частями и обработки журналов аудита в интерактивном режиме, предоставляет администратору безопасности всю необходимую для принятия решений справочную информацию (по вычислительным средствам и пользователям информационных ресурсов, обрабатываемых в корпоративной сети). Устанавливается на выделенный компьютер администратора безопасности.

Сервер аудита СЗИ «ViPNet SafePoint» предназначен для удаленного сбора и обработки аудита реального времени со всех компьютеров в составе сети, на которые устанавливается клиентская часть СЗИ «ViPNet SafePoint». Устанавливается на выделенный компьютер администратора безопасности. Контролируемые события по всем защищаемым объектам в реальном времени отображаются на сервере аудита в окне интерфейса. Сервер аудита может устанавливаться, как на том же компьютере, что и сервер безопасности, так и на отдельном компьютере.

Программа тиражирования настроек СЗИ «ViPNet SafePoint» предназначена для проведения первичной настройки клиентских частей, подключенных к серверной части (сервер безопасности) СЗИ «ViPNet SafePoint».

При первичной настройке клиентская часть подключается к серверу безопасности и к серверу аудита. Реализована возможность подключать одну клиентскую часть к нескольким (неограниченному числу) серверам безопасности и/или к нескольким (неограниченному числу) серверам аудита. Может быть реализована иерархия серверов, включающая: главный сервер, взаимодействующий со всеми клиентскими частями СЗИ «ViPNet SafePoint», установленными в защищаемой корпоративной сети, и подчиненные серверы безопасности (аудита), взаимодействующие с клиентскими частями СЗИ «ViPNet SafePoint» соответствующих подсетей.

1.3. ТЕХНОЛОГИЯ ЗАЩИТЫ И ПОДХОД К РЕАЛИЗАЦИИ

Вычислительное средство – объект защиты, может быть охарактеризовано иерархией имеющихся ролей:

- роль загрузки системы (BIOS, загрузчик ОС);
- роль «система» (процесс System, системные драйверы, службы, процессы и библиотеки);
- функциональная роль объекта защиты (рабочая станция, сервер, терминальный сервер, виртуальная машина и гипервизор и т.д.);
- роль системного администрирования объекта (системный администратор и средства администрирования);

- роль защиты объекта (администратор безопасности, средства защиты и их администрирования);
- роли пользователей (интерактивные пользователи и приложения).

2. Каждая роль в общем случае характеризуется необходимым и достаточным для нее набором субъектов доступа (пользователь, процесс) и соответствующим для роли необходимым и достаточным набором объектов доступа (ресурсов).

3. Реализация технологии защиты в общем случае состоит в решении следующих задач:

- локализация режимов обработки данных в рамках соответствующих ролей: по пользователям, процессам, объектам доступа. В рамках каждой роли должны использоваться только необходимые для нее субъекты и объекты доступа при условии предотвращения несанкционированной возможности изменения их наборов и модификации;
- изоляция режимов обработки данных в рамках различных ролей одного и различных уровней иерархии: для каждой роли должны предоставляться только необходимые и достаточные для ее реализации возможности, а также способы взаимодействия с другими ролями при условии предотвращения несанкционированной возможности их изменения и модификации.

СЗИ «ViPNet SafePoint» реализует иерархическую ролевую модель доступа к ресурсам.

В основе системы защиты лежит контроль доступа субъектов к объектам с согласно правам доступа, заданных для решения задач защиты информации. Не используются какие-либо средства детектирования чего-либо, не позволяющие реализовать защиту в общем виде. Подобные средства могут применяться в дополнение к СЗИ «ViPNet SafePoint» на защищаемых объектах информационных систем.

В СЗИ «ViPNet SafePoint» реализованы следующие три основные группы механизмов защиты:

- механизмы контроля и разграничения прав доступа субъектов к статичным объектам, присутствующим в системе на момент назначения администратором прав доступа субъектов к ним. К таким объектам относятся локальные и сетевые файловые объекты, объекты реестра ОС, файловые накопители, определяемые по идентификаторам с учетом серийных номеров, сетевые объекты, локальные и сетевые принтеры и т.д. Данными механизмами реализуется разграничительная политика доступа субъектов к объектам;
- механизмы контроля и разграничения прав доступа субъектов к создаваемым объектам, отсутствующим в системе на момент назначения администратором прав доступа субъектов к ним. К таким объектам относятся создаваемые файлы и данные, временно хранящиеся в буфере обмена. Данными механизмами реализуется разделительная политика между субъектами доступа;

- механизмы защиты от обхода разграничительной и разделительной политик доступа.

Эти механизмы также реализуют контроль доступа, но уже применительно к системным объектам ОС – к сервисам олицетворения, к возможностям прямого доступа к дискам и внедрения кода в процессы и т.д.

1.4. РЕШАЕМЫЕ ЗАДАЧИ ЗАЩИТЫ

В СЗИ реализована идентификация и аутентификация пользователя при запросах на доступ к системе (на вход в систему) при удаленном входе в систему (по RDP и в терминальном режиме). В СЗИ, как при локальном, так и при удаленном входе в систему реализована как консольная идентификация и аутентификация пользователя, так и аутентификация пользователя с использованием устройств хранения и ввода паролей (ruToken, Aladdin JaCarta – в форматах ключа и смарт-карты).

В СЗИ объекты доступа (наименованные и создаваемые объекты) при задании ПРД идентифицируются их именами (идентификаторами) и масками, внешние накопители – идентификаторами устройств, включая серийные номера для конкретных устройств.

В СЗИ реализовано управление идентификаторами, в том числе создание, присвоение, уничтожение и блокирование через заданный администратором период времени идентификаторов пользователей (учетных записей) и устройств.

В СЗИ реализованы следующие возможности задания ограничений на параметры пароля: длина пароля; наличие букв в разных регистрах; наличие цифр; наличие символов, не являющихся буквами и цифрами; отсутствие цепочек символов, вводимых с клавиатуры. В СЗИ реализовано ограничение максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки; блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на заданный промежуток времени. В СЗИ реализована возможность автоматического генерирования пароля СЗИ с заданием следующих ограничений: длина генерируемого пароля; алфавит генератора паролей.

В СЗИ реализована защита обратной связи «система – субъект доступа» в процессе аутентификации. Вводимые символы пароля отображаются условным знаком «●».

СЗИ разрешает или запрещает вход пользователя в безопасном режиме.

В СЗИ реализована идентификация и аутентификация пользователя при запросах на доступ к разделяемым ресурсам (к наименованным разделяемым в сети объектам удаленной системы). При этом реализована как консольная идентификация и аутентификация пользователя, так и аутентификация пользователя с использованием устройств хранения и ввода паролей.

При консольной аутентификации СЗИ предоставляет возможность назначения пароля, как администратором, так и непосредственно пользователем.

В СЗИ в качестве наименованного субъекта доступа используется сущность «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)», где сущность «Полнопутевое имя процесса» используется для возможности задания различных ПРД для различных процессов (приложений), запускаемых одним и тем же пользователем.

В СЗИ в качестве наименованных объектов доступа выступают:

- локальные и разделенные в сети файловые объекты – файлы, каталоги, подкаталоги, логические диски;
- внешние накопители и файловые объекты – файлы, каталоги, подкаталоги на внешних накопителях;
- объекты реестра ОС – ключи и ветви реестра;
- локальные и разделенные в сети принтеры;
- любые иные устройства, в том числе, как системные, так и внешние по отношению к системе.

СЗИ обеспечивает назначение прав пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами.

В СЗИ для предотвращения загрузки исполняемых объектов, включая исполняемые файлы программ, апплетов и скриптов, обеспечивается контроль доступа по расширениям файлов, позволяющий предотвращать создание, удаление, переименование «из», переименование «в» файлов с заданными расширениями.

В СЗИ для наименованного субъекта доступа «Процесс» контролируется смена исходного идентификатора пользователя (идентификатора, которым запущен процесс) на эффективный идентификатор пользователя (идентификатор пользователя, от лица которого запрашивается доступ к объекту процессом). ПРД задают разрешенные/запрещенные права процессов на смену идентификатора пользователя при запросах доступа.

СЗИ обеспечивает в соответствии с должностными обязанностями (функциями) разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

СЗИ обеспечивает удаление пользователя через заданный период времени (при создании временной учетной записи).

СЗИ осуществляет ограничение неуспешных попыток входа и блокировку учетной записи пользователя при превышении пользователем ограничения заданного количества неуспешных попыток входа в информационную систему как при консольной аутентификации, так и при аутентификации по электронному ключу.

Обеспечивает при консольной идентификации и аутентификации возможность блокирования доступа в систему при удалении из системы устройства ввода пароля или по запросу пользователя.

В СЗИ реализован контроль смены идентификатора пользователя при доступе к наименованным объектам в соответствии с заданными правилами.

В СЗИ для контроля и предотвращения доступа к данным на жестком диске и на внешних накопителях, как к не наименованным объектам (не как к объектам файловой системы) реализован контроль прямого доступа наименованных субъектов к дискам (к жесткому диску и к внешним накопителям) с возможностью задания правил разграничения прямого доступа к дискам. В качестве наименованного субъекта доступа используется сущность «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)».

СЗИ позволяет разграничивать права доступа наименованных субъектов к создаваемым в процессе функционирования системы файлам (файлам, используемым для хранения обрабатываемых данных) в NTFS на жестком диске на основе матрицы доступа, при этом объект доступа исключен из ПРД. Правилами задаются права доступа субъектов к файлам, созданным иным субъектом доступа (все ПРД задаются исключительно между субъектами доступа). Реализованы принципы контроля доступа не наименованных субъектов к наименованным файловым объектам, а между наименованными субъектами – к создаваемым ими файловым объектам, чем реализуется уже не разграничительная, а разделительная политика доступа.

СЗИ позволяет разграничивать права доступа к создаваемым файлам на основе матрицы доступа наименованных субъектов для предотвращения возможности исполнения как системными, так и интерактивными пользователями, что необходимо для защиты от запуска несанкционированных программ.

СЗИ позволяет разграничивать права доступа к создаваемым в процессе функционирования системы данным в буфере обмена на основе матрицы доступа наименованных субъектов, при этом объект доступа исключен из ПРД, Правилами задаются права доступа субъектов к данным,

созданным в буфере обмена иным субъектом доступа (все ПРД задаются исключительно между субъектами доступа).

В СЗИ реализована возможность разграничивать права доступа пользователей, определяемых при задании ПРД назначаемыми им метками безопасности, к создаваемым в процессе функционирования системы файлам (файлам, используемым для хранения обрабатываемой информации) в NTFS на жестком диске – правилами задаётся, какой субъект доступа, какие права доступа имеет к файлам, созданным иным субъектом доступа (все ПРД задаются исключительно между субъектами доступа). В СЗИ в случае контроля доступа на основе меток безопасности ПРД назначаются на основе арифметического сравнения меток безопасности, назначаемых пользователям (метки безопасности вручную администратором не назначаются). При этом метки безопасности автоматически наследуются от пользователей объектами доступа, создаваемыми в процессе работы пользователя.

СЗИ обеспечивает возможность одновременной непротиворечивой работы (по соответствующим настроенным ПРД) на основе матрицы доступа и на основе меток безопасности к создаваемым файлам. При этом запрошенный доступ субъекта к объекту СЗИ разрешается только в том случае, если он не противоречит ни ПРД с использованием меток безопасности, ни ПРД на основе матрицы доступа к создаваемым файлам.

СЗИ обеспечивает управление запуском компонентов программного обеспечения, в том числе определение запускаемых компонентов, контроль за запуском компонентов программного обеспечения. В СЗИ для ограничения программной среды заданием ПРД обеспечивается контроль за запуском исполняемых файлов и обеспечиваться возможность исполнения файлов только из заданных каталогов (папок), с предотвращением возможности их несанкционированного удаления и/или модификации не администратором.

СЗИ обеспечивает управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов. В СЗИ для возможности задания ПРД для каждой пары (субъект-объект) реализована возможность перенаправления запросов доступа к объектам файловой системы, используемая для разделения между наименованными субъектами не разделяемых системой и приложениями наименованных файловых объектов, в частности, каталогов временного хранения файлов.

СЗИ обеспечивает управление доступом к машинным носителям информации.

СЗИ обеспечивает контроль использования интерфейсов ввода (вывода).

СЗИ обеспечивает контроль ввода (вывода) информации на машинные носители информации.

СЗИ обеспечивает управление подключением (монтированием) к системе устройств (любых устройств, в том числе, как системных, так и внешних по отношению к системе), конкретных устройств - по их серийным номерам, по пользователям.

СЗИ обеспечивает возможность задания правил монтирования к системе устройств по пользователям, в которых задаётся, при работе каких пользователей в системе (в том числе, одновременной работе каких пользователей), какие устройства могут быть подключены (подключаться) к системе. При нарушении заданных правил монтирования устройств к системе, в результате смены (регистрации нового) пользователя, СЗИ обеспечивает в качестве реакции автоматическое отключение (отмонтирование) от системы несанкционированных устройств.

В СЗИ обеспечивается регистрация всех событий (вход/выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы; подключение машинных носителей информации и вывод информации на носители информации; запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, подключенным к АРМ; внешним устройствам; программам; томам; каталогам; файлам и иным объектам доступа; попытки удаленного доступа), связанных с реализацией возможностей защиты.

Для каждого из этих событий, по крайней мере, регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- удачно ли осуществилось событие (в частности, обслужен ли запрос на доступ или нет).

В СЗИ реализованы два режима регистрации событий – оперативный и реального времени, для них правила регистрации настраиваются отдельно. Режим оперативной регистрации событий предполагает формирование журнала аудита на клиентской части СЗИ с возможностью его получения администратором по запросу с серверной части СЗИ (сервер безопасности). Режим регистрации событий в реальном времени предполагает немедленную (в реальном времени) передачу зарегистрированных событий (в том числе инцидентов) клиентской частью СЗИ на сервер аудита с соответствующим отображением на нем в реальном времени зарегистрированных событий. Число серверов аудита, подключаемых к клиентской части СЗИ не ограничено.

СЗИ обеспечивает возможность удаленного просмотра и фильтрации журналов (в том числе по пользователям) регистрации событий с сервера безопасности, связанных с правилами разграничения доступа.

СЗИ обеспечивает ограничение максимального размера и количества копий журналов аудита.

СЗИ обеспечивает защиту информации о событиях безопасности. При этом доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам.

СЗИ обеспечивает возможность удаленного просмотра и фильтрации журналов регистрации событий с сервера безопасности, связанных с фильтрацией пакетов.

СЗИ обеспечивает сохранение истории настроек СЗИ.

В СЗИ реализован синхронный (периодический) контроль целостности по расписанию файлов (в том числе, системных файлов, исполняемых файлов СЗИ и файлов ее настройки, файлов, используемых для хранения обрабатываемой информации) и объектов реестра ОС, с возможностью автоматического восстановления из предварительно созданных резервных копий их эталонных значений при несанкционированной модификации.

В СЗИ обеспечивается контроль целостности файлов СЗИ (исполняемых файлов СЗИ и файлов ее настройки) и объектов реестра ОС, используемых СЗИ, при загрузке системы, с возможностью автоматического восстановления из резервной копии эталонных значений контролируемых объектов СЗИ.

СЗИ обеспечивает ограничение прав пользователей по вводу информации в определенные типы объектов доступа (объекты файловой системы, объекты прикладного и специального программного обеспечения) исходя из задач и полномочий, решаемых пользователем в информационной системе.

В СЗИ обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

СЗИ обеспечивает запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые подключены к АРМ.

СЗИ обеспечивает предотвращение несанкционированного использования технологий передачи речи в информационной системе для компьютера в целом или для отдельных пользователей, посредством реализации следующих возможностей: предотвращение запуска

требуемого приложения, предотвращение подключения требуемых устройств, предотвращение взаимодействий через требуемые порты с учетом их номеров.

СЗИ обеспечивает предотвращение несанкционированного использования технологий передачи видеоинформации в информационной системе для компьютера в целом или для отдельных пользователей, посредством реализации следующих возможностей: предотвращение запуска требуемого приложения, предотвращение подключения требуемых устройств, предотвращение взаимодействий через требуемые порты с учетом их номеров.

СЗИ обеспечивает защиту архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

СЗИ обеспечивает загрузку и исполнение прикладного программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения.

СЗИ обеспечивает исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы.

СЗИ обеспечивает защиту периметра (логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

В СЗИ обеспечивает гарантированное удаление наименованных объектов – файлов с возможностью задания шаблонов и числа проходов очистки различных для различных наименованных файловых объектов (файлов, каталогов).

СЗИ предоставляет возможность гарантированного удаления создаваемых объектов – файлов с возможностью задания шаблонов и числа проходов очистки, идентифицируемых в правилах гарантированного удаления не именем файла (папки), а именем создавшего его субъекта доступа сущностью «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)», либо меткой безопасности создавшего его пользователя.

СЗИ обеспечивает синхронный (с заданным периодом) контроль запущенных в системе процессов (включая системные). При обнаружении несанкционированного процесса (не заданного администратором в качестве разрешенного для исполнения), в качестве реакции на обнаруженное событие, СЗИ автоматически завершает неразрешенный для запуска процесс.

СЗИ обеспечивает синхронный (с заданным периодом) контроль активности в системе обязательных процессов, назначаемых администратором. При обнаружении отсутствия

активности обязательного процесса, в качестве реакции на обнаруженное событие, СЗИ автоматически запускает обязательный процесс, с правами того пользователя, который будет задан администратором, включая права системы.

СЗИ обеспечивает контроль запуска процессов (приложений) с временными ограничениями – параметры запуска для процессов (приложений) в формате дата/время, задаются администратором. СЗИ обеспечивает возможность синхронного (с заданным периодом) контроля запущенных в системе процессов, для которых установлены ограничения по запуску в формате дата/время, в качестве реакции на обнаруженное несанкционированное событие (для процесса нарушены ограничения по запуску в формате дата/время), СЗИ автоматически завершает неразрешенный для запуска процесс в соответствии с заданными правилами.

СЗИ позволяет перехватывать и контролировать внедрение (инжектирование) кода и данных, производимое как с запуском отдельного потока, так и без него. Реализация этого механизма не позволит, имея права администратора, повысить привилегии до системных прав за счет внедрения кода в соответствующий системный процесс.

СЗИ позволяет контролировать и запрещать воздействие на системные службы с правами администратора различными способами.

СЗИ обеспечивает удаленное администрирование – настройку всех механизмов защиты клиентской части СЗИ с серверной части СЗИ (с сервера безопасности). Число серверов безопасности, подключаемых к клиентской части СЗИ не ограничено, синхронизируются настройки клиентской части, назначенные на серверных частях или локально.

Для запуска интерфейса сервера безопасности реализована парольная защита, предполагающая использование пароля условно-постоянного действия.

СЗИ обеспечивает аудит реального времени заданных администратором контролируемых событий всех механизмов защиты части СЗИ на сервере аудита СЗИ.

Для запуска интерфейса сервера аудита реализована парольная защита, предполагающая использование пароля условно-постоянного действия.

1.5. ИННОВАЦИИ

В СЗИ «ViPNet SafePoint» внедрены совершенно новые принципы защиты информации, например, контроль доступа (дискреционный и на основе меток безопасности) к создаваемым файлам (в разграничительной политике доступа к файловым объектам, файлы подразделены на создаваемые в процессе функционирования системы, используемые для хранения информации, к которым и имеет смысл реализовывать принцип контроля доступа на основе меток безопасности, и системные, присутствующие на момент реализации разграничительной политики доступа).

Механизм контроля доступа к создаваемым файлам позволяет не только принципиально упростить задачу администрирования, обеспечить, что строго доказано, реализацию корректной разграничительной политики доступа, но обеспечить возможность реализации принципиально новых возможностей защиты, направленных на нейтрализацию в информационной системе наиболее актуальных угроз, таких, как атаки на уязвимости приложений, атаки на приложения, наделяемые вредоносными свойствами, за счет прочтения ими вредоносных файлов (например, скриптовых), реализовать эффективную защиту от хищения обрабатываемой конфиденциальной информации санкционированными пользователями (инсайдерами), в том числе, с использованием сетевых ресурсов – в данном случае крайне важна возможность реализации разграничительной политики доступа процессов (приложений) к буферу обмена, и многое другое. Очень важно то, что эти актуальные задачи защиты решаются реализацией простейших разграничительных политик доступа к файловым объектам.

В СЗИ «ViPNet SafePoint» принципиально изменены принципы построения, как следствие, возможности и широко используемых на практике механизмов защиты. Принципиально изменена собственно парадигма защиты информации от несанкционированного доступа – защита строится в предположении, что угрозу несанкционированного доступа к информации может нести в себе не только пользователь, но и (если не в первую очередь) процесс (приложение). Поскольку в ОС все процессы (приложения) запускаются с правами запустившего их пользователя (наследуют права доступа пользователя к ресурсам), т.е. права доступа всех процессов (приложений), запущенных одним и тем же пользователем, совпадают, в СЗИ «ViPNet SafePoint» реализована возможность реализации различной разграничительной политики доступа к защищаемым ресурсам для различных процессов (приложений), что позволяет эффективно решать принципиально новые задачи защиты информации. В частности, в механизмах дискреционного контроля доступа к защищаемым ресурсам (файловые объекты, объекты реестра ОС, принтеры, буфер обмена и др.) в качестве субъекта доступа в разграничительной политике одновременно выступают три сущности: исходный идентификатор (SID) пользователя, эффективный идентификатор пользователя, полнопутевое имя процесса (имя исполняемого файла процесса). Для упрощения задачи администрирования субъекты доступа могут задаваться масками. При разграничении доступа к защищаемым ресурсам для подобным способом заданного субъекта доступа, СЗИ «ViPNet SafePoint» может решаться множество актуальных задач защиты информации, в частности может быть полностью изолирована работа отдельных критичных приложений.

Принципиальной особенностью реализации механизмов контроля доступа в СЗИ «ViPNet SafePoint» является и то, что права доступа назначаются субъектам, а не присваиваются в качестве атрибутов объектам доступа. Объекты доступа, при назначении правил разграничительной

политики, могут, в том числе, задаваться масками и переменными среды окружения. Это принципиально упрощает настройку механизмов защиты, обеспечивает наглядность представления в интерфейсе реализованной разграничительной политики доступа, и наделяет их принципиально новыми возможностями. Например, при реализации контроля доступа к файловым объектам, объекты могут задаваться расширениями файлов, что позволяет реализовать разграничительную политику доступа в отношении файлов определенных типов – исполняемых, скриптовых и т.д.

Важнейшей особенностью построения СЗИ «ViPNet SafePoint» является и реализация ряда мер, направленных на обеспечение корректности реализации разграничительной политики доступа и дополнительная защита от ее обхода. В частности, основным механизмом обеспечения корректности реализации разграничительной политики доступа к файловым объектам является механизм разделения между субъектами доступа объектов, не разделяемых системой и приложениями. При отсутствии подобного технического решения о корректности контроля доступа в современных информационных системах говорить невозможно. Примерами механизмов защиты, направленных на защиту от обхода разграничительной политики доступа, являются механизм разграничения прав доступа субъектов (пользователь и процесс) к сервисам олицетворения, предоставляемых ОС – штатная возможность современных ОС, предоставляющая возможность повысить привилегии пользователя, и механизм контроля (разграничения прав) субъектов в части возможности прямого доступа к дискам (к любым дискам, включая жесткий диск и внешние накопители).

Важнейший механизм защиты – механизм управления монтированием устройств, включая возможность их идентификации по серийным номерам, позволяет монтировать к системе (отмонтировать от системы) устройства с учетом активности (регистрации в системе) конкретных пользователей. Именно применение данного механизма защиты позволяет корректно реализовать различные режимы обработки пользователями различной информации, в частности, категорируемой, в различных режимах, требующих использования различных устройств.

В СЗИ «ViPNet SafePoint» реализована возможность реализации сессионного контроля доступа, позволяющая работать одному и тому же сотруднику на одном и том же компьютере с информацией различных уровней конфиденциальности, посредством реализации обработки информации различных уровней конфиденциальности под различными учетными записями в различных режимах обработки. Простота настройки разграничительной политики доступа при этом обеспечивается реализацией в СЗИ «ViPNet SafePoint» механизма контроля доступа на основе меток безопасности к создаваемым файлам, требующего задания меток безопасности только для пользователей (не требуется разметки файловых объектов).

Здесь перечислены далеко не все отличительные особенности СЗИ «ViPNet SafePoint», позволяющие ее позиционировать, как инновационную систему защиты. Акцент сделан лишь на наиболее значимых технических решениях.

Механизмы защиты СЗИ «ViPNet SafePoint» работают совместно с механизмами защиты, предусмотренными ОС Microsoft Windows. Для того чтобы доступ к объекту был разрешен субъекту, разрешающие правила должны быть заданы как СЗИ «ViPNet SafePoint», так и средствами ОС. Запреты доступа функционируют, если хотя бы одним из механизмов (механизмы из состава СЗИ или механизмы защиты, предусмотренные ОС) доступ субъекта к объекту запрещен.

1.6. ТРЕБОВАНИЯ К ПРОГРАММНОМУ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

СЗИ «ViPNet SafePoint» может быть установлена на персональные компьютеры, портативные ПК (ноутбуки), серверы (файловые, контроллеры домена, терминального доступа) и виртуальные машины, работающие как в автономном режиме, так и в составе локальной вычислительной сети.

СЗИ «ViPNet SafePoint» может использоваться на рабочих местах под управлением следующих ОС семейства Microsoft Windows:

- Microsoft Windows 10 (64-разрядная), работоспособность и выполнение всех заявленных возможностей гарантируется при использовании версий 1803, 1809;
- Microsoft Windows 8.1 (64-разрядная);
- Microsoft Windows Server 2012 R2 (Standard или Datacenter);
- Microsoft Windows Server 2016 (Standard или Datacenter), работоспособность и выполнение всех заявленных возможностей гарантируется при использовании версий 1607, 1709, 1803, 1809.

Для размещения файлов системы и ее работы требуется не менее 50 Мбайт пространства на системном разделе жесткого диска. Для использования СЗИ «ViPNet SafePoint» на компьютере в составе ЛВС необходимо установить сетевой протокол TCP/IP.

Для использования аппаратных идентификаторов требуется наличие в аппаратной части ПК соответствующих портов: USB-порта.

2. УСТАНОВКА И УДАЛЕНИЕ

2.1. СОСТАВ ДИСТРИБУТИВА

Дистрибутив СЗИ «ViPNet SafePoint» для ОС Microsoft Windows для 64х разрядной системы **safepoint_x64.msi** включает в себя следующие компоненты:

- Клиентская часть СЗИ «ViPNet SafePoint»;
- Сервер безопасности СЗИ «ViPNet SafePoint»;
- Сервер Аудита СЗИ «ViPNet SafePoint».

2.2. УСТАНОВКА И УДАЛЕНИЕ КЛИЕНТСКОЙ ЧАСТИ СЗИ

Установка клиентской части СЗИ

СЗИ «ViPNet SafePoint» имеет оконный графический интерфейс. Установка программы производится с CD-ROM диска или другого носителя, на котором он поставляется. Программа поставляется в виде стандартного дистрибутива.

Для инсталляции необходимо работать под учетной записью администратора (локального или доменного), обладающего правами на запись в реестр и запись драйверов.

Запуск СЗИ «ViPNet SafePoint» производится из каталога, куда было установлено средство защиты. Ярлыки в панели «Пуск» автоматически **не** создаются.

В случае использования иных средств защиты, в первую очередь антивирусных средств, перед установкой СЗИ «ViPNet SafePoint» рекомендуется отключить данные средства защиты для корректного прохождения процедуры инсталляции СЗИ «ViPNet SafePoint».

Для установки клиентской части СЗИ «ViPNet SafePoint» необходимо:

1. Запустить установочный файл **safepoint_x64.msi**.
2. Нажать кнопку «Далее» (рис.2.2.1).

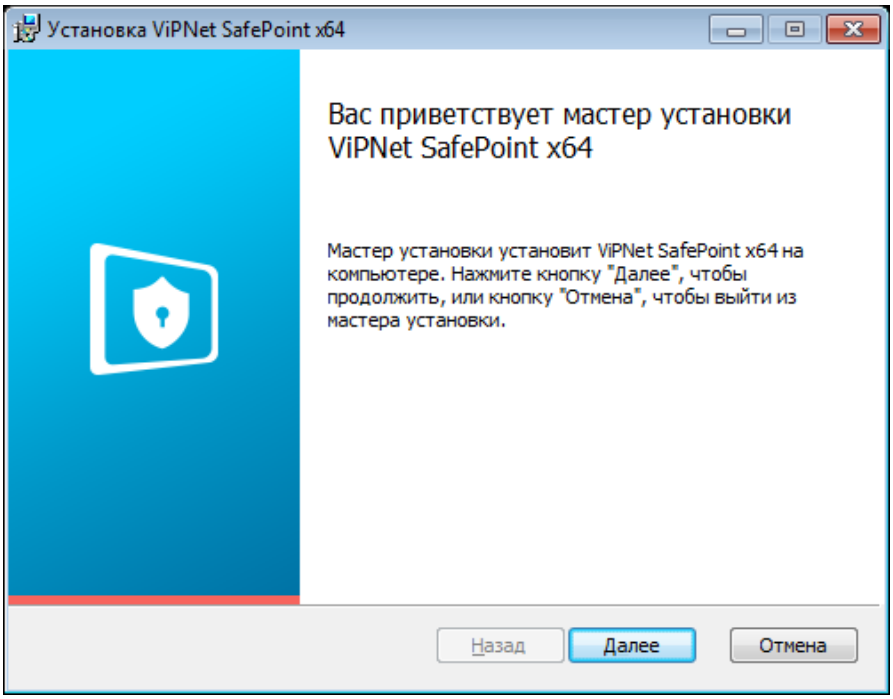


Рис.2.2.1. Окно мастера установки СЗИ "ViPNet SafePoint"

3. В появившемся окне выбрать нужный вариант (рис.2.2.2):

   Обычная установка – устанавливается только клиентская часть;

   Выборочная установка – дает возможность выбрать компоненты, которые будут установлены;

   Полная установка – устанавливаются все компоненты СЗИ «ViPNet SafePoint».

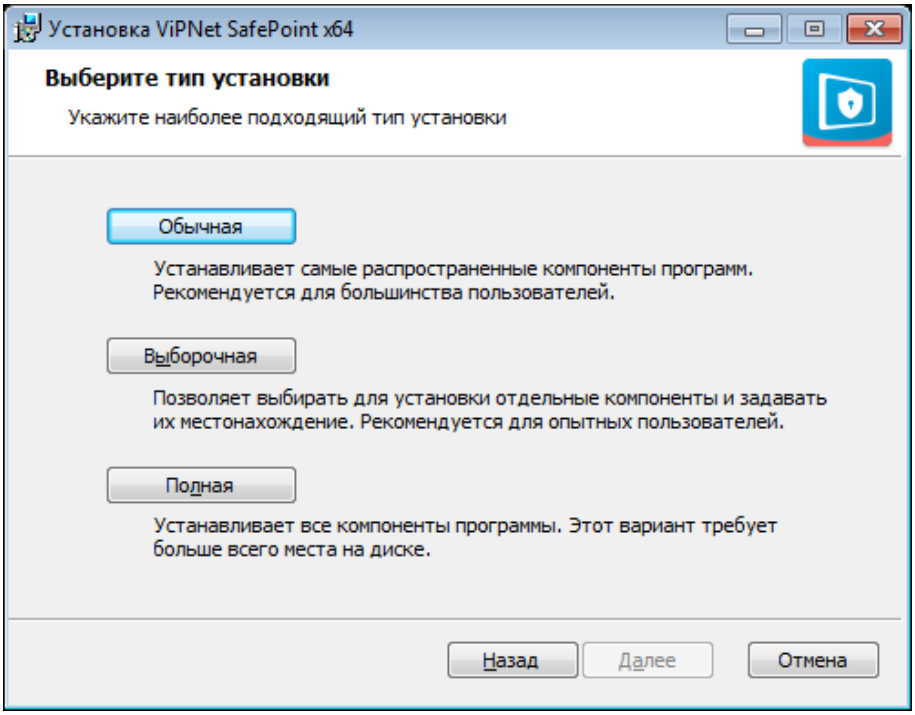


Рис.2.2.2. Окно мастера установки СЗИ «ViPNet SafePoint». Выбор типа установки

4. В следующем окне выбрать каталог установки, воспользовавшись кнопкой «Обзор» (по умолчанию СЗИ «ViPNet SafePoint» устанавливается на системный диск в каталог «Program Files\INFOTECS\VIPNET SAFEPOINT\») (рис.2.2.3) и необходимые компоненты (рис.2.2.4). Для установки клиентской части СЗИ «ViPNet SafePoint» необходимо установить Общие компоненты (необходимые общие компоненты СЗИ «ViPNet SafePoint»), Клиент (Клиентская часть СЗИ «ViPNet SafePoint»). Нажать «Далее».

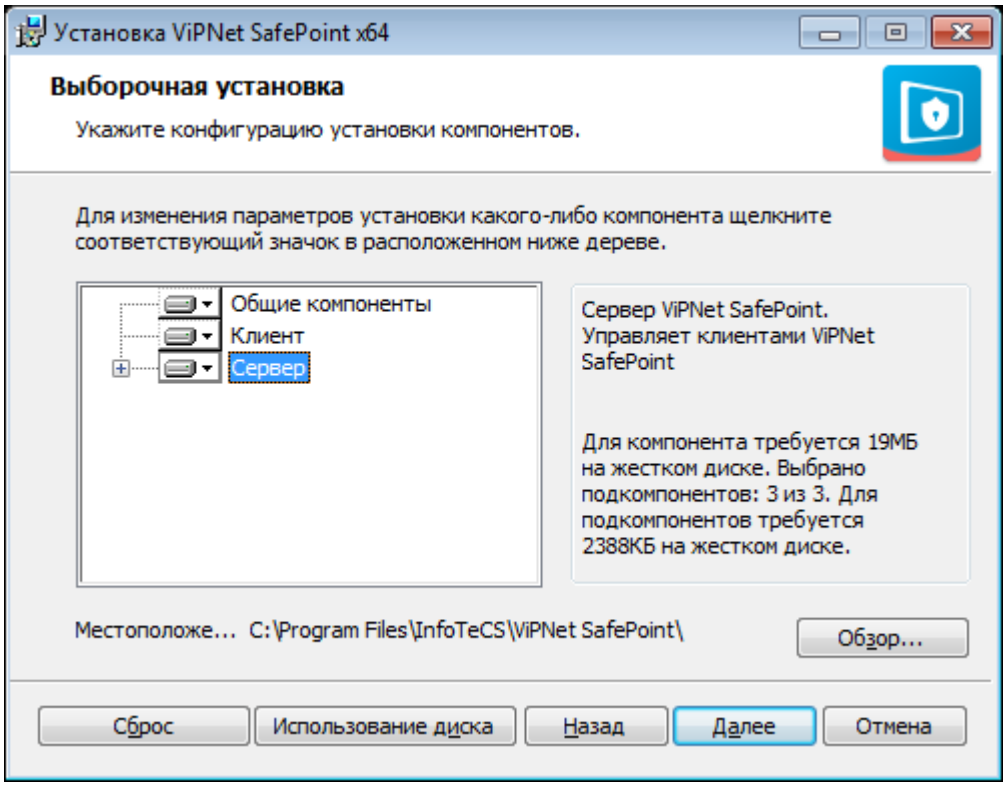


Рис.2.2.3. Окно мастера установки СЗИ «ViPNet SafePoint». Выбор компонент для установки

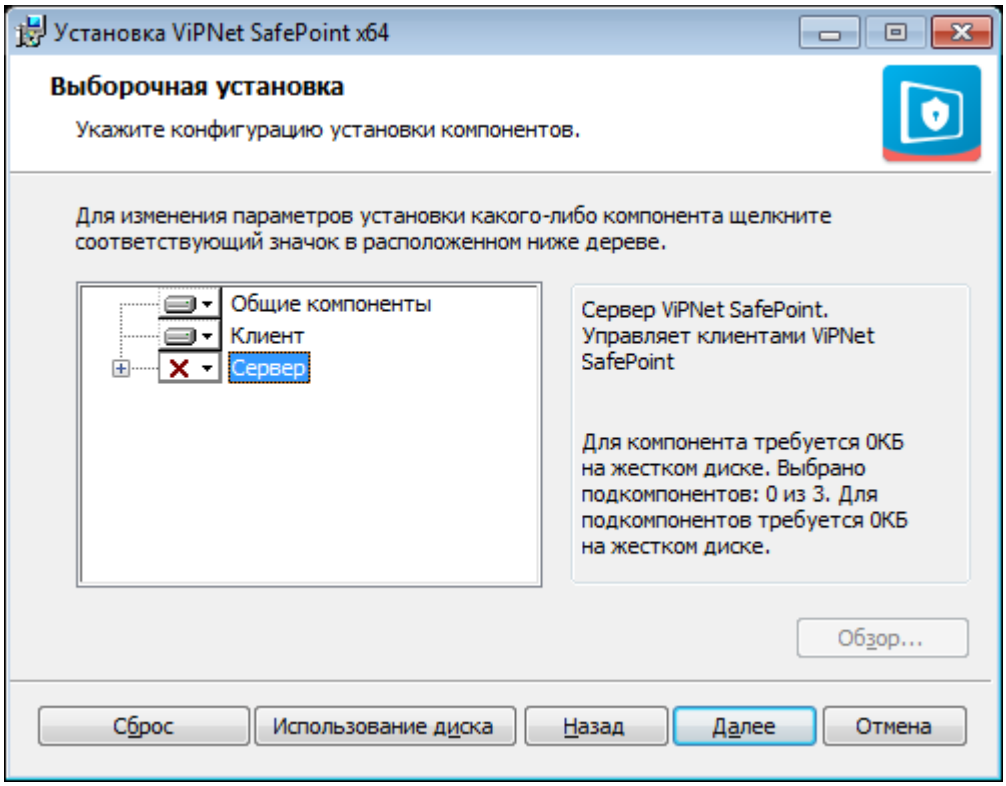


Рис.2.2.4. Окно мастера установки СЗИ «ViPNet SafePoint». Выбранные компоненты для установки

5. В следующем появившемся окне подтвердить факт установки, нажав кнопку «Установить».
6. В следующем появившемся окне нажать кнопку «Готово».

Если устанавливаются и клиентская часть и сервер безопасности СЗИ «ViPNet SafePoint» на один АРМ, и при этом сервер безопасности выполняет роль главного по пользователям домена, то при установке СЗИ «ViPNet SafePoint» до перезагрузки компьютера необходимо установить 1-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config), т.е. добавить 2 к имеющемуся значению.

7. При необходимости управления доменными пользователями с использованием клиентской части необходимо установить 3-й бит в значении параметра реестра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config), т.е. добавить 8 к имеющемуся значению.

Параметр реестра HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config (DWORD) создается при установке СЗИ «ViPNet SafePoint» равным «0», значение следует изменять в ходе установки до перезагрузки ОС. Он отвечает за настройку конкретного экземпляра СЗИ «ViPNet

SafePoint». Представляет собой целочисленное значение, где каждый бит – флаг.

Бит 0 (*десятичное значение – «1»*) – если флаг установлен, то в интерфейсе Управления настройками пропадает всё, что связано с сервером аудита (пропадают флаги «Фиксировать «какое-либо событие» на сервере аудита» и настройки соединения с сервером аудита).

Бит 1 (*десятичное значение – «2»*) – если флаг установлен, то сервер безопасности выполняет роль главного по пользователям домена.

Бит 2 (*десятичное значение – «4»*) – если флаг установлен, то в интерфейсе Управления настройками отключается всё, что связано с мандатным управлением доступа.

Бит 3 (*десятичное значение – «8»*) – если флаг установлен, то разрешено управление доменными пользователями с использованием интерфейса клиентской части.

Бит 4 (*десятичное значение – «16»*) – если флаг установлен, то клиентская часть СЗИ «ViPNet SafePoint» не выполняет команды с сервера безопасности и сервера аудита об удаленном управлении ФС и реестром (обзор и действия в нем), остановом и запуском программ.

Если необходимо установить несколько флагов, то следует сложить десятичные значения и присвоить параметру данное суммарное значение.

8. В появившемся окне с вопросом о перезагрузке компьютера выбрать нужный вариант (перезагрузка компьютера может быть осуществлена сразу автоматически или вручную администратором, после завершения остальных текущих задач на компьютере).

Клиентская часть СЗИ «ViPNet SafePoint» состоит из двух частей – функциональная и диалоговая (интерфейсная). Функциональная часть устанавливается в качестве сервиса операционной системы (ОС) и не нуждается в действиях оператора (основной режим запуска СЗИ «ViPNet SafePoint»). Все действия, связанные с настройкой функциональной части, изменениями настроек, списков процессов и пользователей, выполняются с помощью диалоговой части программного комплекса.

Удаление клиентской части СЗИ «ViPNet SafePoint»

Перед удалением СЗИ «ViPNet SafePoint» необходимо остановить работу службы СЗИ.

В случае использования иных средств защиты, в первую очередь антивирусных средств, перед удалением СЗИ «ViPNet SafePoint» рекомендуется отключить данные средства защиты для корректного прохождения процедуры удаления СЗИ «ViPNet SafePoint».

Для удаления клиентской части СЗИ «ViPNet SafePoint» следует:

1. Запустить установочный файл **safepoint_x64.msi**.
2. Нажать кнопку «Далее» (рис.2.2.6).

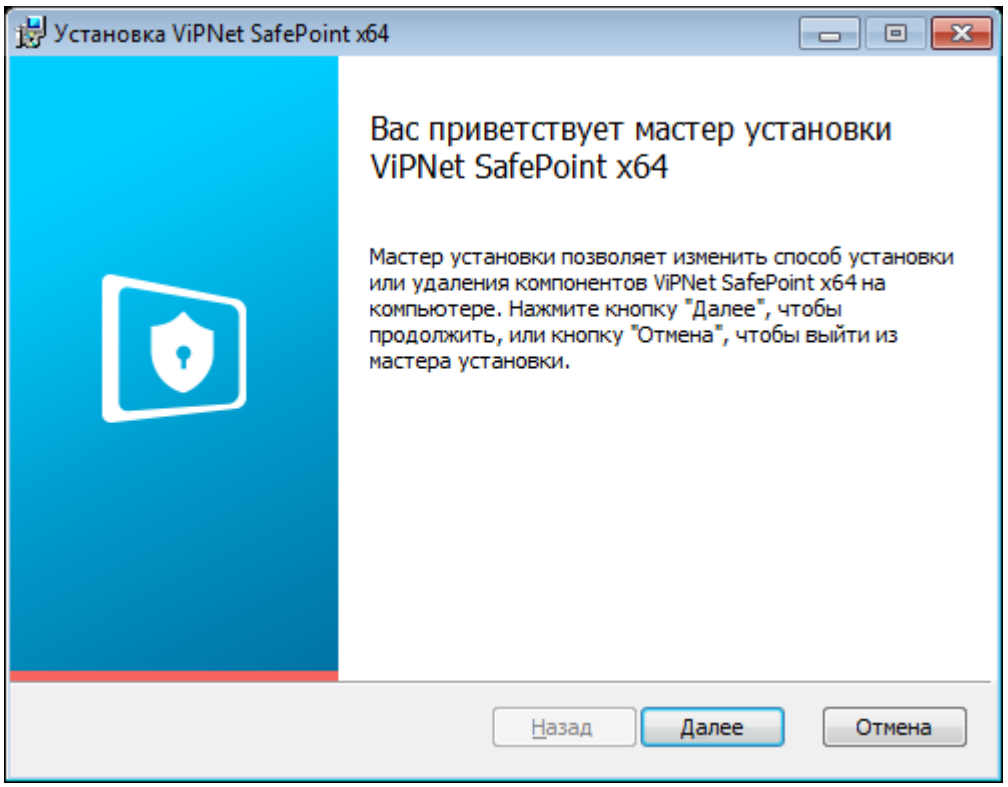


Рис.2.2.6. Окно мастера изменения компонентов СЗИ «ViPNet SafePoint»

3. В новом окне выбрать пункт «Удалить» (рис.2.2.7).

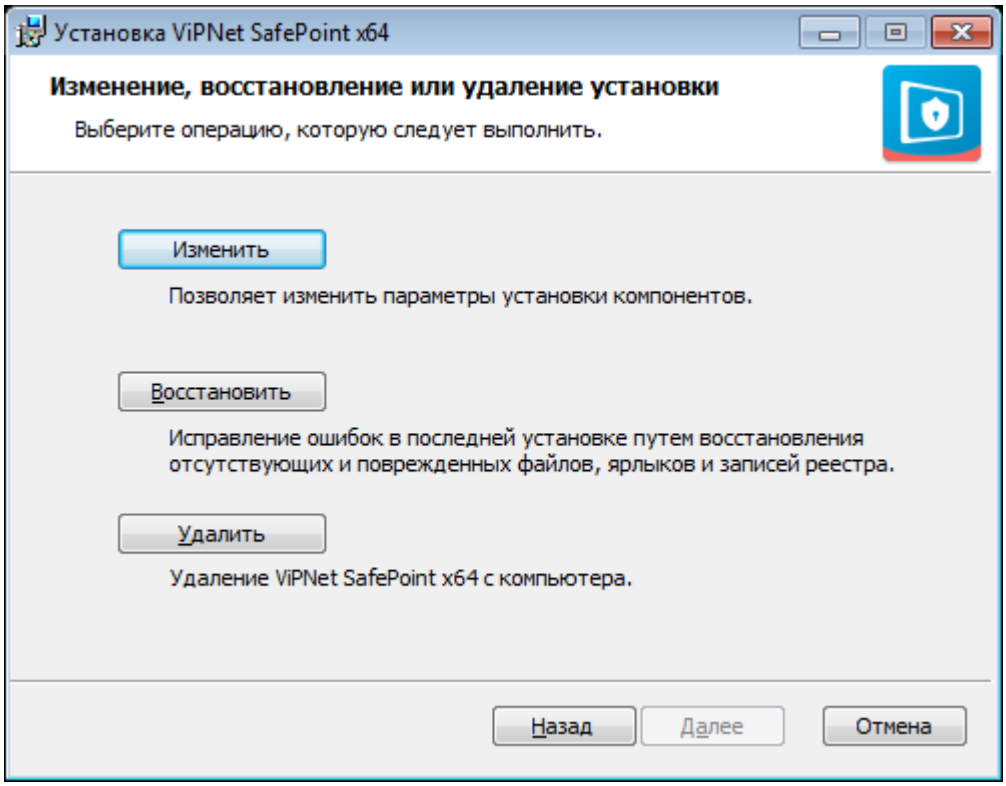


Рис.2.2.7. Окно выбора варианта изменения компонентов

4. В следующем появившемся окне подтвердить удаление, нажать кнопку «Удалить».
5. В появившемся окне нажать «ОК».
6. В следующем появившемся окне нажать кнопку «Готово».
7. В появившемся окне с вопросом о перезагрузке компьютера выбрать нужный вариант.

2.3. СОСТАВ УСТАНОВЛЕННОГО ПО

Каталог «..\INFOTECS\VIPNET SAFEPOINT», в который была произведена установка программы, содержит драйверы и библиотеки, необходимые для работы СЗИ «ViPNet SafePoint», исполняемые файлы, файлы настроек и журналов аудита СЗИ «ViPNet SafePoint». В зависимости от выбранных для установки компонентов СЗИ «ViPNet SafePoint» структура и содержимое каталога «..\INFOTECS\VIPNET SAFEPOINT» могут изменяться, данный раздел относится к составу клиентской части СЗИ «ViPNet SafePoint». Структура каталога «..\INFOTECS\VIPNET SAFEPOINT» представлена на рис.2.3.1.

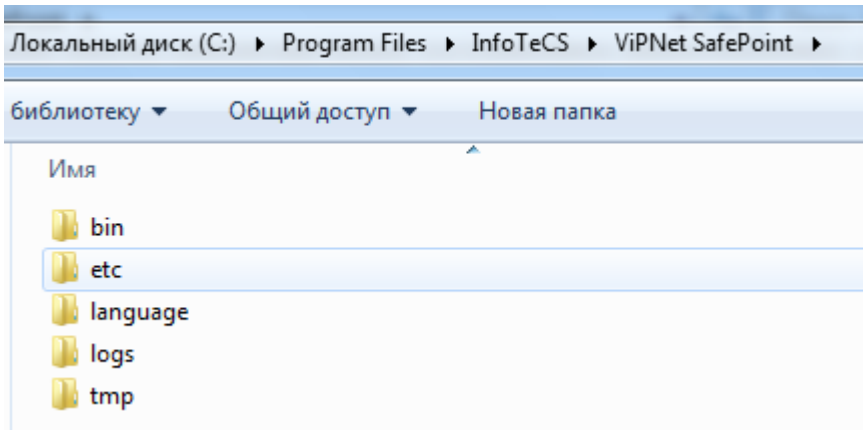


Рис.2.3.1. Структура каталога «..\INFOTECS\VIPNET SAFEPOINT»

Драйверы и библиотеки, отвечающие за реализацию механизмов СЗИ «ViPNet SafePoint», а также вспомогательные утилиты, хранятся в каталоге «bin». Структура каталога «bin» представлена на рис.2.3.2.

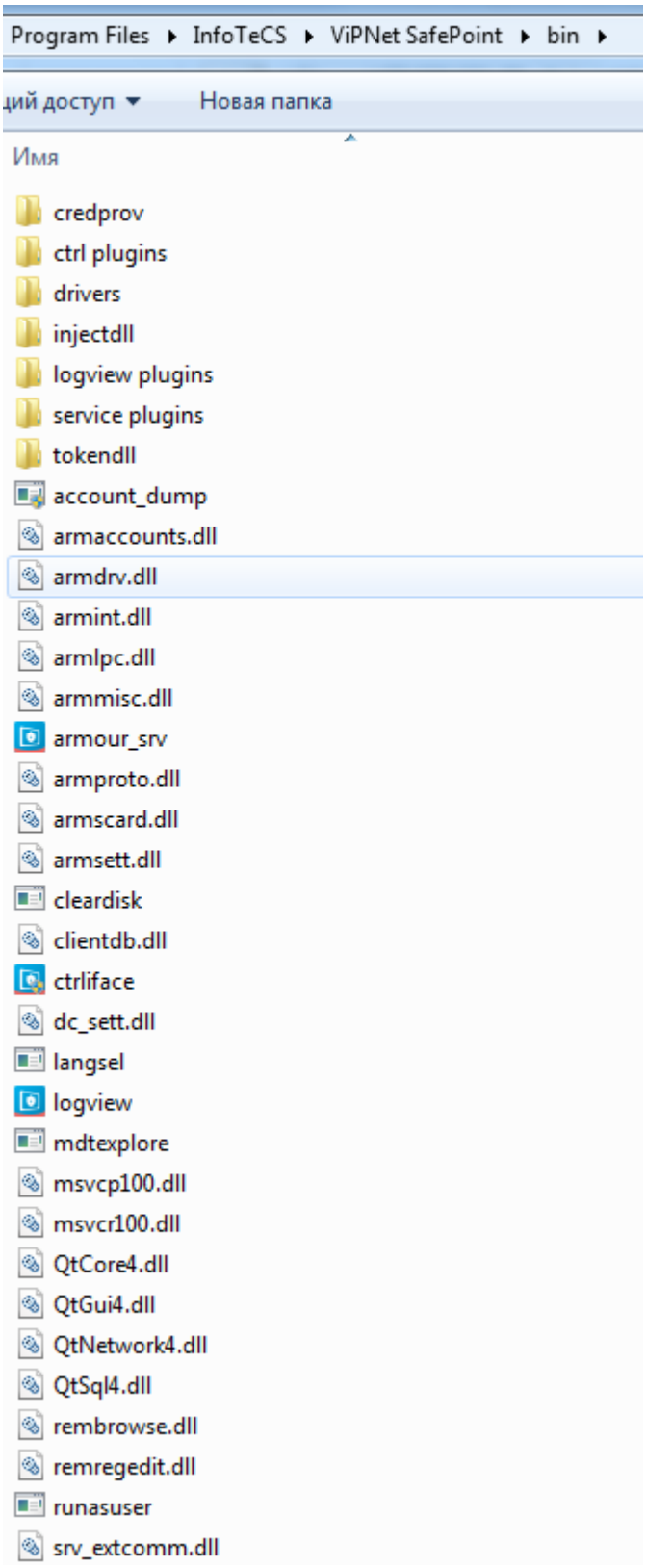


Рис.2.3.2. Структура каталога «..\INFOTECS\VIPNET SAFEPOINT\bin»

Ниже приведено назначение основных файлов из состава СЗИ «ViPNet SafePoint».

В каталоге «credprov» находятся библиотеки, необходимые для интерактивной аутентификации пользователя:

ArmourCredentialProvider.dll	Провайдер входа с консоли
ArmourSCardProvider.dll	Провайдер входа с помощью смарт-карт

Каталог «Ctrl plugins» содержит плагины, необходимые для работы интерфейса управления настройками:

acc_Ctrlplg.dll	механизм идентификации и аутентификации пользователя
cb_Ctrlplg.dll	механизм управления доступом к буферу обмена
cfo_Ctrlplg.dll	механизм контроля доступа к создаваемым файлам
cm_Ctrlplg.dll	механизм гарантированного удаления и очистки памяти, очистка ОЗУ
dc_Ctrlplg.dll	механизм управления монтированием устройств
dda_Ctrlplg.dll	механизм защиты от скрытых действий пользователей, контроль прямого доступа к дискам
fc_Ctrlplg.dll	механизм контроля доступа к статичным файловым объектам
imp_Ctrlplg.dll	механизм защиты от скрытых действий пользователей, контроль олицетворения
inj_Ctrlplg.dll	механизм управления внедрением кода и данных
int_Ctrlplg.dll	механизм контроля целостности
net_Ctrlplg.dll	сетевые настройки клиента
pc_Ctrlplg.dll	механизм контроля целостности, контроль процессов
prf_Ctrlplg.dll	профили субъектов доступа
prn_Ctrlplg.dll	механизмы контроля (разграничения) прав доступа, контроль доступа к принтерам
rc_Ctrlplg.dll	механизм контроля доступа к объектам реестра
rot_Ctrlplg.dll	ротация файлов журнала аудита
subj_Ctrlplg.dll	субъекты доступа
svc_Ctrlplg.dll	механизм управления доступа к службам

Каталог «drivers» содержит драйверы, необходимые для работы СЗИ «ViPNet SafePoint»:

armdrv3.sys	основной драйвер СЗИ «ViPNet SafePoint»;
cleanmem.sys	драйвер управления механизмом гарантированного удаления и очистки памяти, очистка ОЗУ
devCtrl3.sys	драйвер управления механизмом управления

	монтированием устройств
fileCtrl3.sys	драйвер управления механизмом контроля доступа к объектам файловой системы
regCtrl3.sys	драйвер управления механизмом контроля доступа к объектам реестра

В каталоге «injectdll» хранятся библиотеки для внедрения во все работающие процессы системы, библиотеки выполняют перехват некоторых функций и реализуют различные механизмы защиты:

cbhook.dll	механизм управления доступом к буферу обмена
filehook.dll	механизм защиты от скрытых действий пользователей, контроль прямого доступа к дискам
hookldr.dll	загрузка библиотек механизмов защиты
imphook.dll	механизм защиты от скрытых действий пользователей, контроль олицетворения и запуска "от имени"
injhook.dll, injhook2.dll	механизм управления внедрением кода и данных
prnhook.dll	механизмы контроля (разграничения) прав доступа, контроль доступа к принтерам
svchook.dll	механизм управления доступа к службам

Библиотеки, необходимые для работы Просмотрщика журналов аудита, находятся в каталоге «logview plugins»:

acc_logplg.dll	журнал входа/выхода пользователей
cb_logplg.dll	журнал управления доступом к буферу обмена
cm_logplg.dll	журнал очистки оперативной памяти
dc_logplg.dll	журнал управления подключением устройств
dda_logplg.dll	журнал управления прямым доступом к дискам
fc_logplg.dll	журнал доступа к файловой системе
imp_logplg.dll	журнал управления олицетворением
inj_logplg.dll	журнал управления внедрением исполняемого кода и данных
int_logplg.dll	журнал контроля целостности
pc_logplg.dll	журнал управления процессами
prn_logplg.dll	журнал управления доступом к принтерам
rc_logplg.dll	журнал управления доступом к реестру

srv_logplg.dll	журнал служебных событий «ViPNet SafePoint»
svc_logplg.dll	журнал управления доступа к службам

Каталог «service plugins» содержит плагины, управляющие и/или реализующие механизмы защиты СЗИ:

cb_srvplg.dll	механизм управления доступом к буферу обмена
cm_srvplg.dll	механизм гарантированного удаления и очистки памяти, очистка ОЗУ
dc_srvplg.dll	механизм управления монтированием устройств
dda_srvplg.dll	механизм защиты от скрытых действий пользователей, контроль прямого доступа к дискам
fc_srvplg.dll	механизм контроля доступа к объектам файловой системы
imp_srvplg.dll	механизм защиты от скрытых действий пользователей, контроль олицетворения
inj_srvplg.dll	механизм управления внедрением кода и данных
int_srvplg.dll	механизмы контроля целостности
pc_srvplg.dll	механизм контроля целостности, контроль процессов
prn_srvplg.dll	механизмы контроля (разграничения) прав доступа, контроль доступа к принтерам
rc_srvplg.dll	механизм контроля доступа к объектам реестра
svc_srvplg.dll	механизм управления доступа к службам

В каталоге «tokendll» содержатся библиотеки работы с электронными ключами и смарт-картами.

В каталоге «bin» хранятся исполняемые файлы основных компонентов и общие для всех компонентов комплекса библиотеки:

armour_srv.exe	служба СЗИ «ViPNet SafePoint»
Ctrliface.exe	интерфейс управления настройками
logview.exe	просмотрщик журналов аудита
armaccounts.dll	функции работы с учетными записями пользователей СЗИ «ViPNet SafePoint»
armdrv.dll	доступ к функциям драйвера armdrv для приложений
armint.dll	функции поддержки механизма собственной целостности СЗИ

armlpc.dll	классы и функции для использования механизма LPC
armmisc.dll	общее: пути к компонентам СЗИ, получение хеш-функций данных, работа с файлами
armproto.dll	протокол взаимодействия клиент-сервер
armscard.dll	функции работы с электронными ключами и смарт-картами
armsett.dll	функции работы с общими настройками СЗИ «ViPNet SafePoint»
clientdb.dll	функции работы с БД клиента на сервере безопасности
dc_sett.dll	функции работы с настройками механизма управления подключением устройств
rembrowse.dll	диалоги удаленного обзора объектов файловой системы
remregedit.dll	диалоги удаленного обзора объектов реестра
srv_extcomm.dll	поддержка взаимодействия «приложение ↔ сервер ↔ клиент»
account_dump.exe	формирует и синхронизирует БД учетных записей СЗИ «ViPNet SafePoint» и ОС
cleardisk.exe	реализует механизм очистки устройств хранения данных
langsel.exe	выбор языка для СЗИ «ViPNet SafePoint»
mdtexplore.exe	обзор разметки файлов
runasuser.exe	запуск от имени пользователя, прошедшего аутентификацию

В каталоге «etc» содержатся файлы настроек СЗИ «ViPNet SafePoint»:

Учетные записи	
accounts.conf	настройки механизма идентификации и аутентификации пользователя, настройка параметров паролей
*.accounts.db	база данных пользователей (локальных или доменных)
mdtlevels.conf	список уровней доступа
Управление олицетворением	
impCtrl.conf	настройки механизма управления олицетворением
Субъекты доступа	
subjects.conf	заведенные субъекты доступа

Профили	
profiles.conf	настройки профилей; правила доступа, заданные для профилей в механизмах: управления доступом к статичным объектам ФС; управления прямым доступом к дискам; управления доступом к реестру; управления доступом к принтерам
Управление доступом к статичным объектам ФС	
filecontrol.conf	настройки механизма управления доступом к статичным файловым объектам
fs_objs.conf	заведенные статичные файловые объекты
secuwipe.conf	настройки механизма гарантированного удаления статичных файловых объектов
cleardisk.conf	настройки механизма полной очистки дисков
Управление доступом к создаваемым файлам	
cfo.conf	настройки механизма управления доступом к создаваемым файлам
cfo_markinglock.conf	настройки механизма ограничения доступа
cfo_secuwipe.conf	настройки механизма гарантированного удаления создаваемых файлов
Управление прямым доступом к дискам	
ddaCtrl.conf	настройки механизма управления прямым доступом к диску
Управление доступом к объектам реестра	
reg_objs.conf	заведенные объекты реестра, механизм управления доступом к объектам реестра
Управление доступом к принтерам	
printers.conf	заведенные принтера, механизм управления доступом к принтерам
Управление доступом к службам	
svcCtrl.conf	настройки механизма управления доступом к службам
Управление устройствами	
devCtrl.conf	настройки механизма управления монтированием

	устройств
devices.conf	контролируемые устройства механизмом управления монтированием устройств
Управление доступом к буферу обмена	
clipboard.conf	настройки механизма управления доступом к буферу обмена
Управление внедрением кода и данных	
injprot.conf	настройки механизма управления внедрением кода и данных
Очистка ОЗУ	
cleanmem.conf	настройки механизма очистки ОЗУ
Управление процессами	
procCtrl.conf	настройки механизма управления процессами
Контроль целостности	
backupfile.db	настройки механизма контроля целостности, резервные копии файловых объектов
backupreg.db	настройки механизма контроля целостности, резервные копии объектов реестра
Настройки ротации	
alog.conf	настройки ротации журналов аудита
Настройки сети	
aproto.conf	настройки взаимодействия клиентской части с сервером(ами) безопасности
alognet.conf	настройки взаимодействия клиентской части с сервером(ами) аудита

Также в этом каталоге хранится история изменения настроек в виде скрытых файлов и каталог «db», содержащий базы данных для работы механизмов контроля целостности.

В каталоге «language» хранятся файлы для изменения языка на английский или на русский.

В каталоге «logs» хранятся журналы аудита и их копии.

2.4. ПРОВЕРКА КОРРЕКТНОСТИ УСТАНОВКИ

После перезагрузки системы, для проверки корректности установки необходимо убедиться в том, что в просмотрщике локальных служб (меню «Пуск» → Панель управления → Администрирование → Службы) появились службы:

- **armour service – основная служба, управляет механизмами защиты**

В поле «Состояние» должно быть «Работает», в поле «Тип запуска» должно быть «Автоматически».

В диспетчере задач, во вкладке «процессы» должны присутствовать:

- **armor_srv.exe – основная служба**

В системных драйверах (команда Windows «msinfo32») должны присутствовать драйвера:

1. Основной драйвер СЗИ «ViPNet SafePoint» **armdrv3**:
    - В поле «Работает» должно быть «Да»;
    - В поле «Состояние» должно быть «Работает»;
    - В реестре должен появиться раздел:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\armdrv3.
2. Драйвер управления доступом к файловой системе **fileCtrl3**:
    - В поле «Работает» должно быть «Да»;
    - В поле «Состояние» должно быть «Работает»;
    - В реестре должен появиться раздел:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\fileCtrl3.
3. Драйвер управления доступом к реестру **regCtrl3**:
    - В поле «Работает» должно быть «Да»;
    - В поле «Состояние» должно быть «Работает»;
    - В реестре должен появиться раздел:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\regCtrl3.
4. Драйвер управления подключением **devCtrl3**:
    - В поле «Работает» должно быть «Да»;
    - В поле «Состояние» должно быть «Работает»;
    - В реестре должна появиться запись:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\devCtrl3.
5. Драйвер очистки оперативной памяти **clearmem**:
    - В поле «Работает» должно быть «Да»;
    - В поле «Состояние» должно быть «Работает»;
    - В реестре должна появиться запись:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ClearMEM.

СЗИ «ViPNet SafePoint» не отображается в списке установленных программ (меню «Пуск» → «Панель управления» → «Программы» → «Программы и компоненты»).

При работе с ОС Windows 8 и выше команда Windows «msinfo32» может не отображать часть драйверов СЗИ «ViPNet SafePoint». В таком случае, для проверки корректности установки необходимо воспользоваться командной строкой (cmd), запущенной от имени администратора, и командой «net start имя_драйвера» проверить, запущен ли он.

3. ИНТЕРФЕЙС КЛИЕНТСКОЙ ЧАСТИ

3.1. ПЕРВЫЙ ЗАПУСК ИНТЕРФЕЙСА КЛИЕНТСКОЙ ЧАСТИ

Для запуска интерфейса клиентской части СЗИ «ViPNet SafePoint» необходимо запустить файл Ctrliface.exe в каталоге установленной СЗИ «ViPNet SafePoint» «..\INFOTECS\VIPNET SAFEPOINT\bin» (рис.3.1.1, рис.3.1.2).

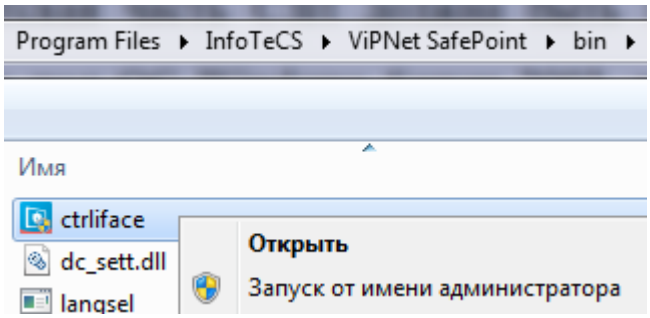


Рис.3.1.1. Запуск с помощью файла Ctrliface.exe интерфейса клиентской части СЗИ «ViPNet SafePoint»

При первом запуске СЗИ «ViPNet SafePoint» предложит завести пароль на запуск интерфейса. При этом появится дополнительное сообщение (рис.3.1.3).

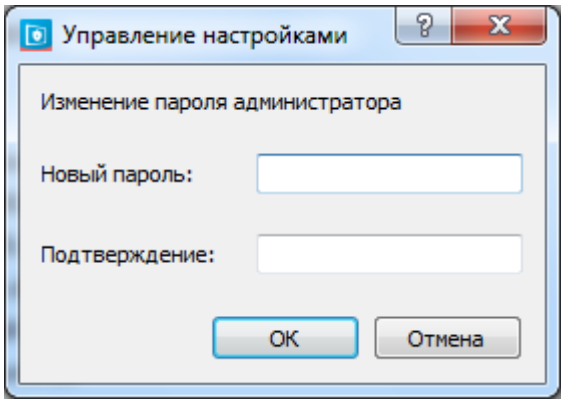


Рис.3.1.3. Окно ввода пароля

Возможно отключить парольную защиту, оставив поля «Новый пароль» и «Подтверждение» пустыми. В появившемся окне подтвердить отключение парольной защиты (рис.3.1.4).

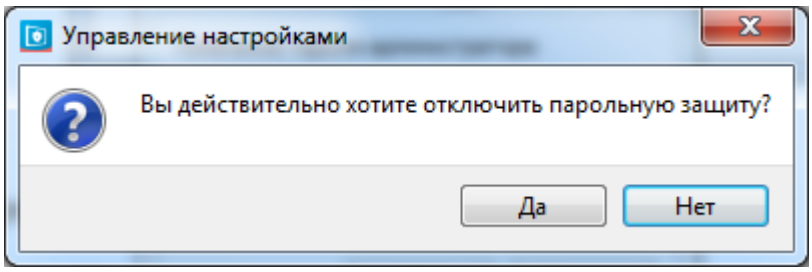


Рис.3.1.4. Окно подтверждения отключения парольной защиты

Данный пароль хранится в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT Control Interface\Administrator password». Если пароль был забыт, необходимо удалить параметр «Administrator password». После этого при запуске СЗИ «ViPNet SafePoint» будет предложено ввести новый пароль.

После настройки парольной защиты запустится интерфейс СЗИ «ViPNet SafePoint».

3.2. СТРУКТУРА ИНТЕРФЕЙСА КЛИЕНТСКОЙ ЧАСТИ. ОСНОВНОЕ МЕНЮ

По умолчанию СЗИ «ViPNet SafePoint» включает в себя ряд настроек, установленных «по умолчанию» с целью реализации корректного функционирования системы, а также для иллюстрации возможностей СЗИ «ViPNet SafePoint» по настройке механизмов защиты.

На рис.3.2.1. представлена структура интерфейса клиентской части СЗИ «ViPNet SafePoint», содержащего:

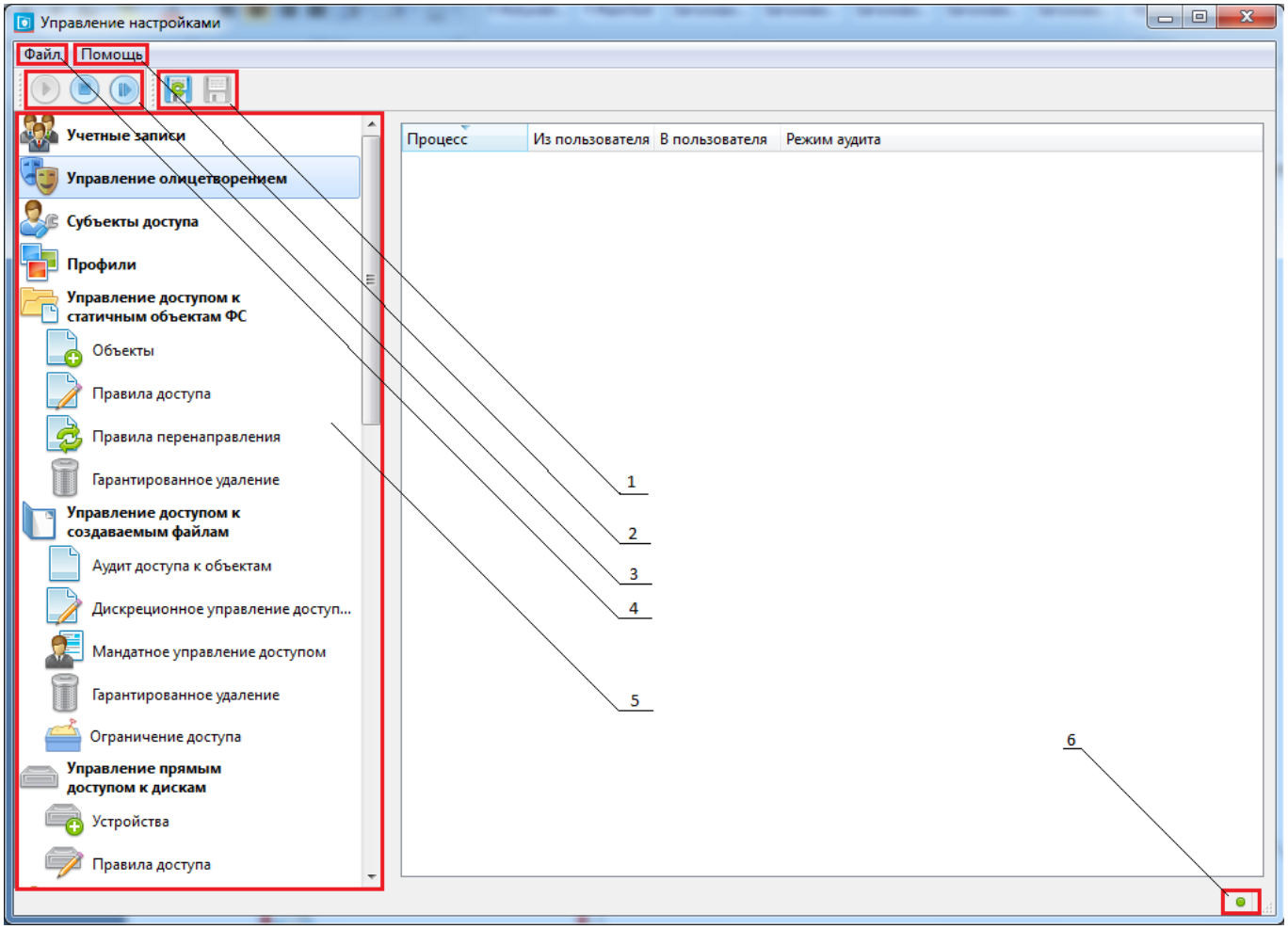


Рис.3.2.1. Структура интерфейса клиентской части

1 - Меню сохранения настроек и возврата к предыдущим настройкам

Для сохранения внесенных настроек требуется нажать кнопку  .

Возвратиться к предыдущим настройкам возможно, если внесенные настройки еще не сохранены. Для их загрузки нажать кнопку  .

2 - Меню «Помощь»

Меню «Помощь» содержит информацию о СЗИ «ViPNet SafePoint».

3 - Меню запуска, остановки, перезапуска службы (armour service).

Данное меню используется для остановки, запуска и/или перезапуска службы СЗИ «ViPNet SafePoint». Меню состоит из трех кнопок:

 Остановка службы

 Запуск службы

 Перезапуск службы

Возможность остановки, запуска и/или перезапуска службы СЗИ «ViPNet SafePoint» предназначена для обновления драйверов СЗИ «ViPNet SafePoint». Процесс перезапуска службы является альтернативой перезагрузки компьютера. Но необходимо учитывать, что процесс перезапуска службы является ресурсозатратным процессом, поэтому может приводить к зависаниям системы и поэтому в общем случае рекомендуется пользоваться перезагрузкой компьютера.

4 - Меню «Файл»

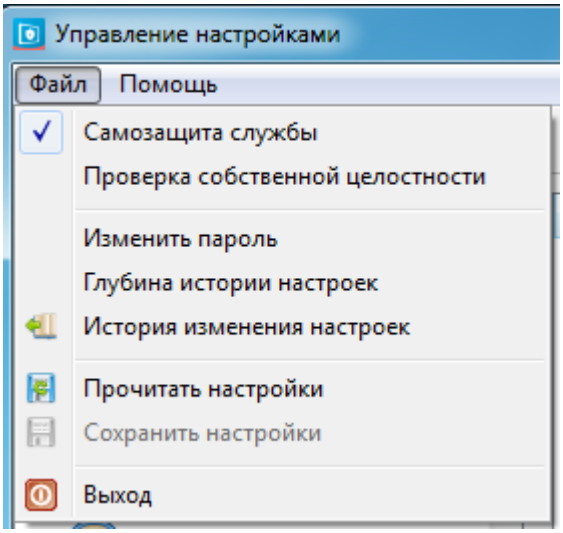


Рис.3.2.2. Меню «Файл»

Основное меню «Файл» (рис.3.2.2) включает в себя ряд возможностей:

- Самозащита службы;
- Проверка собственной целостности
- Изменить пароль;
- Глубина изменения настроек;
- История изменения настроек;
- Прочитать настройки;
- Сохранить настройки.

Настройка из меню «Файл»:

- Самозащита службы. При включенной самозащите службы (установлена галочка «Самозащита службы») становится невозможным «убиение» процесса службы СЗИ «ViPNet SafePoint», в стандартной оснастке «Службы» отсутствует возможность остановки и перезапуска службы.

Существует возможность отключения функций самозащиты. Для этого необходимо для параметра реестра «HKLM\SYSTEM\CurrentControlSet\services\armdrv3\Self Protection\ Flags» задать значения:

- 0x00000001 - отключение защиты зарегистрированных процессов от TerminateProcess().
- 0x00000002 - отключение защиты службы СЗИ «ViPNet SafePoint» от остановки.

- Проверка собственной целостности. Запускает вручную механизм проверки целостности кода и данных «ViPNet SafePoint» и значений реестра, критичных для работы «ViPNet SafePoint».
- Изменить пароль. Изменяется пароль, устанавливаемый для запуска интерфейса СЗИ «ViPNet SafePoint» администратором. Для изменения пароля необходимо открыть меню «Файл» → «Изменить пароль». В окне «Изменение пароля администратора» (рис.3.2.3) задать пароль и его подтверждение;

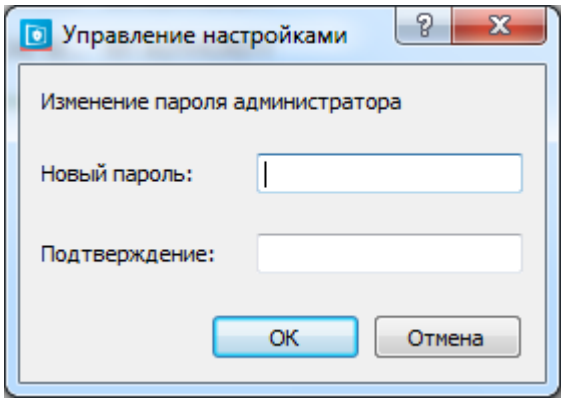


Рис.3.2.3. Изменение пароля администратора

- Глубина изменения настроек. Для удобства администрирования, СЗИ «ViPNet SafePoint» позволяет сохранять файлы предыдущих настроек (формируемых после сохранения настроек СЗИ «ViPNet SafePoint») с возможностью их восстановления. Для задания и изменения глубины истории изменения настроек (числа хранящихся файлов с изменения настроек) необходимо открыть меню «Файл» → «Изменить глубину истории настроек». В окне «Изменения глубины истории настроек» (рис.3.2.4) требуется ввести необходимое значение. Максимальное значение «100»;

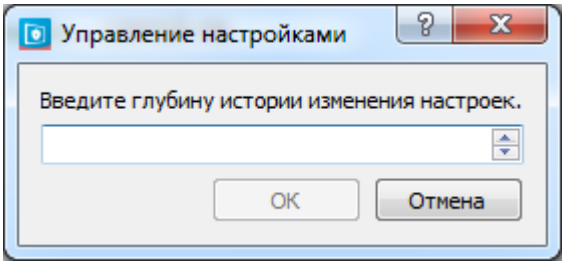


Рис.3.2.4. Изменения глубины истории настроек

- История изменения настроек. Отображается история изменения настроек с указанием даты их изменения. Для загрузки истории настроек необходимо открыть меню «Файл»→ «История изменения настроек».

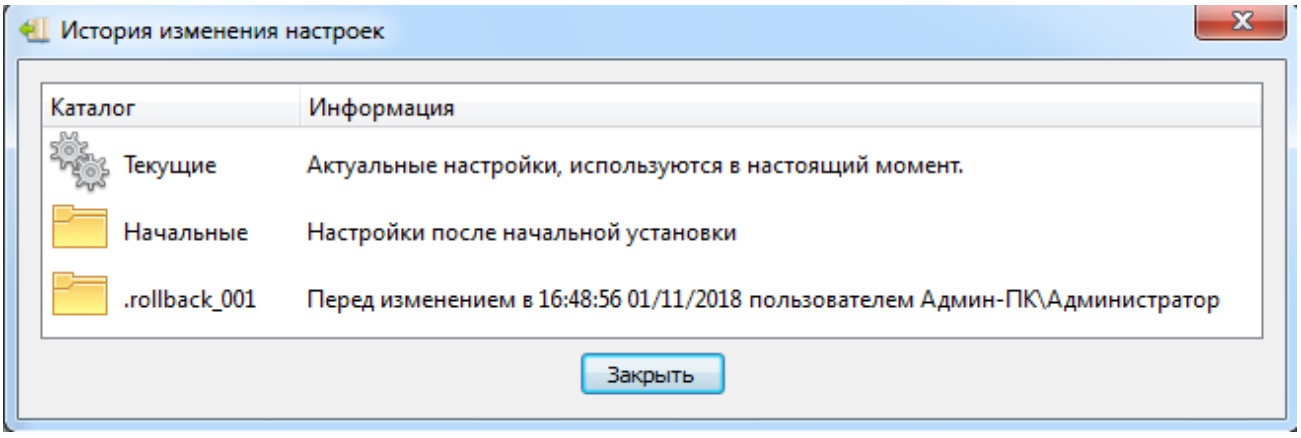


Рис.3.2.5. История изменения настроек

В окне «История изменения настроек» (рис.3.2.5) можно перейти (вернуться) к сделанным ранее или начальным настройкам (двойное нажатие левой кнопкой мыши по названию настроек). В окне «Подтверждение загрузки настроек» (рис.3.2.6) выбрать «Да». При этом в СЗИ «ViPNet SafePoint» загрузятся выбранные предыдущие настройки.

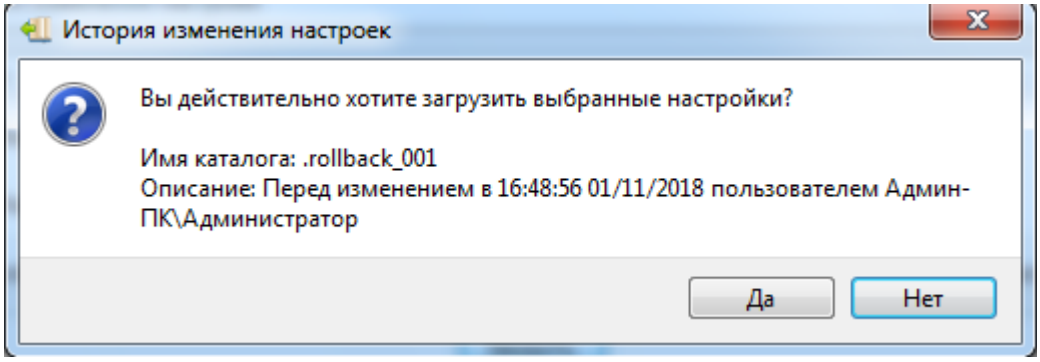


Рис.3.2.6. Подтверждение загрузки настроек

- Прочитать настройки. Для загрузки выбранных предыдущих настроек необходимо открыть меню «Файл» → «Прочитать настройки»;
- Сохранить настройки. Для сохранения внесенных настроек необходимо открыть меню «Файл» → «Сохранить настройки».

Текущие сохраненные настройки при этом будут сохранены в качестве предыдущих. К ним можно будет также возвратиться.

5 – Меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint»

Группы настроек механизмов защиты, реализованных в СЗИ «ViPNet SafePoint» включают в себя:

- Учетные записи;
- Управление олицетворением;
- Субъекты доступа;
- Профили;
- Управление доступом к статичным объектам ФС:
  - Объекты;
  - Правила доступа;
  - Правила перенаправления;

- Гарантированное удаление;

Управление доступом к создаваемым файлам:

- Аудит доступа к объектам;
- Дискреционное управление доступом;
- Мандатное управление доступом;
- Гарантированное удаление;
- Ограничение доступа;

Управление прямым доступом к диску:

- Устройства;
- Правила доступа;

Управление доступом к реестру:

- Объекты;
- Правила доступа;

Управление доступом к принтерам:

- Принтеры;
- Правила доступа;

Управление доступом к службам Windows:

- Службы;
- Правила доступа;

Управление устройствами:

- Устройства;
- Правил□ подключения;

Управление доступом к буферу обмена;

Управление внедрением кода или данных;

Очистка ОЗУ;

Управление процессами:

- Разрешенные процессы;
- Обязательные процессы;
- Расписание работы;

Контроль целостности:

- Файловая система;
- Реестр;

Настройки ротации;

Настройки сети.

> Назначение и настройка каждого из этих механизмов СЗИ «ViPNet SafePoint» описаны в следующих частях документа.

В интерфейсах наиболее сложных механизмов, при просмотре заданных объектов и назначенных правил, при наведении курсора на значимые поля появляются всплывающие окна-подсказки (рис.3.2.7).

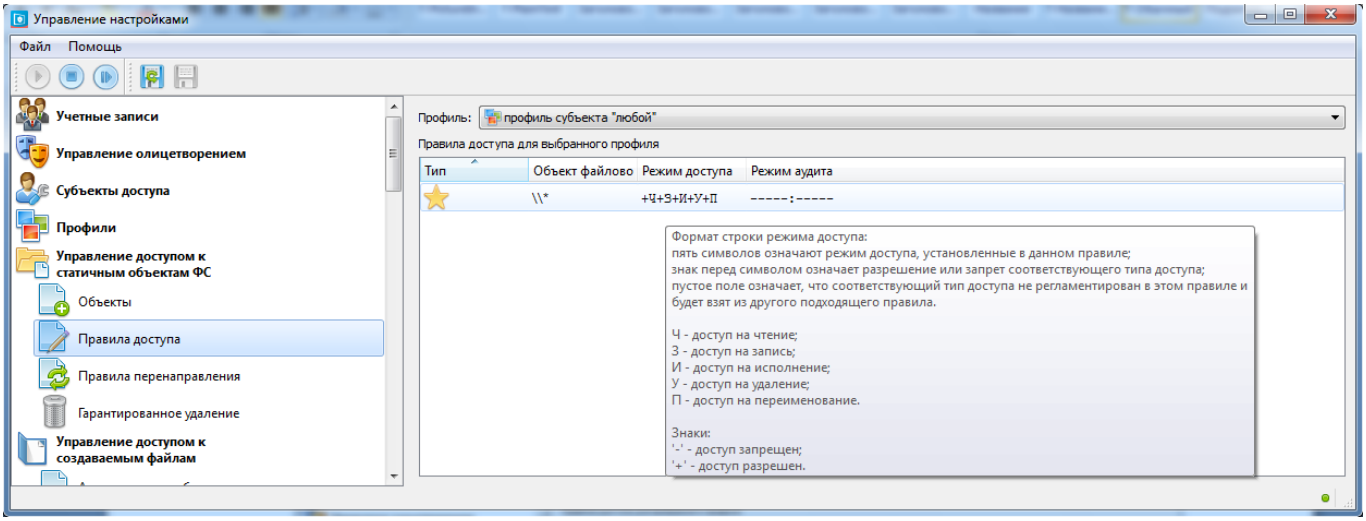


Рис.3.2.7. Пример всплывающих окон с подсказками

6 - Индикатор активности службы СЗИ «ViPNet SafePoint»

- зеленый цвет индикатора оповещает о том, что служба запущена.
- красный цвет индикатора оповещает о том, что служба остановлена.

4. ПЕРВИЧНАЯ НАСТРОЙКА. ЗАПУСК И ОСТАНОВКА СЗИ «VIPNET SAFEPOINT»

4.1. ЗАПУСК, ПЕРЕЗАПУСК, ОСТАНОВКА СЛУЖБЫ

Возможность остановки, запуска и/или перезапуска службы СЗИ «ViPNet SafePoint» предназначена для обновления драйверов СЗИ «ViPNet SafePoint». Процесс перезапуска службы является альтернативой перезагрузки компьютера. Но необходимо учитывать, что процесс перезапуска службы является ресурсозатратным процессом, поэтому может приводить к зависаниям системы и поэтому в общем случае рекомендуется пользоваться перезагрузкой компьютера.

Службой клиентской части СЗИ «ViPNet SafePoint» является служба «Armour service». В отношении службы СЗИ «ViPNet SafePoint» могут быть выполнены следующие действия:

- Остановка службы. Для остановки службы необходимо нажать кнопку  .
- Запуск службы. Для запуска службы необходимо нажать кнопку  .
- Перезапуск (останов и последующий запуск) службы. Для перезапуска службы необходимо нажать кнопку  .

Для просмотра событий, связанных с работой службы СЗИ «ViPNet SafePoint» «ViPNet SafePoint» следует открыть в Просмотрщике журналов аудита «Журнал служебных событий ViPNet SafePoint».

В активном режиме работы служба «Armour service» должна быть запущена, тип запуска - «Автоматически».

Для предотвращения конфликтов с СЗИ «ViPNet SafePoint» при установке приложений, драйверов сторонних производителей на защищаемый компьютер необходимо остановить службу СЗИ «ViPNet SafePoint» для корректной установки ПО.

Служба СЗИ «ViPNet SafePoint» настроена на автоматический перезапуск при аварии так, что ОС пытается перезапустить ее через 5 секунд после аварийной остановки. Если перезапустить службу не удается в течение 120 секунд – компьютер перезагружается.

4.2. НАСТРОЙКА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КЛИЕНТСКОЙ ЧАСТИ С СЕРВЕРОМ БЕЗОПАСНОСТИ И С СЕРВЕРОМ АУДИТА

Окно интерфейса настройки сетевого взаимодействия клиентской части СЗИ «ViPNet SafePoint» с сервером (серверами) безопасности и с сервером (серверами) аудита представлено на рис.4.2.1.

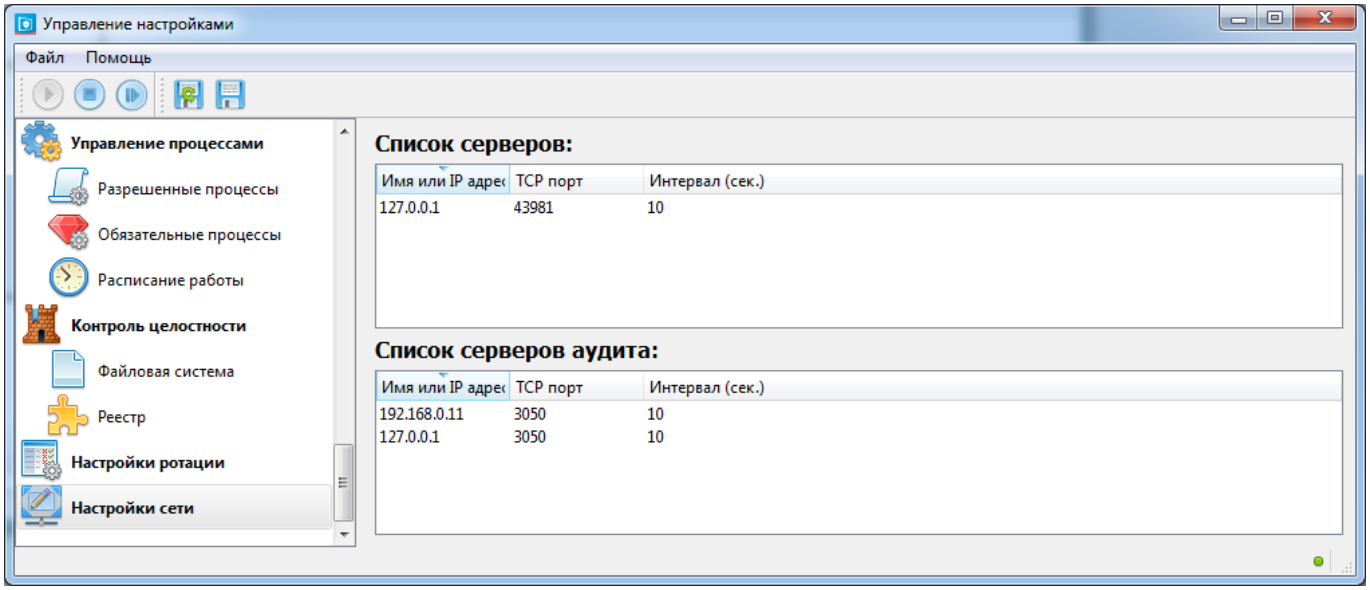


Рис.4.2.1. Интерфейс механизма настройки сети

Для настройки сетевого взаимодействия между клиентской частью и сервером (серверами) безопасности в интерфейсе клиентской части СЗИ «ViPNet SafePoint» необходимо задать параметры сервера безопасности:

1. В списке серверов нажать правой кнопкой мыши по пустому полю и выбрать «Добавить новый сервер» или для изменения параметров уже существующего сервера выбрать, нажав правой кнопкой мыши, «Изменить параметры сервера».

2. В появившемся окне «Добавление нового сервера» (рис.4.2.2) (либо, при изменении существующего сервера безопасности, в окне «Изменение параметров сервера», аналогичного окну «Добавление нового сервера»):

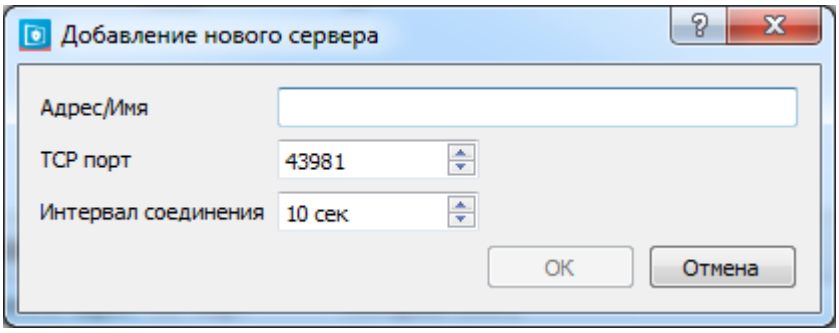


Рис.4.2.2. Окно добавления нового сервера СЗИ

1) Ввести параметры:
   - В строке «Адрес/Имя» ввести IP адрес сервера или имя сервера безопасности, заданное сетевым именем или доменным именем компьютера;
   - TCP порт (порт, к которому клиент пытается подключиться), по умолчанию используется порт 43981;
   - Интервал соединения в секундах (интервал времени, по прошествии которого клиент пытается подключиться к серверу).
2) Нажать кнопку «ОК».

Назначенные правила сетевого взаимодействия будут применены только после сохранения и перезапуска службы. Перезапуск службы может быть осуществлен автоматически при перезагрузке ОС или вручную.

Возможность перезапуска службы СЗИ «ViPNet SafePoint» предназначена для обновления драйверов СЗИ «ViPNet SafePoint». Процесс перезапуска службы является альтернативой перезагрузки компьютера. Но необходимо учитывать, что процесс перезапуска службы является ресурсозатратным процессом, поэтому может приводить к зависаниям системы и поэтому в общем случае рекомендуется пользоваться перезагрузкой компьютера.

Существует возможность подключить клиентскую часть одновременно к нескольким серверным частям. По отношению к клиентской части они будут равноправными.

Если клиентская часть запущена на локальной машине, то при попытке запустить ее с сервера безопасности появится окно (рис.4.2.3) с информацией о том, что интерфейс клиентской части запущен на локальной машине.

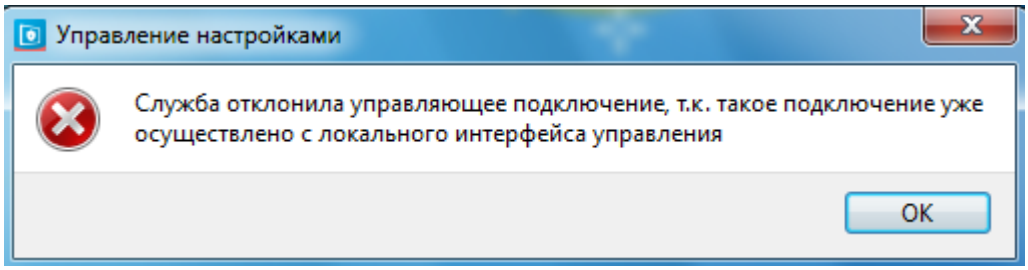


Рис.4.2.3. Окно информации о запущенном интерфейсе

Если интерфейс настройки клиентской части был запущен на сервере безопасности, то при попытке запустить интерфейс на локальной машине появится окно (рис.4.2.4) с информацией о том, что интерфейс клиентской запущен на стороне сервера.

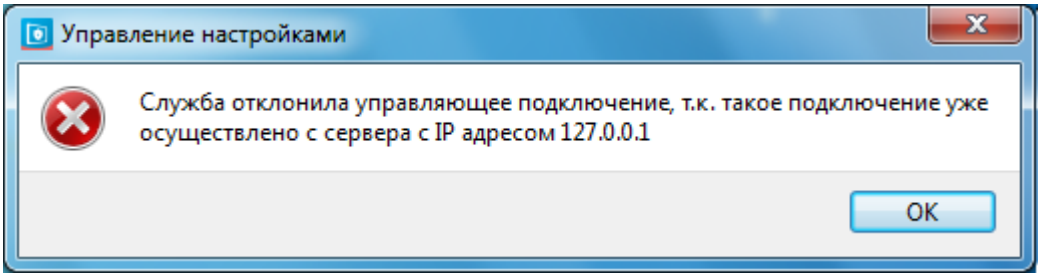


Рис.4.2.4. Окно информации о запущенном интерфейсе

Для настройки сетевого взаимодействия между клиентской частью и сервером (серверами) аудита в интерфейсе клиентской части СЗИ «ViPNet SafePoint» необходимо:

1. В списке серверов аудита нажать правой кнопкой мыши по пустому полю и выбрать «Добавить сервер» или для изменения параметров уже существующего сервера выбрать «Изменить параметры сервера».
2. В появившемся окне «Добавление нового сервера аудита» (рис.4.2.5):

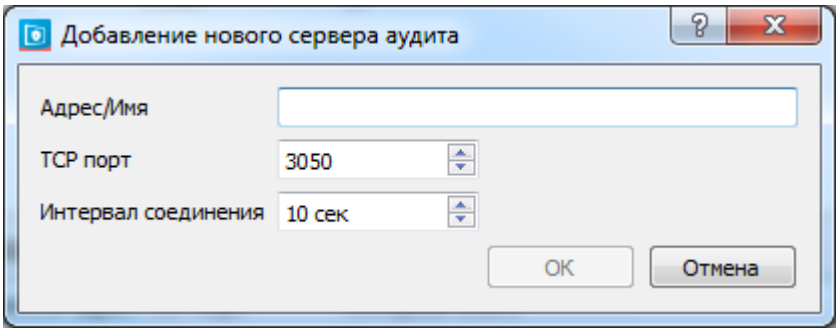


Рис.4.2.5. Окно добавления нового сервера аудита

1) Вести параметры

- В строке «Адрес/Имя» ввести IP адрес сервера или имя сервера аудита, заданное сетевым именем или доменным именем компьютера;
- TCP порт (порт, к которому клиент пытается подключиться), по умолчанию используется порт 3050;

- Интервал соединения в секундах (интервал времени, по прошествии которого клиент пытается подключиться к серверу аудита).

2) Нажать кнопку «ОК».

Назначенные правила сетевого взаимодействия будут применены только после сохранения и перезапуска службы. Перезапуск службы может быть осуществлен автоматически при перезагрузке ОС или вручную.

Возможность остановки, запуска и/или перезапуска службы СЗИ «ViPNet SafePoint» предназначена для обновления драйверов СЗИ «ViPNet SafePoint». Процесс перезапуска службы является альтернативой перезагрузки компьютера. Но необходимо учитывать, что процесс перезапуска службы является ресурсозатратным процессом, поэтому может приводить к зависаниям системы и поэтому в общем случае рекомендуется пользоваться перезагрузкой компьютера.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

4.3. НАСТРОЙКИ РОТАЦИИ ЖУРНАЛОВ

Окно интерфейса «Настройки ротации» журналов представлено на рис.4.3.1. Эти настройки заданы в СЗИ «ViPNet SafePoint» «по умолчанию», при необходимости их можно изменить.

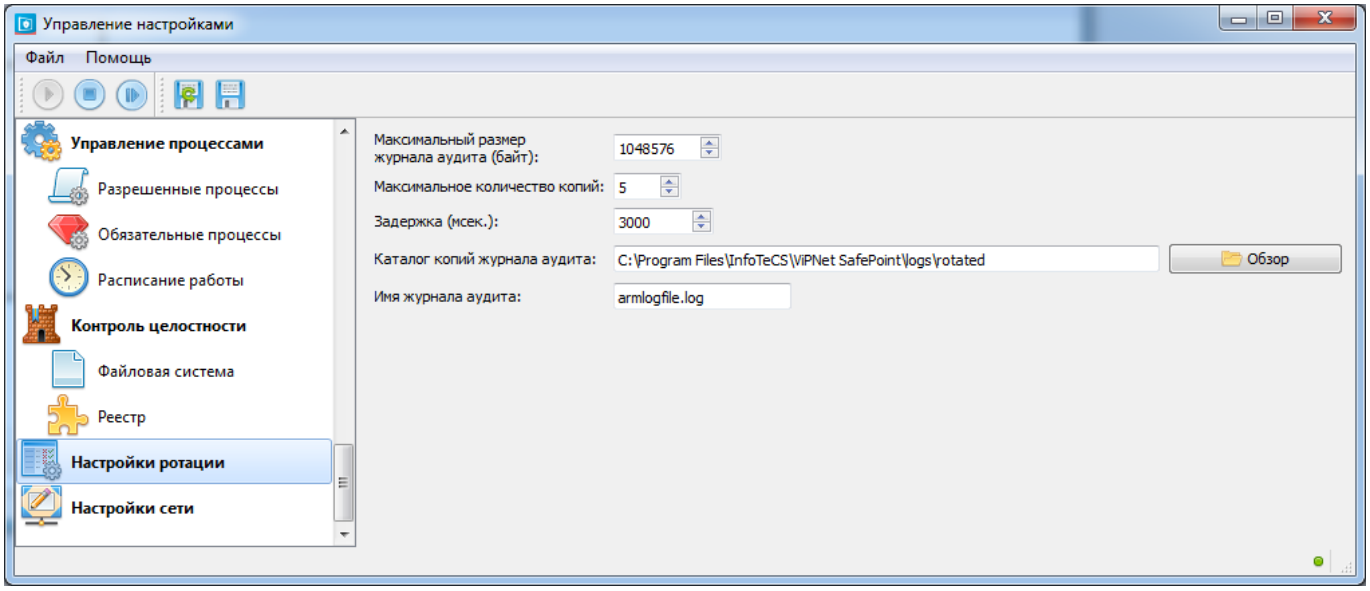


Рис.4.3.1. Интерфейс механизма настройки ротации журналов

Для изменения настроек ротации журналов аудита необходимо:

1. В меню групп настроек механизмов интерфейса СЗИ «ViPNet SafePoint» выбрать пункт «Настройки ротации».

2. Задать максимальный размер журнала аудита в байтах. Максимально возможный размер равен 1 000 000 000 байт (1 млрд. байт ~ 1 Гб ~ 953 Мб).
3. Задать максимальное количество копий журнала аудита. Максимально возможное их число равно 10 000.
4. Задать задержку в миллисекундах (интервал времени, через который осуществляется опрос драйвера на предмет наличия информации для лог-файла, а также контроль размера файла);
5. Задать каталог, в котором будут сохраняться копии журнала аудита, используя «Обзор» или вручную.
6. Задать имя журнала аудита, т.е. имя файла, в который будет происходить запись данных аудита.

Заданные параметры ротации журналов будут применены только после сохранения и перезапуска службы. Перезапуск службы может быть осуществлен автоматически при перезагрузке ОС или вручную.

Возможность перезапуска службы СЗИ «ViPNet SafePoint» предназначена для обновления драйверов СЗИ «ViPNet SafePoint». Процесс перезапуска службы является альтернативой перезагрузки компьютера. Но необходимо учитывать, что процесс перезапуска службы является ресурсозатратным процессом, поэтому может приводить к зависаниям системы и поэтому в общем случае рекомендуется пользоваться перезагрузкой компьютера.

Для сохранения настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

4.4. ВЫБОР ЯЗЫКА СЗИ «VIPNET SAFEPOINT»

Интерфейсы всех компонентов СЗИ «ViPNet SafePoint» первоначально русскоязычные. В процессе эксплуатации системы может понадобиться поменять язык на английский. Для этого необходимо воспользоваться утилитой **langsel.exe,** находящейся в каталоге *..\INFOTECS\VIPNET SAFEPOINT\bin*. Утилиту необходимо запускать от имени администратора, после запуска утилиты откроется окно (рис.4.4.1):

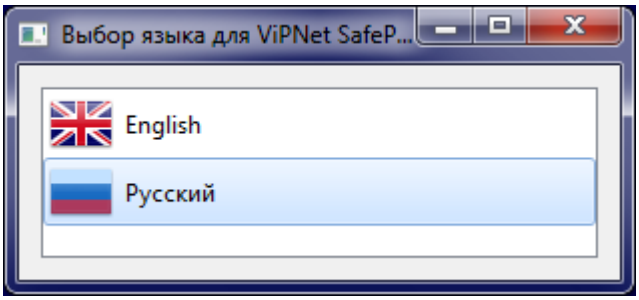


Рис.4.4.1. Выбор языка СЗИ «ViPNet SafePoint»

В этом окне необходимо выбрать язык двойным нажатием левой кнопки мыши. После этого появится окно подтверждения выбора языка (рис.4.4.2), в котором необходимо нажать кнопку «ОК».

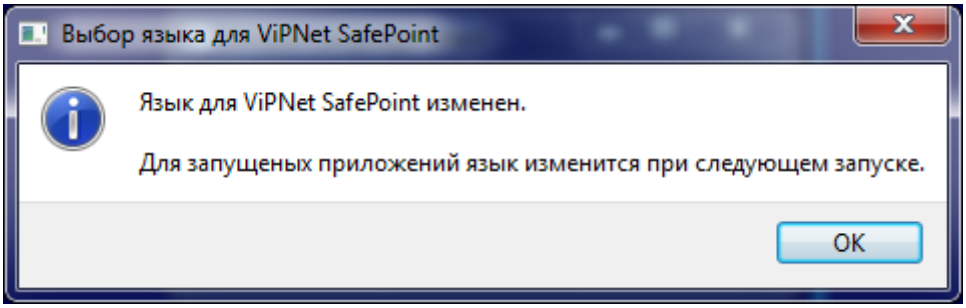


Рис.4.4.2. Окно подтверждения смены языка для СЗИ «ViPNet SafePoint»

Если до запуска утилиты **langsel.exe**, интерфейсы СЗИ «ViPNet SafePoint» были запущены, то необходимо закрыть их и заново запустить. Если же интерфейс не был запущен, то при его запуске язык будет соответствовать выбранному.

5. МЕХАНИЗМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

5.1. НАЗНАЧЕНИЕ, ВОЗМОЖНОСТИ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Механизм идентификации и аутентификации предназначен для реализации контроля локального и удаленного входа пользователей в систему. В ОС и в СЗИ «ViPNet SafePoint» ведутся собственные списки (базы данных) учетных записей. Для возможности входа под учетной записью пользователя в систему, с последующим доступом к ресурсам в рамках реализованной разграничительной политики, соответствующая учетная запись должна быть заведена и в ОС, и в СЗИ «ViPNet SafePoint». Для удобства заведения учетных записей и их синхронизации, в СЗИ «ViPNet SafePoint» реализованы возможности импорта учетной записи из ОС (из AD) в СЗИ «ViPNet SafePoint» и, наоборот, экспорта учетной записи из СЗИ «ViPNet SafePoint» в ОС (в AD) в том случае, если учетная запись, отсутствующая в ОС, заводится в СЗИ «ViPNet SafePoint».

Механизм идентификации и аутентификации СЗИ «ViPNet SafePoint» по сравнению с ОС расширен возможностью задания правил и контролем входа в систему в безопасном режиме.

Механизм идентификации и аутентификации СЗИ «ViPNet SafePoint» предлагает пользователю идентифицироваться и аутентифицироваться в тех же случаях, что и ОС:

- локальный вход в систему;
- запуск приложения с правами другого пользователя (если данная возможность разрешена СЗИ «ViPNet SafePoint»);
- удаленный доступ к разделенным сетевым ресурсам локальной сети;
- удаленный доступ по RDP;
- доступ к терминальной сессии;
- для разблокировки системы, посредством снятия заставки.

Механизм идентификации и аутентификации СЗИ «ViPNet SafePoint» позволяет осуществлять ввод пароля, как с консоли, так и с устройств хранения и ввода паролей – по электронному ключу или по смарт-карте ruToken, по электронному ключу или по смарт-карте Aladdin JaCarta. Поддерживаются следующие модели Aladdin: JaCarta LT, JaCarta PKI, JaCarta PKI / ГОСТ, JaCarta 2 PKI / ГОСТ. Поддерживаются следующие модели ruToken: ruToken ЭЦП 2.0, ruToken (S), ruToken PKI / ЭЦП, ruToken Lite.

В данном случае реализуется централизованная политика задания паролей – пароли задаются администратором безопасности (записываются на устройства хранения и ввода паролей, которые им затем раздаются пользователям). При использовании устройств хранения и ввода паролей реализуется двухфакторная аутентификация, которая, при необходимости, администратором может быть отключена. Дополнительно реализована возможность

одновременной установки разных типов аутентификации для разных учетных записей пользователей и разных типов аутентификации для одной учетной записи пользователя (вход по паролю с консоли и вход по электронному ключу или по смарт-карте ruToken, по электронному ключу или по смарт-карте Aladdin JaCarta).

Политика задания паролей при консольной аутентификации может быть, как централизованной, так и распределенной (пароли задаются непосредственно пользователями с учетом задаваемых администратором ограничений на параметры паролей). Возможности консольной аутентификации СЗИ «ViPNet SafePoint» существенно расширены. В том числе СЗИ «ViPNet SafePoint» предлагает воспользоваться генератором паролей (из состава СЗИ «ViPNet SafePoint»), позволяющим создавать пароли (как администратором, так и пользователями) случайным образом. При этом может быть задан алфавит генератора паролей (определяемый числом символов и их типом).

Реализованы различные политики разблокирования учетных записей. Блокирование учетных записей осуществляется СЗИ «ViPNet SafePoint» в случае нарушения заданной администратором безопасности политики обработки событий, связанных с преднамеренными, либо ошибочными действиями пользователей при выполнении процедуры идентификации и аутентификации.

При включенном механизме идентификации и аутентификации вход пользователей в систему возможен только при условии, что служба СЗИ «ViPNet SafePoint» запущена, в противном случае вход в систему возможен только под учетной записью администратора (***в данном случае под учетной записью администратора понимается пользователь, для которого в СЗИ «ViPNet SafePoint» разрешен вход в ОС в безопасном режиме***).

5.2. ИНТЕРФЕЙС МЕХАНИЗМА АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ, ОБЩИЕ НАСТРОЙКИ

СЗИ «ViPNet SafePoint» реализует собственный контроль и регистрацию доступа пользователей в систему. Окно интерфейса механизма «Учетные записи» представлено на рис.5.2.1. В окне находятся настройки механизма аутентификации, аудита, параметров паролей.

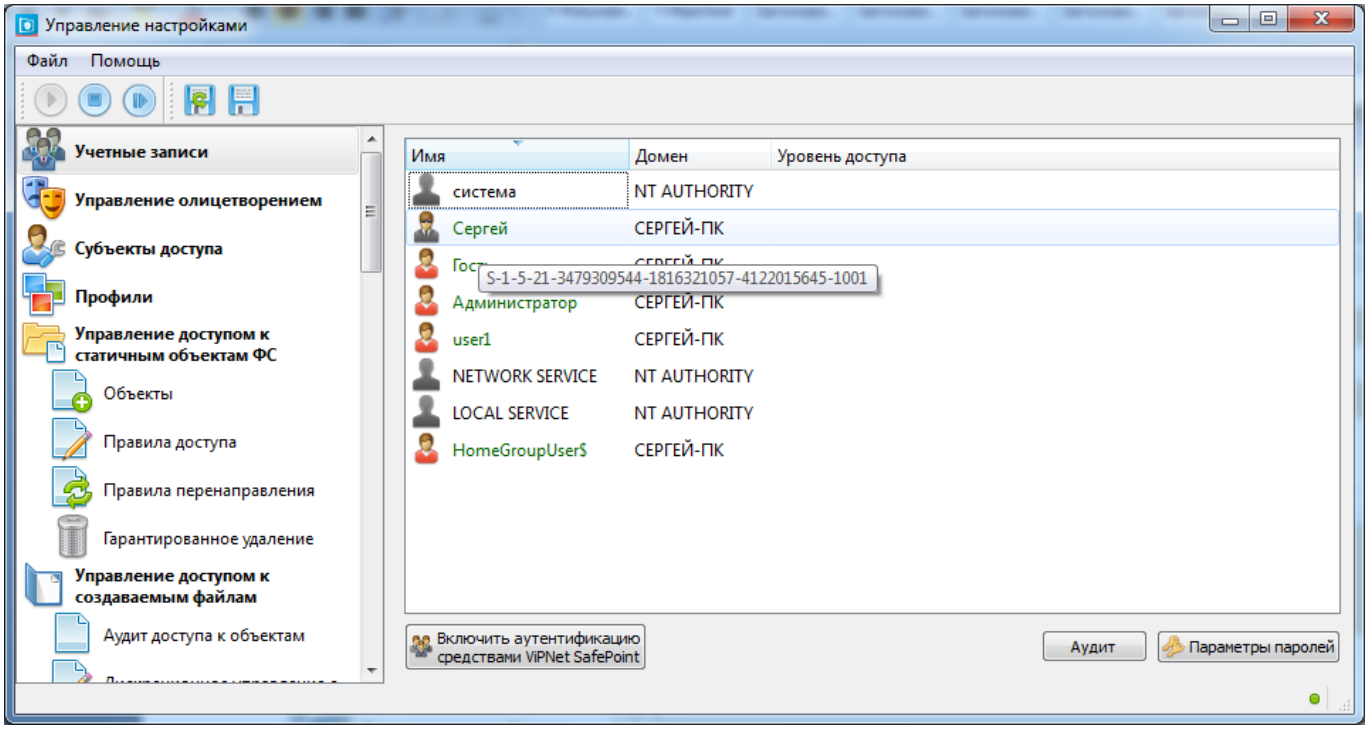


Рис.5.2.1. Окно настройки механизма авторизации, вкладка «Учетные записи»

В СЗИ «ViPNet SafePoint» ведется собственный список учетных записей пользователей, который должен включать разрешенные для входа в ОС учетные записи пользователей. Пользователи указываются как локальные, так и доменные.

Прежде чем заводить учетную запись пользователя в СЗИ «ViPNet SafePoint», необходимо настроить некоторые параметры паролей при любом типе аутентификации. Пароль «ViPNet SafePoint» устанавливается при любом типе аутентификации.

Под паролем «ViPNet SafePoint» понимается секретное слово пользователя, которое используется при входе в ОС с использованием механизма идентификации и аутентификации СЗИ «ViPNet SafePoint».

Под аутентификацией понимается процедура проверки подлинности процесса идентификации с использованием секретного слова – пароля.

Настройка начинается с задания общих параметров пароля. Для этого следует:

1. Открыть интерфейс «Управление настройками».

2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать на кнопку «Параметры паролей» и в открывшемся меню «Редактирование параметров паролей» (рис.5.2.2) настроить требуемые параметры:

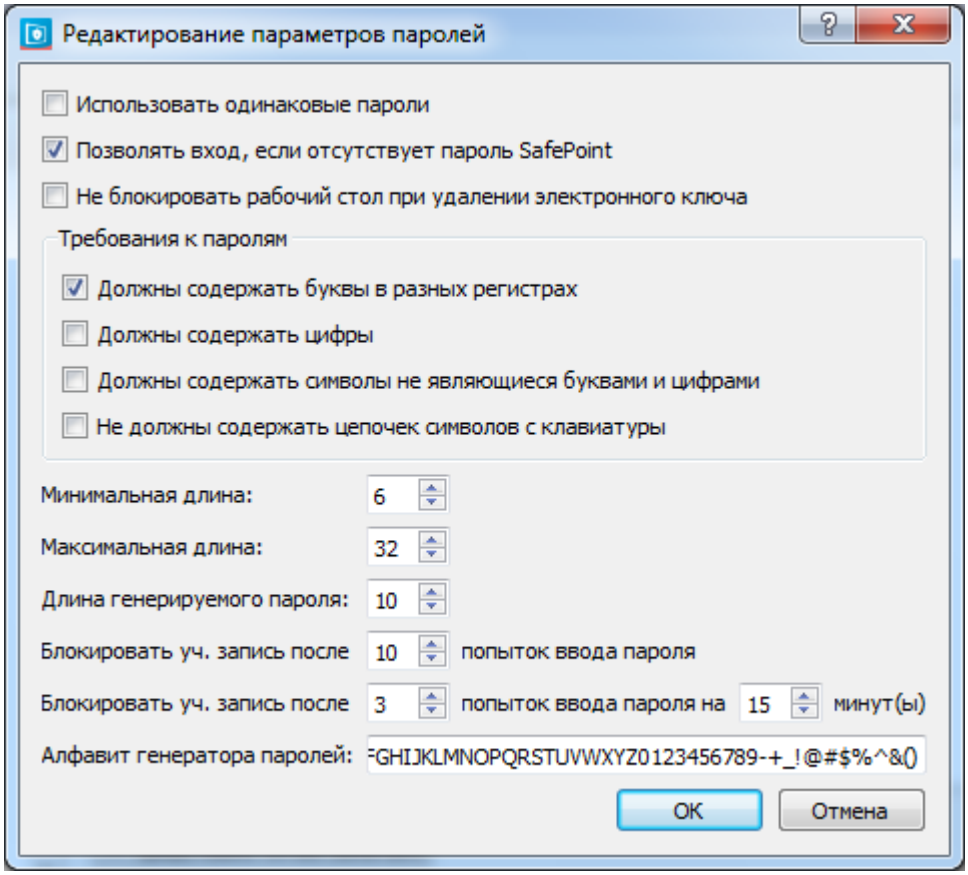


Рис.5.2.2. Окно редактирования параметров паролей

- *флаг «Использовать одинаковые пароли»*, установка не обязательна. Установленный флаг «Использовать одинаковые пароли» означает, что при аутентификации будет запрошен только пароль «ViPNet SafePoint», пароль Windows будет заменен на пароль «ViPNet SafePoint»;
- *флаг «Позволять вход, если отсутствует пароль SafePoint»*, установка не обязательна. Установленный флаг «Позволять вход, если отсутствует пароль «ViPNet SafePoint» означает, что после того как будет включена «Аутентификация средствами ViPNet SafePoint», пользователь, у которого не заведен пароль «ViPNet SafePoint», сможет войти в Windows, используя только пароль Windows;
- *флаг «Не блокировать рабочий стол при удалении электронного ключа»*, установка не обязательна. Установленный флаг «Не блокировать рабочий стол при удалении электронного ключа» означает, что при включенной «Аутентификации средствами ViPNet SafePoint» при отключении электронного ключа пользователем, рабочий стол не будет заблокирован;

- *флаги требований к паролям*, установка не обязательна. Установленные флаги требований к паролям позволяют задать характеристики пароля:
  - наличие букв в разных регистрах;
  - наличие цифр;
  - наличие символов, не являющихся буквами и цифрами;
  - отсутствие цепочек символов с клавиатуры.
- *параметры генератора паролей*, установка не обязательна:
  - длина генерируемого пароля;
  - алфавит генератора паролей.

Генератор паролей используется для автоматического создания пароля «ViPNet SafePoint» или пароля Windows при создании или редактировании пользователей, а также при изменении пароля. Пароль создается после двойного нажатия левой кнопкой мыши по полю ввода пароля.

4. После завершения редактирования параметров паролей нажать кнопку «ОК».

Настройка параметров аудита описана в разделе 15.2.1. Вход в систему. Механизм идентификации и аутентификации.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

5.3. СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ, СИНХРОНИЗАЦИЯ С СИСТЕМОЙ, УДАЛЕНИЕ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

В СЗИ «ViPNet SafePoint» **создание** учетной записи пользователя (локального или доменного) возможно двумя способами:

- **импорт** «Учетных записей Windows» в СЗИ «ViPNet SafePoint»;
- **экспорт** при создании новой учетной записи пользователя в СЗИ «ViPNet SafePoint» с их экспортом в «Учетные записи Windows».

Клиентская часть СЗИ «ViPNet SafePoint» позволяет управлять только локальными учетными записями. Для управления доменными учетными записями необходимо использовать специальную программу для управления пользователями домена, которая входит в состав Сервера безопасности СЗИ «ViPNet SafePoint».

При использовании механизма аутентификации учетной записи пользователя задается требование пройти аутентификацию только в окне СЗИ «ViPNet SafePoint» (на экран выводится только окно аутентификации СЗИ «ViPNet SafePoint», штатное окно ОС не выводится),

аутентификация учетной записи пользователя в операционной системе осуществляется автоматически.

После добавления пароля учетной записи пользователя и/или установки типа аутентификации имя учетной записи пользователя изменяет цвет.

Доменные пользователи, которых нельзя редактировать, выделены другим цветом фона.

Если установлен 3-й бит значения параметра реестра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config), то доменные пользователи не будут выделены другим цветом фона, так как их можно редактировать.

Цветовое отображение **имен учетных записей** пользователей в интерфейсе, рис.5.2.1:

Красный	у учетной записи пользователя не заведен пароль «ViPNet SafePoint» и не установлен флаг «Позволять вход, если отсутствует пароль «ViPNet SafePoint».
Зеленый	у учетной записи пользователя установлен тип аутентификации СЗИ «ViPNet SafePoint» или установлен флаг «Позволять вход, если отсутствует пароль «ViPNet SafePoint».
Серый	для учетной записи пользователя не выбран тип аутентификации.
Черный	системная учетная запись пользователя.
Синий	учетная запись удалена из ОС средствами ОС.

Отображение **пиктограмм учетных записей** пользователей в интерфейсе, рис.5.2.1:

	у учетной записи пользователя не заведен пароль «ViPNet SafePoint».
	у учетной записи пользователя установлен тип аутентификации СЗИ «ViPNet SafePoint» и задан пароль «ViPNet SafePoint».
	для учетной записи пользователя не выбран тип аутентификации, но задан пароль «ViPNet SafePoint».
	системная учетная запись пользователя.
	учетная запись администратора (пользователю разрешен вход в ОС в безопасном режиме).

При ***удалении*** учетной записи пользователя(ей) из СЗИ «ViPNet SafePoint», учетная запись пользователя так же удаляется и из Windows.

5.4. НАСТРОЙКА МЕХАНИЗМА АУТЕНТИФИКАЦИИ ЛОКАЛЬНОЙ ИЛИ ДОМЕННОЙ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

Настройка механизма аутентификации и идентификации производится в несколько этапов:

1. Общие настройки (см. в разделе 5.2).
2. Создание списка учетных записей.
3. Настройка типа аутентификации.
4. Включение механизма.

Создание списка учетных записей описано в каждом разделе настройки типа аутентификации (разделы 5.4.1, 5.4.2, 5.4.3). Для включения механизма идентификации и аутентификации необходимо нажать кнопку «Включить аутентификацию средствами «ViPNet SafePoint» во вкладке «Учетные записи».

Операционная система Windows позволяет войти в безопасном режиме без загрузки драйверов, данный режим несет угрозу, поэтому в СЗИ «ViPNet SafePoint» реализована дополнительная возможность ограничить вход учетной записи пользователя в этом режиме.

При работе с ОС Windows, если при установке был заведен пользователь, добавленный по учетной записи Microsoft, его необходимо удалить средствами ОС или СЗИ «ViPNet SafePoint». Либо при установке ОС не заводить данного пользователя, т.к. пользователь, заведенный по учетной записи Microsoft, является виртуальным.

СЗИ «ViPNet SafePoint» при первом запуске автоматически синхронизирует базу данных пользователей СЗИ с базой локальных учетных записей Windows.

Для включения механизма аутентификации необходимо в «Настройках данных пользователя» **хотя бы для одного** пользователя установить флаг «Разрешить вход при работе ОС в безопасном режиме» и задать пароль «ViPNet SafePoint».

Для включения механизма аутентификации средствами СЗИ «ViPNet SafePoint» должна быть **запущена служба**.

Для включения механизма идентификации и аутентификации необходимо нажать **кнопку «Включить аутентификацию средствами СЗИ «ViPNet SafePoint»** во вкладке «Учетные записи».

Для любой учетной записи пользователя может быть установлен любой тип аутентификации (вход по паролю с консоли, вход по электронному ключу ruToken, вход по электронному ключу Aladdin JaCarta или по смарт-карте) или одновременно два типа аутентификации (вход по паролю с консоли и вход по электронному ключу ruToken или по электронному ключу Aladdin JaCarta).

В СЗИ «ViPNet SafePoint» предусмотрен режим входа в ОС без предварительного задания пароля «ViPNet SafePoint». При использовании данного режима пользователь должен самостоятельно задать консольный пароль «ViPNet SafePoint» после входа в систему.

При добавлении новой учетной записи пользователя в СЗИ «ViPNet SafePoint», если она не заведена в Windows, автоматически производится добавление учетной записи в Windows.

Настройка локальных пользователей осуществляется при помощи интерфейса клиентской части или сервера безопасности СЗИ «ViPNet SafePoint». Настройка доменных пользователей при помощи программы управления пользователей домена, которая входит в состав сервера безопасности СЗИ «ViPNet SafePoint».

5.4.1. Аутентификация по паролю с консоли

Настройка параметров паролей и блокировки учетных записей

Помимо общих настроек параметров паролей (см. в разделе 5.2., рис.5.2.1) существуют дополнительные возможности настройки параметров паролей:

- существует возможность ограничивать максимальную и минимальную длину пароля «ViPNet SafePoint».

Дополнительно возможно настроить **блокировку учетных записей**

- в случае неверного ввода паролей:

- блокировка учетной записи на заданный интервал времени, после неверного ввода заданного количества раз (максимальное количество попыток 31, максимальное значение интервала 60 минут);
- блокировка учетной записи по количеству попыток неверного ввода пароля (максимальное количество попыток 32).

Создание новой учетной записи пользователя средствами СЗИ «ViPNet SafePoint»

Для создания новой учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» открыть «Учетные записи».
3. Нажать правой кнопкой мыши по окну «Учетных записей».
4. В появившемся контекстном меню выбрать «Добавить пользователя». Появится окно «Добавление нового пользователя» (рис.5.4.1.1, рис.5.4.1.2).

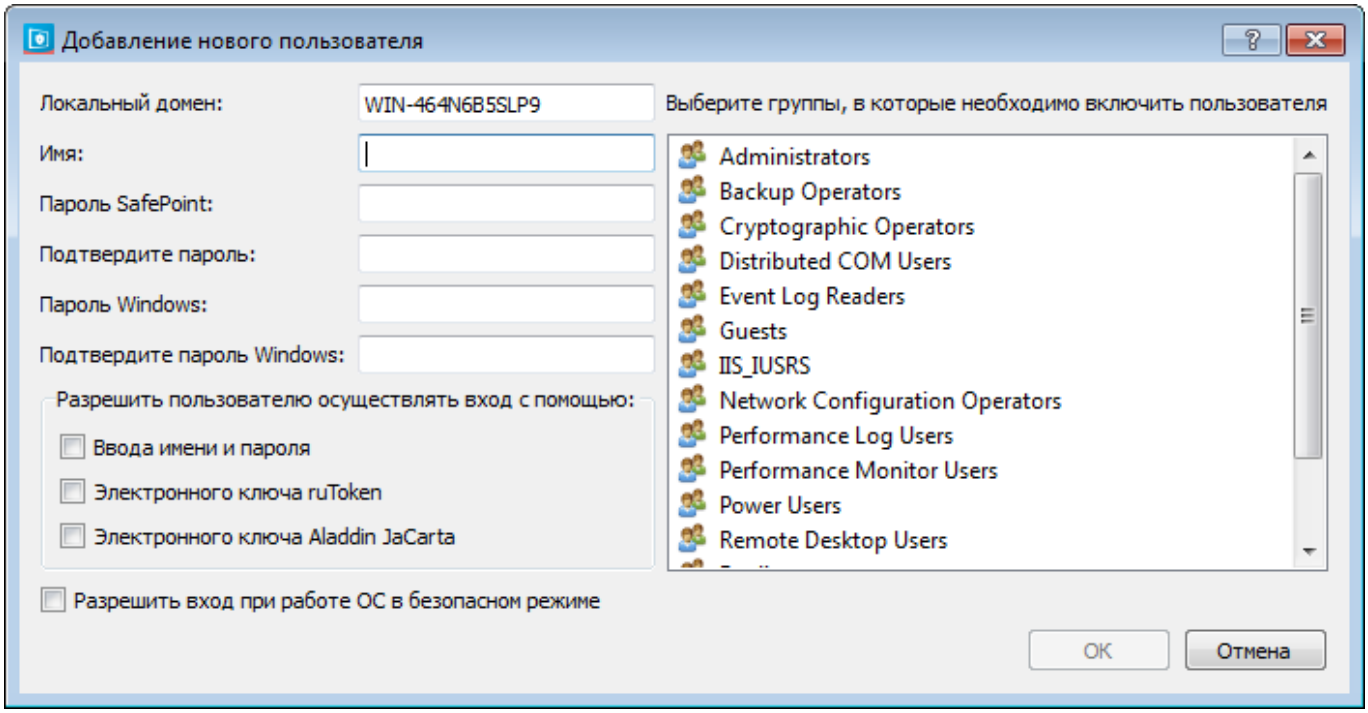


Рис.5.4.1.1. Окно добавления новой учетной записи пользователя

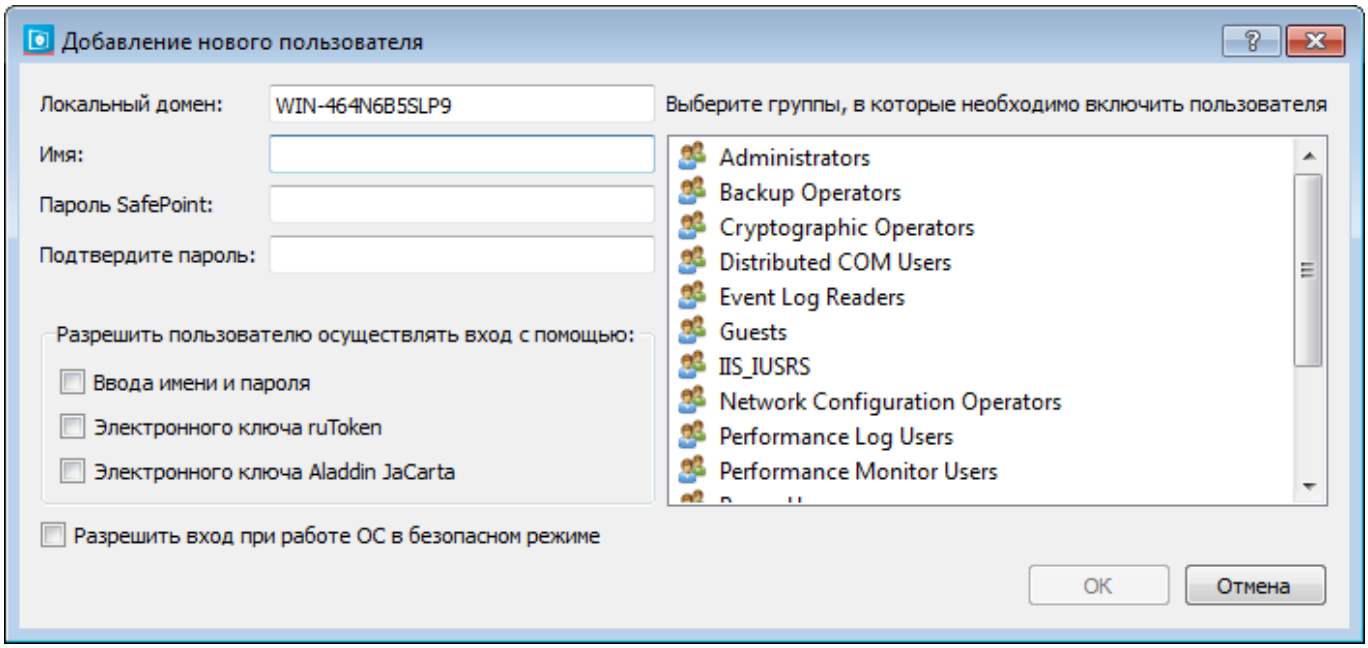


Рис.5.4.1.2. Окно добавления новой учетной записи пользователя, флаг «Использовать одинаковые пароли» установлен

5. В поле «Имя» ввести имя учетной записи пользователя, которую необходимо завести в СЗИ «ViPNet SafePoint» и добавить в Windows.
6. В поля для ввода пароля в зависимости от заданного ранее режима (с использованием одинаковых паролей или нет) следует ввести пароль или сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение (рис.5.4.1.2).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.1.1).

7. Выбрать группу (группы) учетных записей пользователей Windows, в которую будет включен пользователь.

Если группа не будет выбрана, то по умолчанию учетная запись пользователя будет помещена в группу «Пользователи».

8. Установить флаг «Ввод имени и пароля».

9. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
10. Нажать кнопку «ОК».

В результате проделанных настроек учетная запись пользователя появится в окне «Учетные записи» (рис.5.2.1) и будет добавлена в Windows.

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал входа/выхода пользователей».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Редактирование уже существующей в Windows учетной записи пользователя

Для редактирования уже существующей в Windows учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по учетной записи пользователя и выбрать строку «Редактировать пользователя», либо двойное нажатие левой кнопки мыши по имени учетной записи пользователя. При этом откроется окно «Редактирование данных пользователя» (рис.5.4.1.3, рис.5.4.1.4).

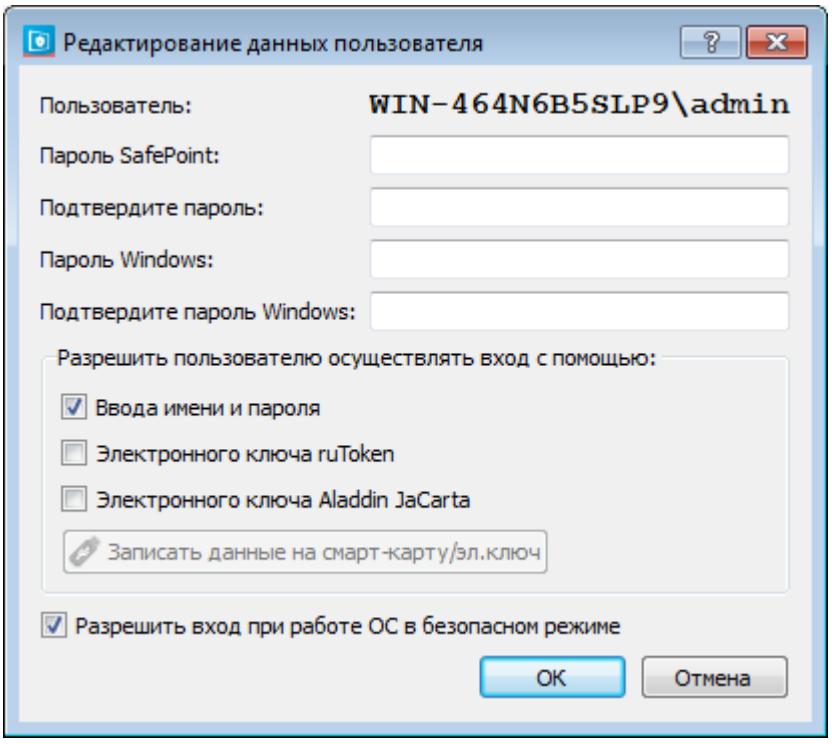


Рис.5.2.1.3. Окно редактирования данных учетных записей пользователя

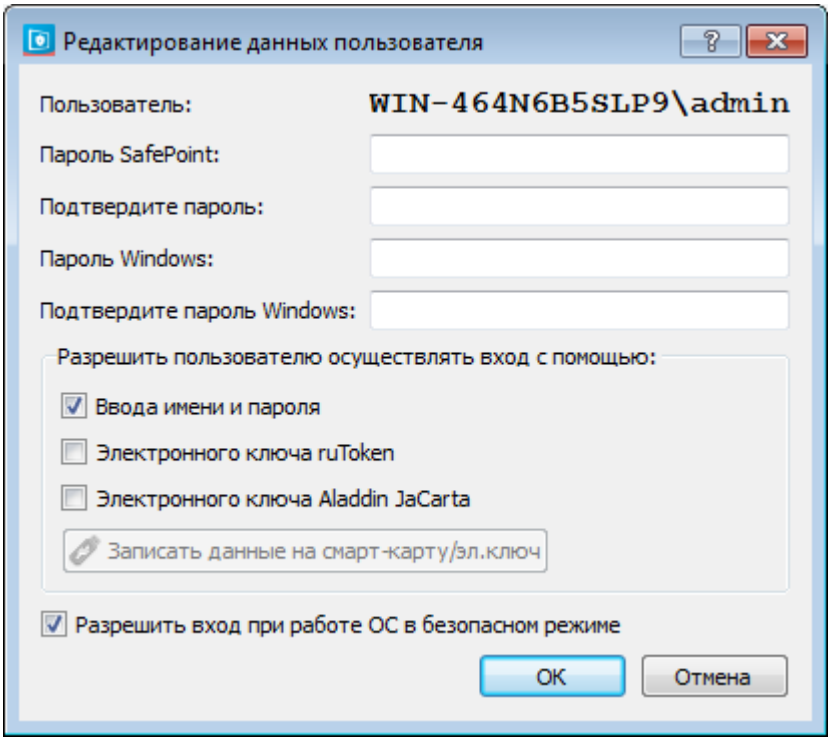


Рис.5.4.1.4. Окно редактирования данных учетных записей пользователя, флаг «Использовать одинаковые пароли» установлен

4. В зависимости от заданного ранее режима (с использованием одинаковых паролей или нет) ввести пароль или сгенерировать его двойным кликом мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение (рис.5.4.1.4).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.1.3).

В случае если установлен флаг «Позволять вход, если отсутствует пароль «ViPNet SafePoint» (рис.5.2.1), то можно поля «Пароль «ViPNet SafePoint», «Пароль Windows» и поля подтверждения пароля оставить пустыми. Тогда при первом входе пользователю нужно будет сменить пароль.

5. Установить флаг «Ввод имени и пароля».
6. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
7. Нажать кнопку «ОК».

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

Для редактирования других пользователей повторите пункты 3 – 7.

Результат заданных настроек можно посмотреть в окне «Учетные записи» (рис.5.2.1).

Для сохранения настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Смена пароля

Для смены пароля следует после входа пользователя в систему нажать сочетание кнопки «Ctrl», «Alt», «Del» и выполнить в появившемся окне (рис.5.8.1) следующие действия:

1. В поле «Пароль» ввести существующий пароль «ViPNet SafePoint». В случае отсутствия пароля «ViPNet SafePoint» в данное поле вводится пароль Windows.

2.1. Если требуется *изменить пароль «ViPNet SafePoint»*, то необходимо в поле «Новый пароль» и «Подтверждение» ввести новый пароль «ViPNet SafePoint» или создать случайный пароль при помощи генератора паролей СЗИ «ViPNet SafePoint». В поля «Новый пароль Windows» и «Подтверждение пароля Windows» следует ввести текущий пароль Windows;

2.2. Если требуется *изменить пароль Windows*, то необходимо в поле «Новый пароль Windows» и «Подтверждение пароля Windows» ввести новый пароль Windows или создать случайный пароль при помощи генератора паролей СЗИ «ViPNet SafePoint». В поля «Новый пароль» и «Подтверждение» следует ввести текущий пароль «ViPNet SafePoint».

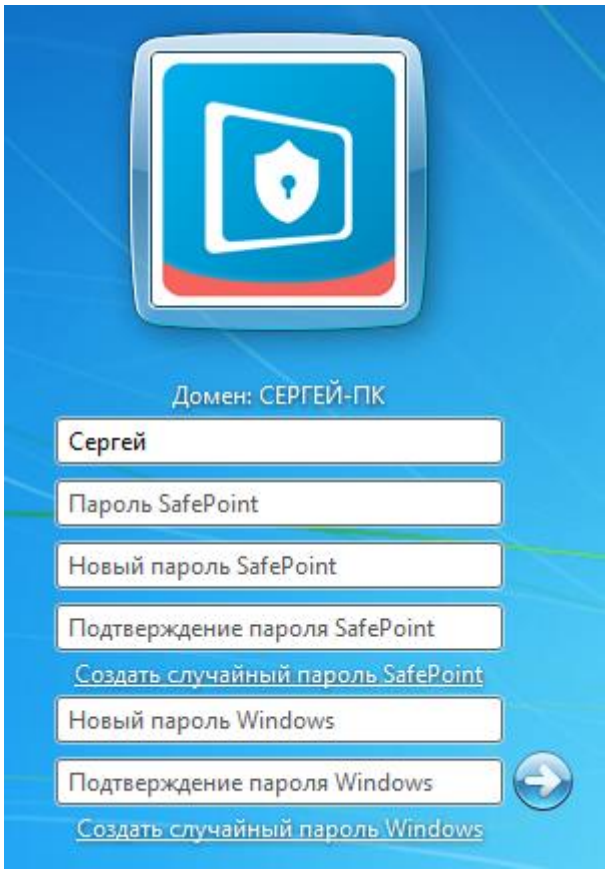


Рис.5.4.1.6. Окно смены пароля Windows или СЗИ «ViPNet SafePoint»

Сменить пароль возможно и через интерфейс «Управление настройками». Для этого следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» открыть «Учетные записи».
2. Нажать правой кнопкой мыши по имени учетной записи пользователя или выделить имя учетной записи пользователя и нажать кнопку «Enter» или двойным щелчком левой кнопкой мыши вызвать окно редактирования данных учетной записи пользователя.
3. В зависимости от выбранного ранее режима (с использованием одинаковых паролей или нет) ввести пароль или сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

5.4.2. Аутентификация по электронному ключу или по смарт-карте ruToken

При извлечении ключа происходит блокировка рабочего стола.

В случае, когда ключ был вставлен после загрузки окна авторизации, появление окна для ввода пин-кода появится с временной задержкой.

Создание новой учетной записи пользователя средствами СЗИ «ViPNet SafePoint»

Для создания новой учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» открыть «Учетные записи».
3. Нажать правой кнопкой мыши по пустому окну «Учетных записей».
4. В появившемся контекстном меню выбрать «Добавить пользователя». Появится окно «Добавление нового пользователя» (рис.5.4.2.1, рис.5.4.2.2).

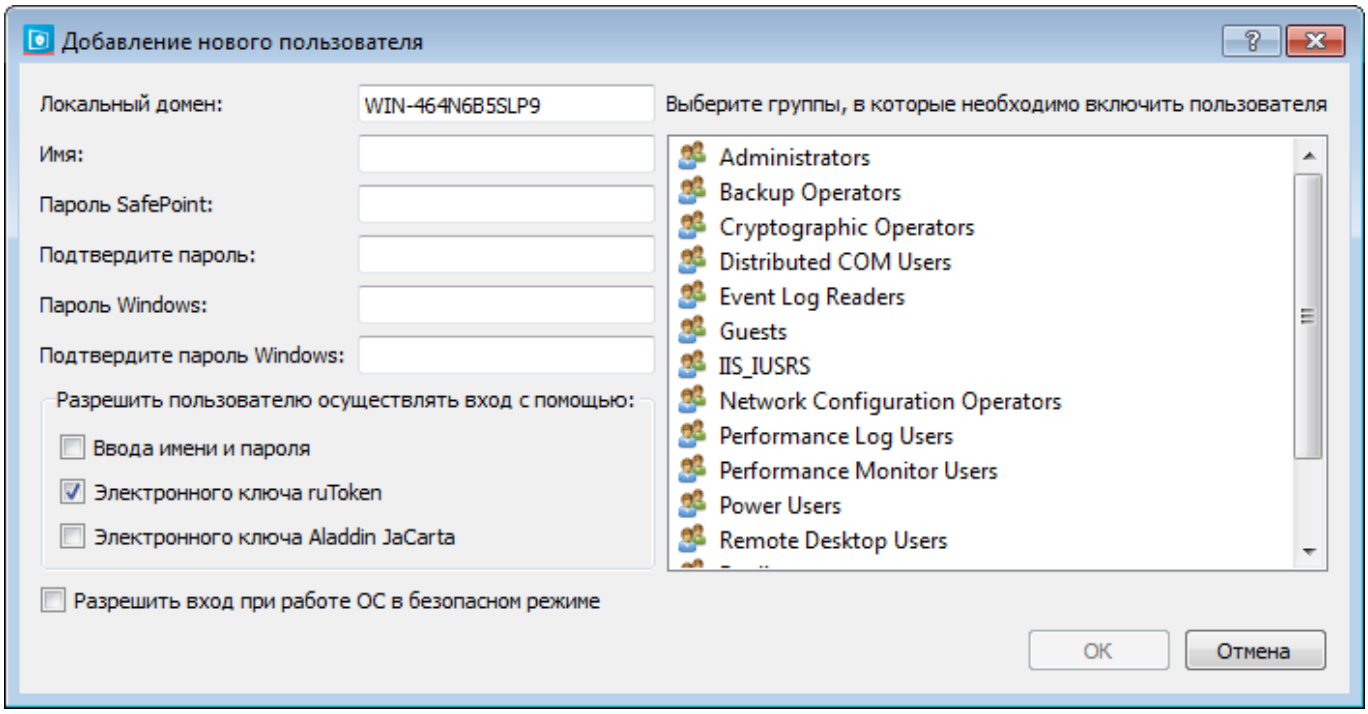


Рис.5.4.2.1. Окно добавления новой учетной записи пользователя

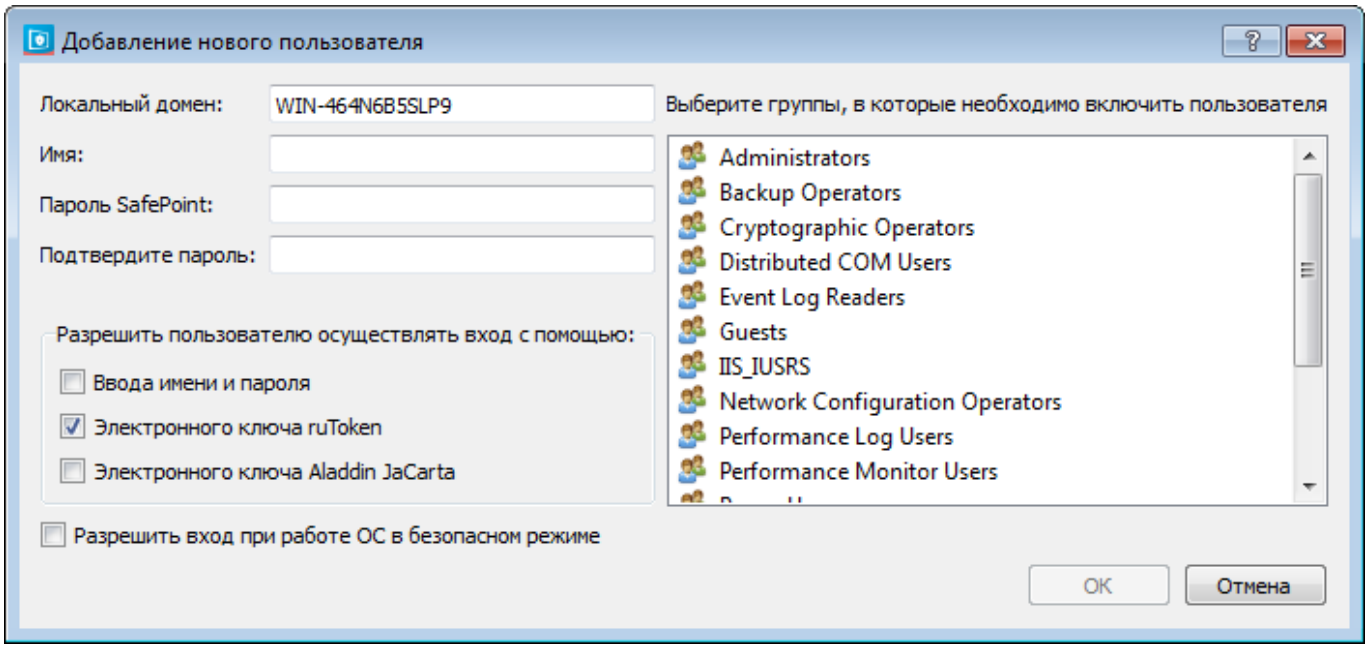


Рис.5.4.2.2. Окно добавления новой учетной записи пользователя, флаг «Использовать одинаковые пароли» установлен

5. В поле «Имя» ввести имя учетной записи пользователя, которую необходимо завести в СЗИ и добавить в Windows.
6. В поля для ввода пароля в зависимости от заданного ранее режима (с использованием одинаковых паролей или нет) следует ввести пароль или сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль СЗИ «ViPNet SafePoint» и его подтверждение (рис.5.4.2.2).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.2.1).

7. Выбрать группу (группы) учетных записей пользователей Windows, в которую будет включен пользователь.

Если группа не будет выбрана, то по умолчанию учетная запись пользователя будет помещена в группу «Пользователи».

8. Установить флаг «Электронного ключа ruToken».
9. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
10. Нажать кнопку «ОК».
11. В появившемся всплывающем окне «PIN ключа ruToken» (рис.5.4.2.3) ввести пин-код от ключа и, в случае необходимости, выставить флаг «Запомнить PIN на ключе».

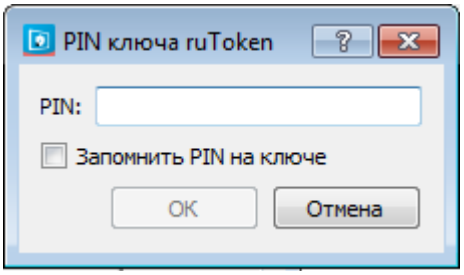


Рис.5.4.2.3. Окно ввода пин-кода ключа ruToken

Существует возможность установить флаг «Запомнить PIN на ключе» для отдельных пользователей. При входе пользователя в систему в этом случае будет реализовываться однофакторная аутентификация.

Если флаг будет установлен «Запомнить PIN на ключе», то для его изменения необходимо заново редактировать учетную запись пользователя, при этом не устанавливать флаг «Запомнить PIN на ключе». Отсутствует возможность снять данный флаг через интерфейс СЗИ.

12. Нажать кнопку «ОК».

При правильной настройке имя пользователя должно отображаться зеленым цветом.

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

В результате заданных настроек учетная запись пользователя появится в окне «Учетные записи» (рис.5.2.1) и будет добавлена в Windows.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал входа/выхода пользователей».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Редактирование уже существующей в Windows учетной записи пользователя

Для редактирования уже существующей в Windows учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по учетной записи пользователя и выбрать строку «Редактировать пользователя», либо двойное нажатие левой кнопки мыши по имени учетной записи пользователя. При этом откроется окно «Редактирование данных пользователя» (рис.5.4.2.4, рис.5.4.2.5).

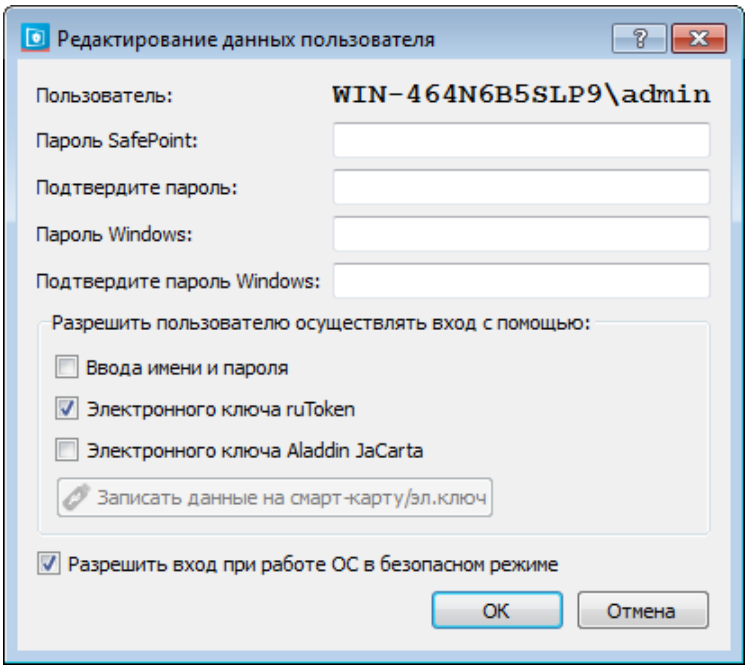


Рис.5.4.2.4. Окно редактирования данных учетных записей пользователя

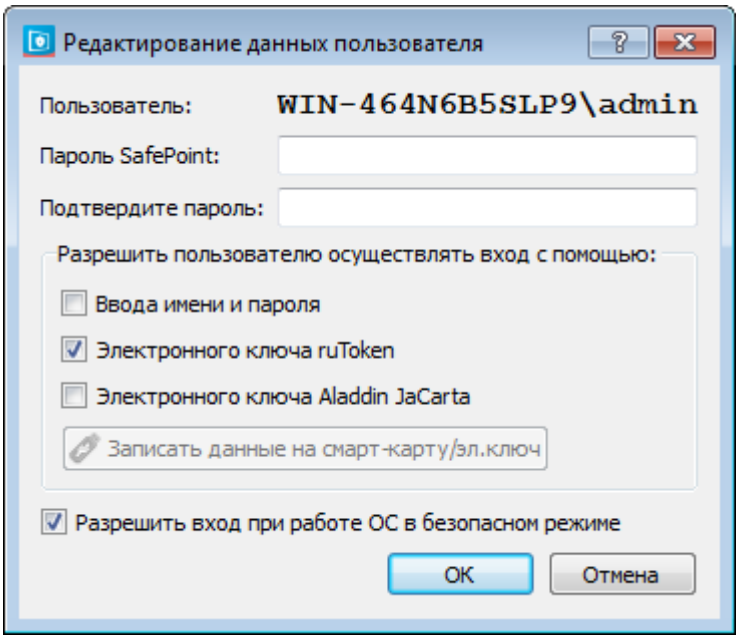


Рис.5.4.2.5. Окно редактирования данных учетных записей пользователя, флаг «Использовать одинаковые пароли» установлен

4. В поля для ввода пароля в зависимости от заданного ранее режима (с использованием одинаковых паролей или нет) следует ввести пароль или сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение (рис.5.4.2.5).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.2.4).

5. Установить флаг «Электронного ключа ruToken».
6. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
7. Нажать кнопку «ОК».
8. В появившемся окне «PIN ключа ruToken» (рис.5.4.2.6) ввести пин-код от ключа и, в случае необходимости, выставить флаг «Запомнить PIN на ключе».

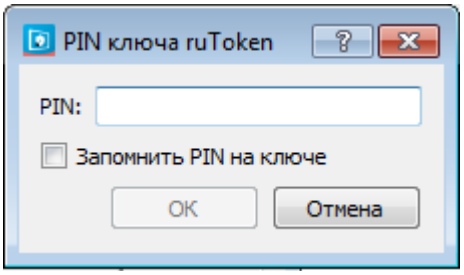


Рис.5.4.2.6. Окно ввода пин-кода ключа ruToken

Существует возможность установить флаг «Запомнить PIN на ключе» для отдельных пользователей. При входе пользователя в систему в этом случае будет реализовываться однофакторная аутентификация.

9. Нажать кнопку «ОК».

При правильной настройке имя пользователя должно отображаться зеленым цветом.

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается

автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

Результат заданных настроек можно посмотреть в окне «Учетные записи» (рис.5.2.1).

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал входа/выхода пользователей».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

5.4.3. Аутентификация по электронному ключу или по смарт-карте Aladdin JaCarta

Для совместной работы СЗИ «ViPNet SafePoint» с электронным ключом или смарт-картой Aladdin JaCarta следует использовать драйвера для Единого Клиента JaCarta и JaCarta SecurLogon (JaCartaUnifiedClient).

При извлечении ключа происходит блокировка рабочего стола.

В случае, когда ключ был вставлен после загрузки окна авторизации, появление окна для ввода пин-кода появится с временной задержкой.

Создание новой учетной записи пользователя средствами СЗИ «ViPNet SafePoint»

Для добавления новой учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по пустому окну «Учетных записей».
4. В появившемся контекстном меню выбрать «Добавить пользователя». Появится окно «Добавление нового пользователя» (рис.5.4.3.1, рис.5.4.3.2).

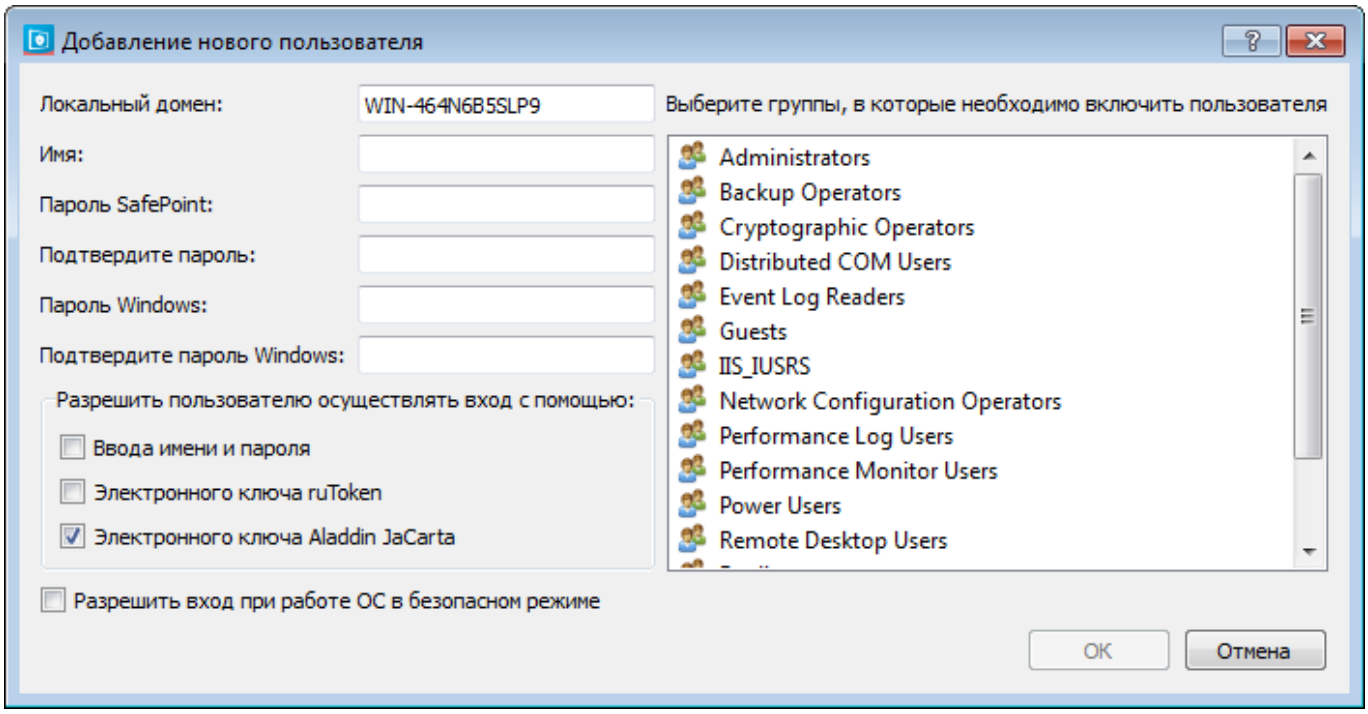


Рис.5.4.3.1. Окно добавления новой учетной записи пользователя

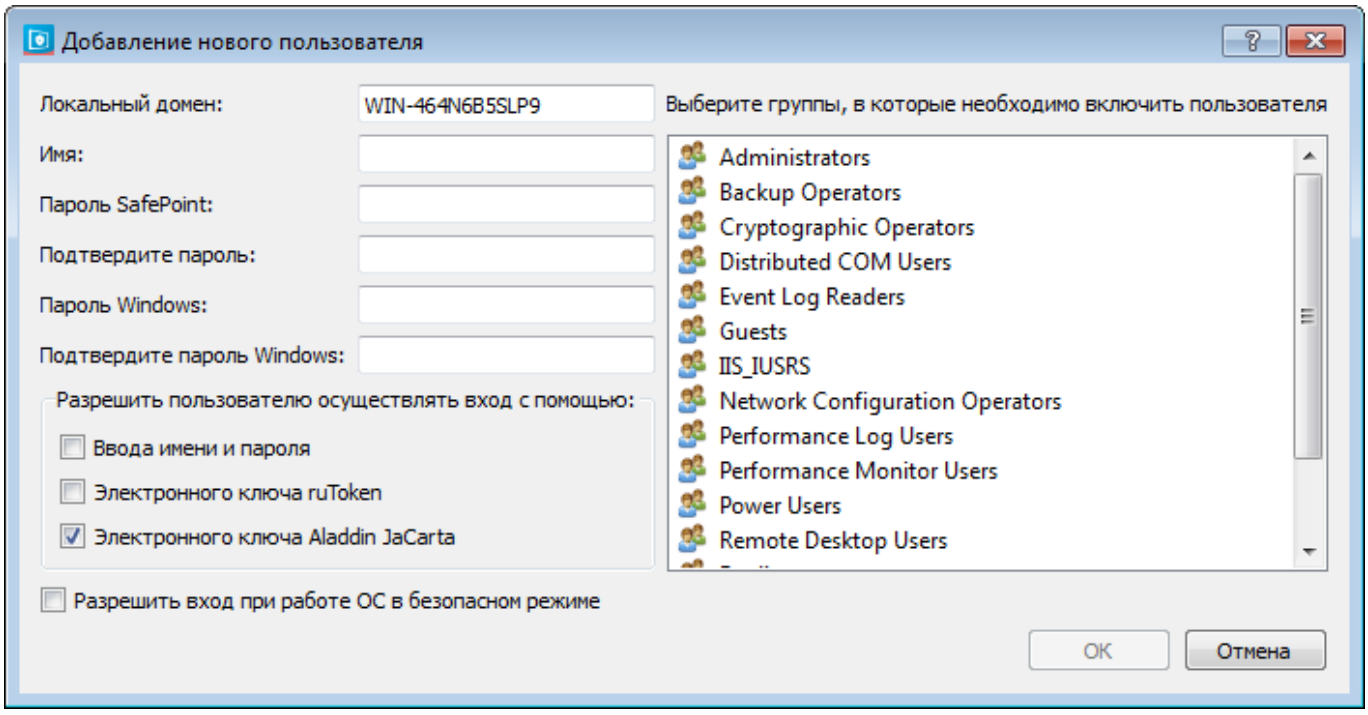


Рис.5.4.3.2. Окно добавления новой учетной записи пользователя, флаг «Использовать одинаковые пароли» установлен

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли» то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение.

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли» то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением.

5. В поле «Имя» ввести имя учетной записи пользователя, которую необходимо завести в СЗИ «ViPNet SafePoint» и добавить в Windows.
6. В зависимости от выбранного ранее режима (с использованием одинаковых паролей или нет) ввести пароль или сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение (рис.5.4.3.2).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.3.1).

7. Выбрать группу (группы) учетных записей пользователей Windows, в которую будет включен пользователь.

Если группа не будет выбрана, то по умолчанию учетная запись пользователя будет помещена в группу «Пользователи».

8. Установить флаг «Электронного ключа Aladdin JaCarta».
9. Нажать кнопку «ОК».
10. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
11. В появившемся всплывающем окне «PIN ключа JaCarta» (рис.5.4.3.3) ввести пин-код от JaCarta или смарт-карты и, в случае необходимости, выставить флаг «Запомнить PIN на ключе».

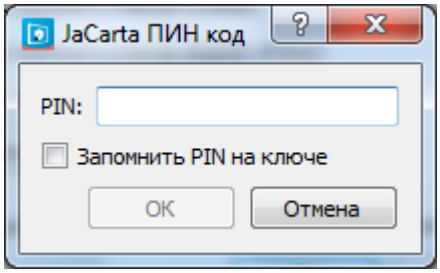


Рис.5.4.3.3. Окно ввода пин-кода ключа JaCarta

Существует возможность установить флаг «Запомнить PIN на ключе» для отдельных пользователей. При входе пользователя в систему в этом случае будет реализовываться однофакторная аутентификация.

12. Нажать кнопку «ОК».

При правильной настройке имя пользователя должно отображаться зеленым цветом.

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

В результате проделанных настроек учетная запись пользователя появится в окне «Учетные записи» (рис.5.2.1) и будет добавлена в Windows.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал входа/выхода пользователей».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Редактирование уже существующей в Windows учетной записи пользователя

Для редактирования уже существующей в Windows учетной записи пользователя следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по учетной записи пользователя и выбрать строку «Редактировать пользователя», либо двойное нажатие левой кнопки мыши по имени

учетной записи пользователя. При этом откроется окно «Редактирование данных пользователя» (рис.5.4.3.4, рис.5.4.3.5).

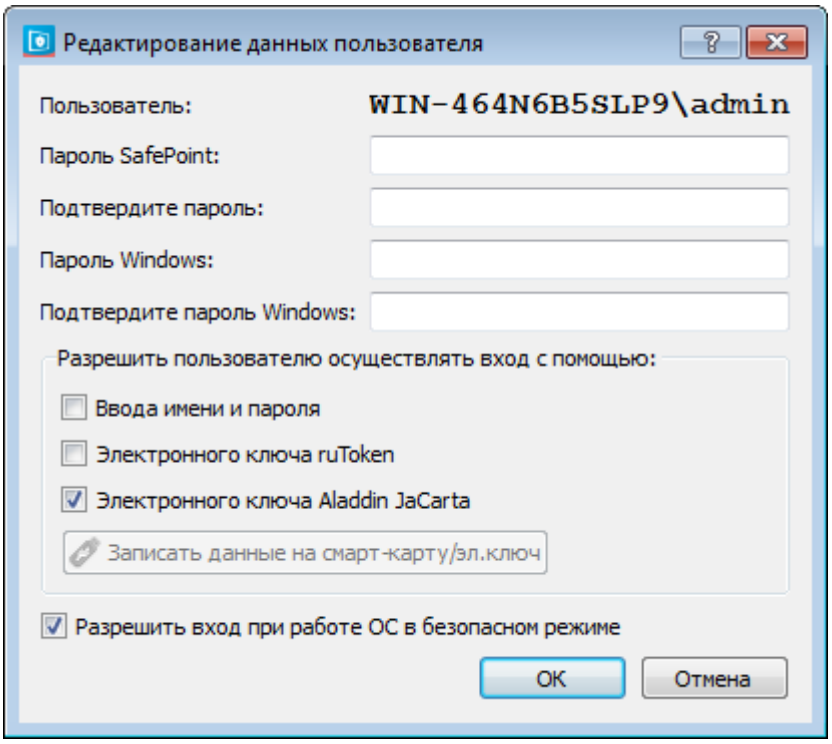


Рис.5.4.3.4. Окно редактирования данных учетных записей пользователя

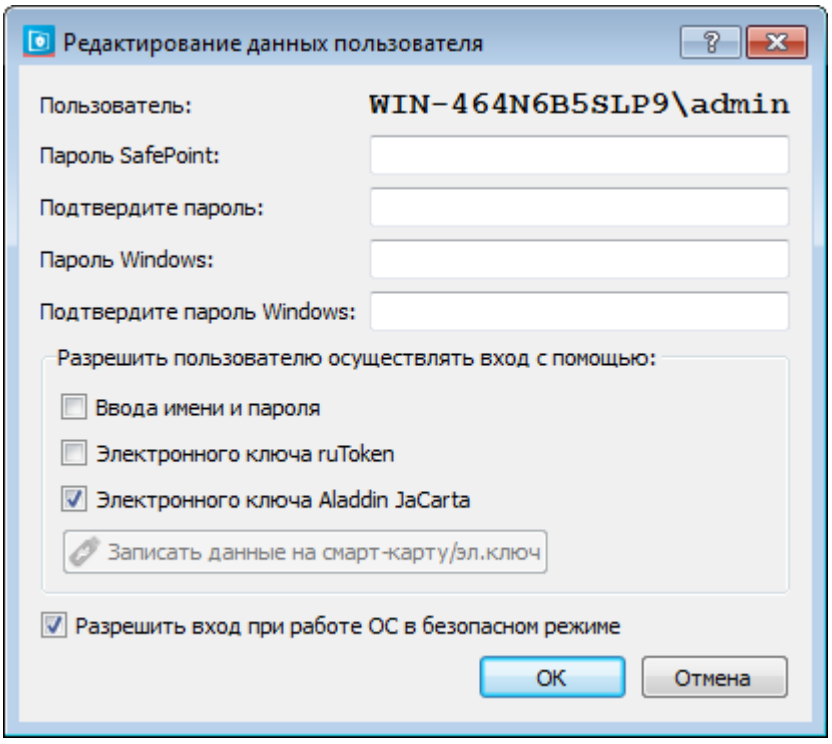


Рис.5.4.3.5. Окно редактирования данных учетных записей пользователя, флаг «Использовать одинаковые пароли» установлен

4. В поля для ввода пароля в зависимости от заданного ранее режима (с использованием одинаковых паролей или нет) следует ввести пароль или

сгенерировать его двойным нажатием левой кнопки мыши по пустому полю для ввода пароля.

Если в ранее заданных настройках «Параметры паролей» был установлен флаг «Использовать одинаковые пароли», то отображаться будет только пароль «ViPNet SafePoint» и его подтверждение (рис.5.4.3.5).

Если в ранее заданных настройках «Параметры паролей» не был установлен флаг «Использовать одинаковые пароли», то отображаться будет пароль «ViPNet SafePoint» с его подтверждением и пароль Windows с его подтверждением (рис.5.4.3.4).

5. Установить флаг «Электронного ключа Aladdin JaCarta».
6. Нажать на кнопку «Записать данные на смарт-карту/эл.ключ».
7. В появившемся окне «PIN ключа JaCarta» (рис.5.4.3.6) ввести пин-код от JaCarta или смарт-карты и, в случае необходимости, выставить флаг «Запомнить PIN на ключе».

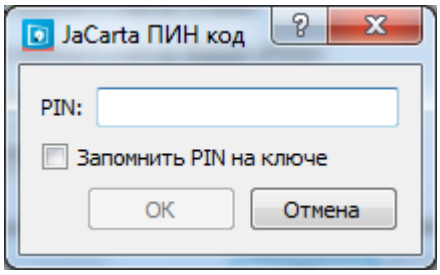


Рис.5.4.3.6. Окно ввода пин-кода ключа JaCarta

8. Нажать кнопку «ОК».
9. Установить флаг «Разрешить вход ОС при работе в безопасном режиме» (если это требуется согласно политикам безопасности).
10. Нажать кнопку «ОК».

При правильной настройке имя учетной записи пользователя должно отображаться зеленым цветом.

Установленный флаг «**Разрешить вход ОС при работе в безопасном режиме**» регламентирует возможность входа пользователей в систему при ее загрузке в безопасном режиме. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС необходимо создать в ветви реестра «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers» параметр «ProhibitFallbacks», типа «DWORD» с

присвоенным значением «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

Результат заданных настроек можно посмотреть в окне «Учетные записи» (рис.5.2.1).

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал входа/выхода пользователей».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

5.5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

5.5.1. Аутентификация при доступе к сетевым ресурсам

На машине, которая пытается получить доступ к разделенным сетевым ресурсам локальной сети, установлена СЗИ «ViPNet SafePoint» и настроена аутентификация.

В случае доступа к сетевому ресурсу через ip-адрес удаленной машины \\ip\folder или имя удаленной машины \\name\folder, а также при добавлении сетевого диска всплывает запрос на аутентификацию СЗИ «ViPNet SafePoint» (рис.5.5.1.1).

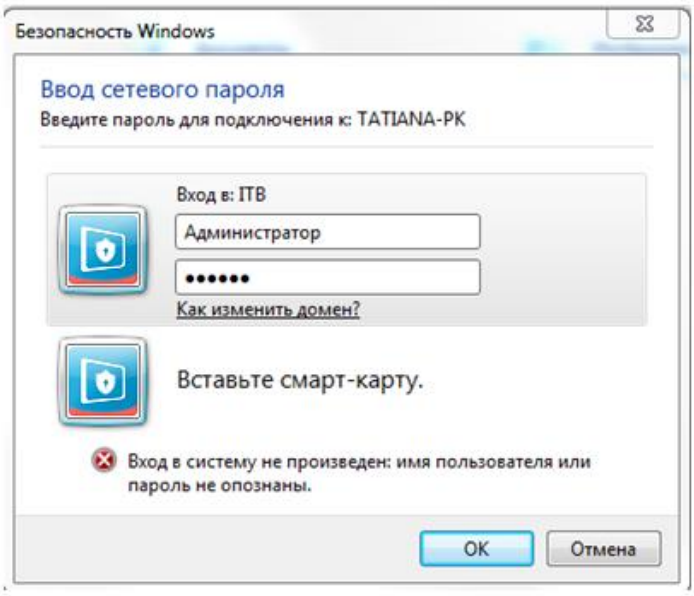


Рис.5.5.1.1 Пример получения доступа к разделенным сетевым ресурсам локальной сети

Для прохождения аутентификации в данном окне следует:

1. Ввести учетную запись пользователя в окне «Безопасность Windows» (рис.5.5.1.1), заведенного в СЗИ «ViPNet SafePoint».

Данная учетная запись пользователь должна быть добавлена в список разрешенных пользователей в механизме аутентификации СЗИ «ViPNet SafePoint» (см. в разделе 5.4).

2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).

(Также для подключения сетевого ресурса можно ввести известную учетную запись пользователя и его пароль Windows).

5.5.2. Аутентификация при подключении по RDP

1) На машине, с которой происходит подключение к другому компьютеру по RDP, установлена СЗИ «ViPNet SafePoint» и настроена аутентификация. На машине, к которой происходит подключение, также установлена СЗИ «ViPNet SafePoint» и настроена аутентификация.

При подключении к другому компьютеру по RDP всплывет окно «Безопасность Windows» (рис.5.2.2.1).

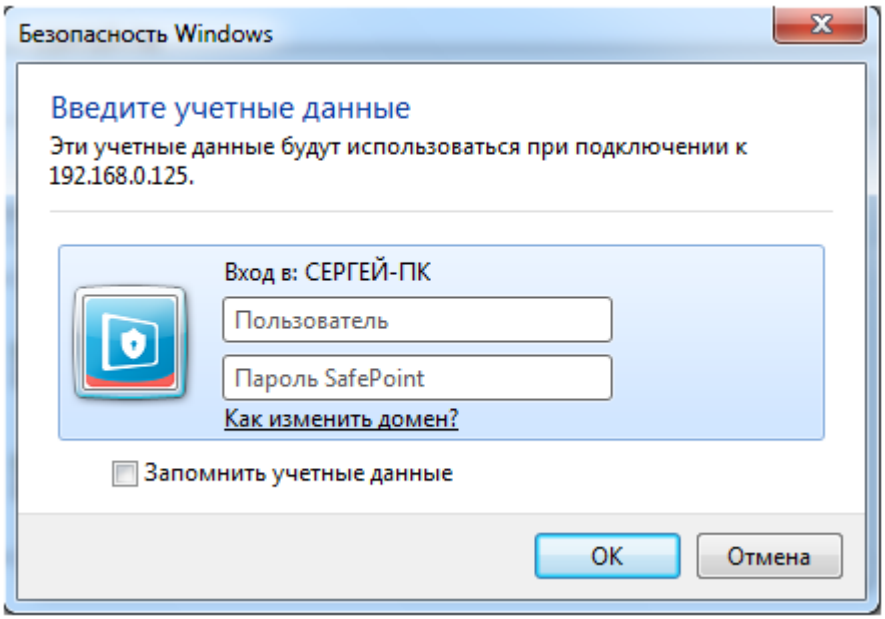


Рис.5.2.2.1 Пример подключения по RDP

Для прохождения аутентификации в данном окне следует:

1. Ввести учетную запись пользователя, от имени которого необходимо установить соединение.

Данная учетная запись пользователь должна быть добавлена в список разрешенных пользователей в механизме аутентификации СЗИ «ViPNet SafePoint» (см. в разделе 5.4).

2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).

(Также для подключения к другому компьютеру по RDP можно ввести учетную запись пользователя на удаленной машине и его пароль Windows).

3. Нажать кнопку «ОК».

Далее, после успешного подключения, в окне модуля аутентификации СЗИ необходимо:

1. Ввести учетную запись пользователя на удаленной машине.
2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).
3. Нажать кнопку «ОК».

2) На машине, с которой происходит подключение к другому компьютеру по RDP, не установлена СЗИ «ViPNet SafePoint». На машине, к которой происходит подключение, установлена СЗИ «ViPNet SafePoint» и настроена аутентификация.

При подключении к другому компьютеру по RDP всплывет окно «Безопасность Windows» (рис.5.2.2.2).

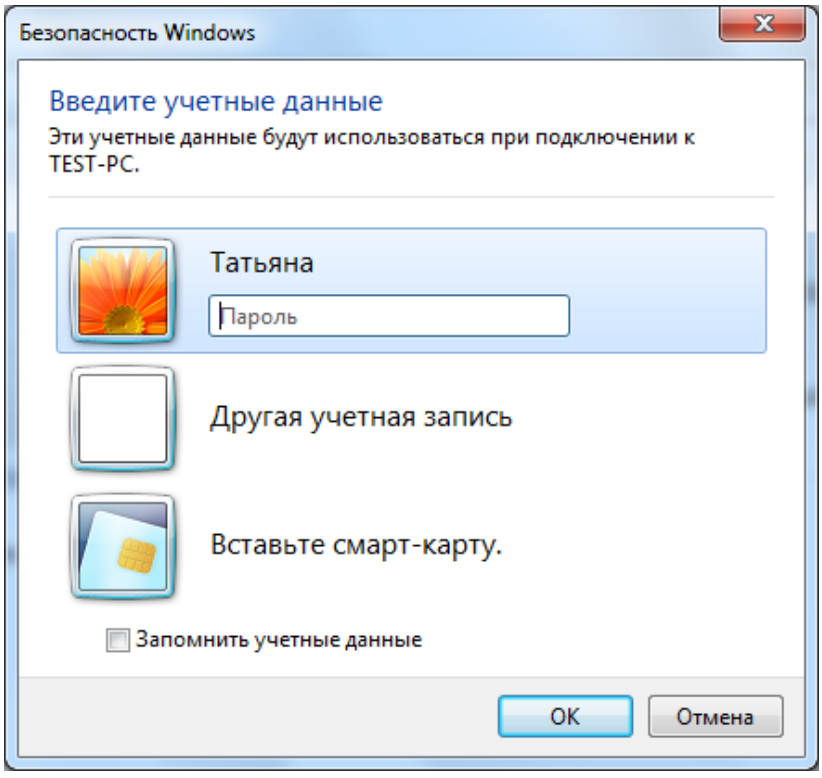


Рис.5.2.2.2 Пример подключения по RDP

Для прохождения аутентификации в данном окне следует:

1. Ввести учетную запись пользователя на удаленной машине.
2. Ввести пароль Windows или ПИН-код (в случае использования авторизации по ключу).
3. Нажать кнопку «ОК».

Далее, после успешного подключения, в окне модуля аутентификации СЗИ, необходимо:

1. Ввести учетную запись пользователя на удаленной машине.
2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).
3. Нажать кнопку «ОК».

5.5.3. Аутентификация при запуске исполняемых файлов с запросом учетных данных администратора (UAC)

При запуске исполняемых файлов от имени администратора, если подобная возможность не запрещена средствами СЗИ «ViPNet SafePoint», всплывет окно «Контроль учетных записей пользователей(UAC)» (рис.5.5.3.1):

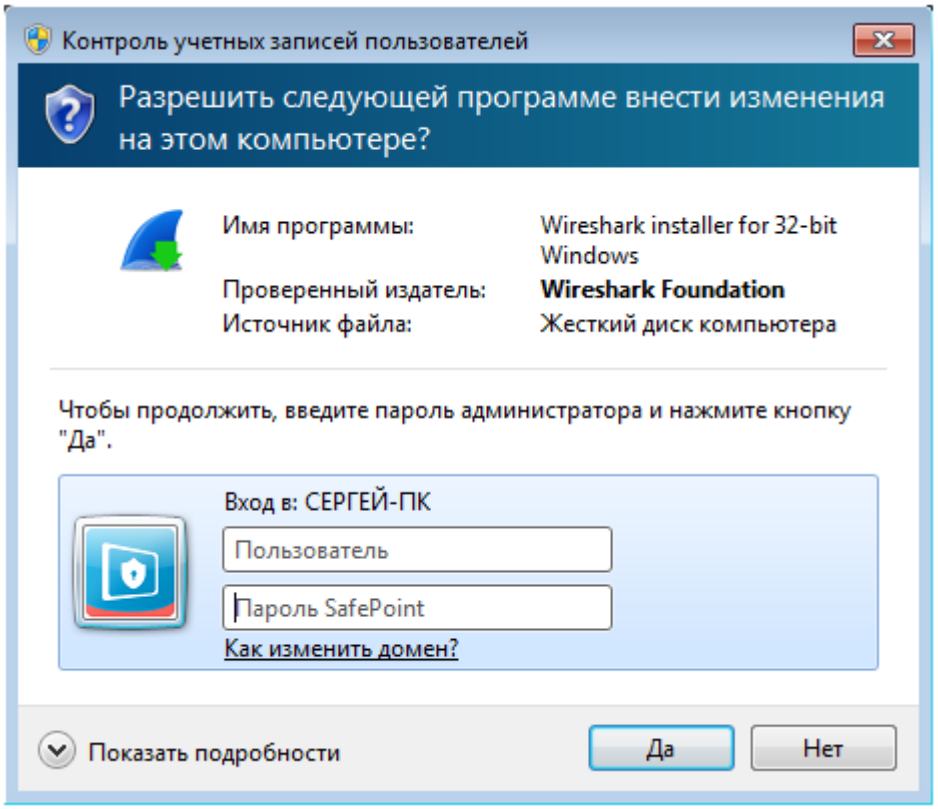


Рис.5.5.3.1. Пример запроса учетных данных администратора (UAC)

Для прохождения аутентификации в данном окне следует:

1. Ввести пользователя, являющегося администратором.

Данная учетная запись пользователя должна быть добавлена в список разрешенных пользователей в механизме аутентификации СЗИ «ViPNet SafePoint» (см. в разделе 5.4).

2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).
3. Нажать кнопку «ОК».

5.5.4. Аутентификация при блокировке экрана заставкой с парольной защитой (screensaver)

В случае использования блокировки экрана заставкой с парольной защитой, для разблокирования следует:

1. Ввести учетную запись пользователя.

Данная учетная запись пользователя должна быть добавлена в список разрешенных пользователей в механизме аутентификации СЗИ «ViPNet SafePoint» (см. в разделе 5.4).

2. Ввести пароль «ViPNet SafePoint» или ПИН-код (в случае использования авторизации по ключу).
3. Войти в систему.

5.6. БЛОКИРОВКА И РАЗБЛОКИРОВКА ПОЛЬЗОВАТЕЛЯ

Блокировка учетной записи на вход в Windows осуществляется только при включенной аутентификации средствами СЗИ «ViPNet SafePoint».

Для блокировки учетной записи пользователя, необходимо:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по необходимой учетной записи пользователя и в контекстном меню выбрать строку «Блокировать пользователя» (рис.5.6.1).

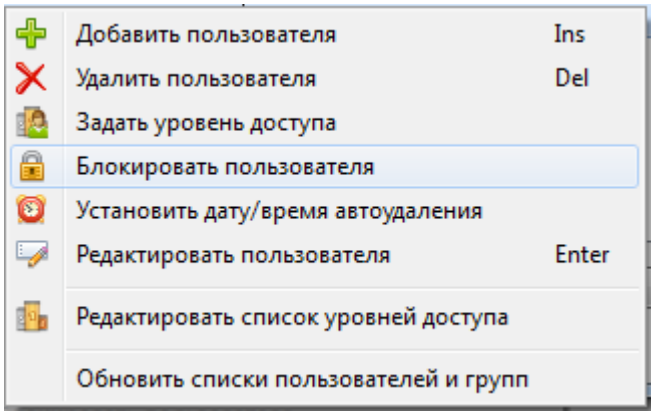


Рис.5.6.1. Блокировка пользователя

4. В появившемся окне подтверждения блокировки (рис.5.6.2) нажать «Да».

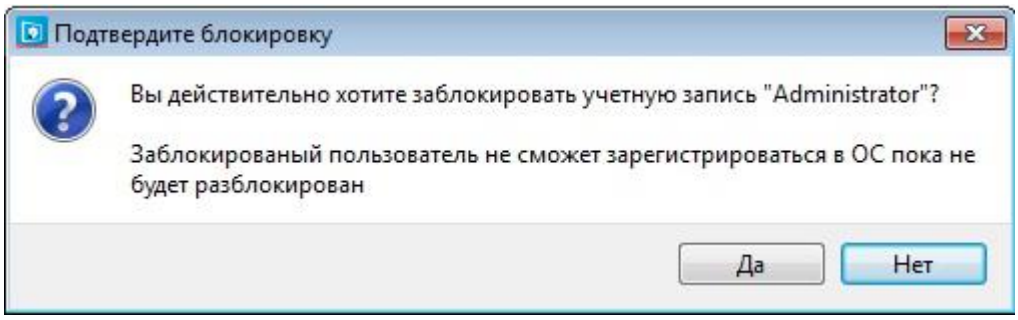


Рис.5.6.2. Окно подтверждения блокировки учетной записи пользователя

На рисунке заблокированной учетной записи пользователя устанавливается значок блокировки. Вход в систему для данной учетной записи становится невозможен.

Для разблокировки учетной записи пользователя необходимо нажать правой кнопкой мыши по необходимой учетной записи пользователя и в появившемся контекстном меню (рис.5.6.3) выбрать «Разблокировать пользователя». После чего с учетной записи пользователя будет снята блокировка.

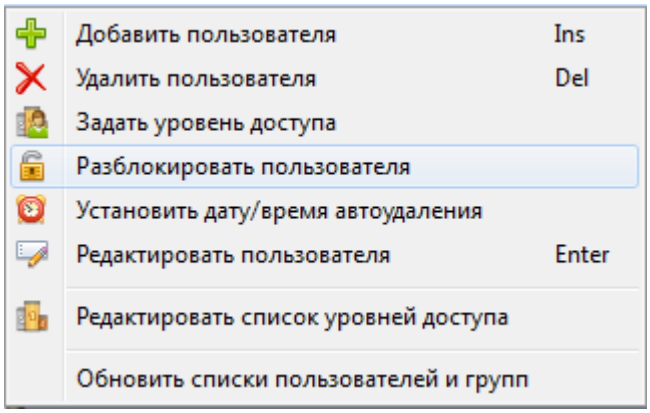


Рис.5.6.3. Разблокировка пользователя

Для сохранения настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

5.7. СМЕНА ТИПА АУТЕНТИФИКАЦИИ

Для изменения типа аутентификации следует:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по имени учетной записи пользователя или выделить имя учетной записи пользователя и нажать кнопку «Enter» или двойным щелчком вызвать меню редактирования данных учетной записи пользователя.
4. В появившемся окне «Редактирование данных пользователя» изменить на нужный тип аутентификации:
   - Для смены способа входа на *ввод логина и пароля* достаточно выбрать данный тип аутентификации, при этом для входа будет использоваться пароль, который был введен при заведении учетной записи пользователя в СЗИ «ViPNet SafePoint»;
   - Для смены на *вход по электронному ключу ruToken или Aladdin JaCarta* следует заново ввести пароль «ViPNet SafePoint», его подтверждение, пароль Windows и его подтверждение. Далее следует нажать на кнопку «Записать данные на смарткарту/эл.ключ» и в появившемся окне ввести ПИН-код, нажать кнопку «ОК»;
5. Нажать кнопку «ОК».

Для сохранения настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

5.8. УДАЛЕНИЕ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

При удалении учетной записи пользователя(ей) из СЗИ «ViPNet SafePoint», учетная запись пользователя так же удаляется и из Windows.

Для удаления учетной записи пользователя из базы СЗИ «ViPNet SafePoint» следует:

1. Открыть интерфейс «Управление настройками».
2. В меню «Управление настройками» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по необходимой учетной записи пользователя либо учетным записям пользователей, предварительно выделенных путем комбинации клавиши «Ctrl» и левой кнопки мыши.

4. В появившемся всплывающем окне (рис.5.9.1) выбрать строку «Удалить пользователя (ей)».
5. В появившемся окне «Подтверждение удаления» нажать «Да» или «Нет» (рис.5.8.1).

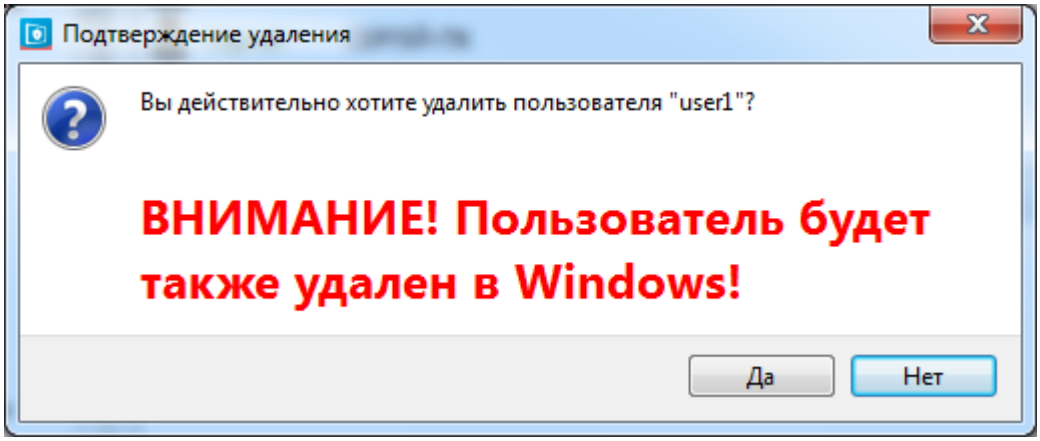


Рис.5.8.1. Окно подтверждения удаления пользователя

В СЗИ «ViPNet SafePoint» существует возможность автоматического удаления пользователя в заданное время.

Автоматическое удаление пользователей в заданное время возможно только в случае, если не реализована доменная структура.

Для удаления пользователя автоматически из системы в определенное время необходимо:

1. Открыть интерфейс «Управление настройками».
2. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать «Учетные записи».
3. Нажать правой кнопкой мыши по необходимой учетной записи пользователя и в контекстном меню выбрать «Установить дату/время автоудаления» (рис.5.8.2).

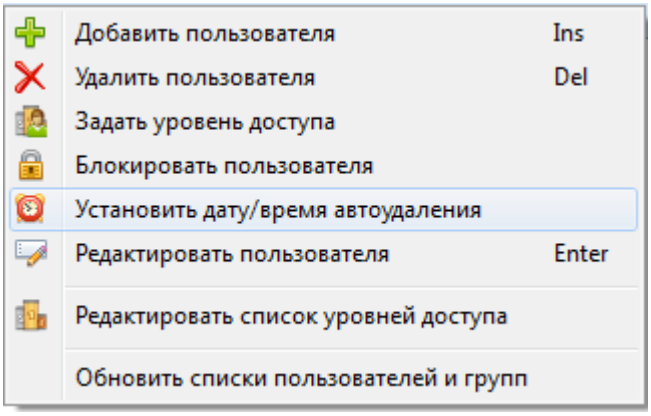


Рис.5.8.2. Удаление пользователя автоматически из системы

4. В появившемся окне задать дату и время удаления учетной записи.
5. Нажать кнопку «ОК».

Учетная запись пользователя будет удалена из СЗИ «ViPNet SafePoint» и из системы в заданный момент времени.

Для отмены автоматического удаления учетной записи пользователя необходимо нажать правой кнопкой мыши по необходимой учетной записи пользователя и в контекстном меню (рис.5.8.3) выбрать «Отменить автоудаление».

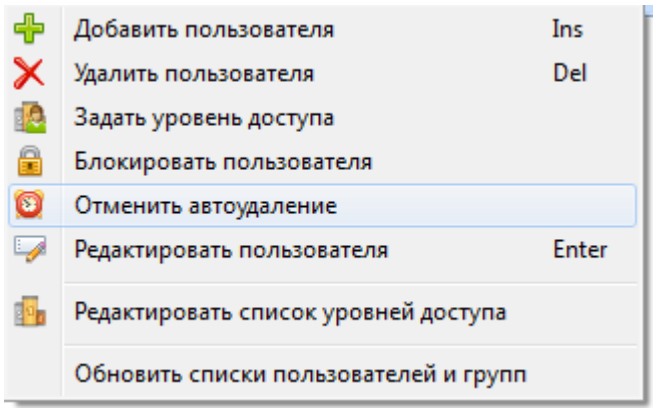


Рис.5.8.3. Отмена автоматического удаления пользователя

После чего учетная запись не будет удалена, при достижении заданной даты и времени удаления.

Для сохранения настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6. ПРОФИЛИ И СУБЪЕКТЫ ДОСТУПА

6.1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Субъект доступа – это важнейший элемент контроля доступа (реализации разграничительной политики доступа к защищаемым ресурсам), в отношении которого и реализуется разграничительная политика – именно для субъектов устанавливаются правила доступа к защищаемым ресурсам (объектам). В качестве субъекта доступа в разграничительной политике должна использоваться сущность, потенциально несущая в себе угрозу несанкционированного доступа к информации. В современных условиях эксплуатации информационных систем – это две сущности: пользователь (учетная запись) и процесс (системный процесс или приложение). Сущность «процесс» задается полнопутевым именем исполняемого файла процесса.

Без учета сущности «процесс» в средстве защиты невозможно реализовать эффективную защиту информации от несанкционированного доступа, поскольку именно процессы подвержены атакам, как сетевым, так и локальным. В широко распространенных ОС, в том числе, ОС семейства Windows, для идентификации субъектов, выполняющих в системе различные действия, используются идентификаторы защиты (security identifiers, SID). Все работающие в системе процессы и потоки выполняются в контексте защиты того пользователя, от имени которого они так или иначе были запущены, – ими наследуются права доступа к ресурсам, заданные для пользователя, т.е. для всех процессов, запущенных одним и тем же пользователем, права доступа к ресурсам одинаковы – это права доступа к ресурсам этого пользователя.

В СЗИ «ViPNet SafePoint» основными сущностями задания субъекта доступа являются эффективный пользователь (учетная запись, от лица которой происходит обращение к ресурсу), и имя процесса, т.е. в разграничительной политике доступа правила назначаются для субъекта, определяемого каким пользователем, каким процессом запрашивается доступ к ресурсу.

С точки зрения дополнительной защиты от обхода разграничительной политики доступа, в субъект доступа в СЗИ «ViPNet SafePoint» включена третья сущность первичный пользователь (учетная запись, от лица которой запущен процесс, запрашивающий доступ к ресурсу), что обусловливается решением следующей задачи защиты. Для идентификации контекста защиты процесса или потока в ОС используется объект, называемый маркером доступа (access token). В процессе регистрации в системе создается начальный маркер, представляющий пользователя, который входит в систему, и сопоставляет его с процессом оболочки, применяемой для регистрации пользователя.

Маркер может быть основным (идентифицирует контекст защиты процесса) или олицетворяющим (применяется для временного заимствования потоком другого контекста защиты

— обычно другого пользователя). Олицетворение (impersonation) — средство, используемое в модели защиты Windows, предоставляющее возможность отдельному потоку выполняться в контексте защиты отличном от контекста защиты процесса, т.е. действовать от лица другого пользователя. Олицетворение, например, применяется в модели программирования «клиент-сервер».

Таким образом, ОС предоставляет санкционированную возможность запроса и получения процессом прав другого пользователя (смены учетной записи, от лица которой будет осуществлен доступ к ресурсу), что несет в себе реальную угрозу обхода разграничительной политики доступа.

Для решения, в том числе, и задачи защиты от обхода разграничительной политики доступа к ресурсам, в СЗИ «ViPNet SafePoint» используются три сущности задания субъекта доступа: первичный пользователь (учетная запись, от лица которой запущен процесс, запрашивающий доступ к ресурсу), эффективный пользователь (учетная запись, от лица которой происходит обращение к ресурсу), и имя процесса, т.е. в разграничительной политике доступа правила назначаются для субъекта, определяемого каким пользователем запущен процесс, каким пользователем запрашивается доступ к ресурсу, каким процессом запрашивается доступ к ресурсу.

При задании субъекта доступа могут назначаться, как интерактивные, так и системные пользователи, как приложения, так и системные процессы.

В частном случае разграничения доступа могут задаваться только для пользователей (с учетом, либо без контроля сервисов олицетворения) или только для процессов. С этой целью при задании элементов субъекта доступа используется соответствующая маска «Любой» (см. далее).

При задании разграничительной политики могут использоваться не отдельные учетные записи, а группы пользователей ОС, в которые могут включаться пользователи, создаваемые в СЗИ «ViPNet SafePoint».

В СЗИ «ViPNet SafePoint» создается и используется для различных механизмов контроля доступа к ресурсам (при реализации разграничительных политики доступа к различным защищаемым ресурсам) единый список субъектов доступа.

6.2. СОЗДАНИЕ, ИЗМЕНЕНИЕ И УДАЛЕНИЕ СУБЪЕКТА ДОСТУПА

6.2.1. Создание субъекта доступа

Окно интерфейса «Субъекты доступа» представлено на рис.6.2.1. В окне отображаются информация о созданном субъекте доступа: тип, имя субъекта доступа, имя процесса, имя «эффективного» пользователя и имя «первичного» пользователя.

По умолчанию в СЗИ «ViPNet SafePoint» заведены субъекты доступа система (процесс – system, «Эффективный» пользователь – System, «Первичный» пользователь – Любой), службы (процесс – Любой, «Эффективный» пользователь – System, «Первичный» пользователь – Любой), службы СЗИ ViPNet SafePoint (процесс – %ARMOUR_ROOT%\bin*srv.exe, «Эффективный» пользователь – Любой, «Первичный» пользователь – Любой), программы СЗИ ViPNet SafePoint (процесс – %ARMOUR_ROOT%\bin*.exe, «Эффективный» пользователь – Любой, «Первичный» пользователь – Любой) и любой (процесс – Любой, «Эффективный» пользователь – Любой, «Первичный» пользователь – Любой).

Субъекты считаются различными в случае, если их имена одинаковы, но написаны буквами разных регистров (например, «IE» и «ie», «ADMIN» и «Admin»), и заданы различные наборы параметров.

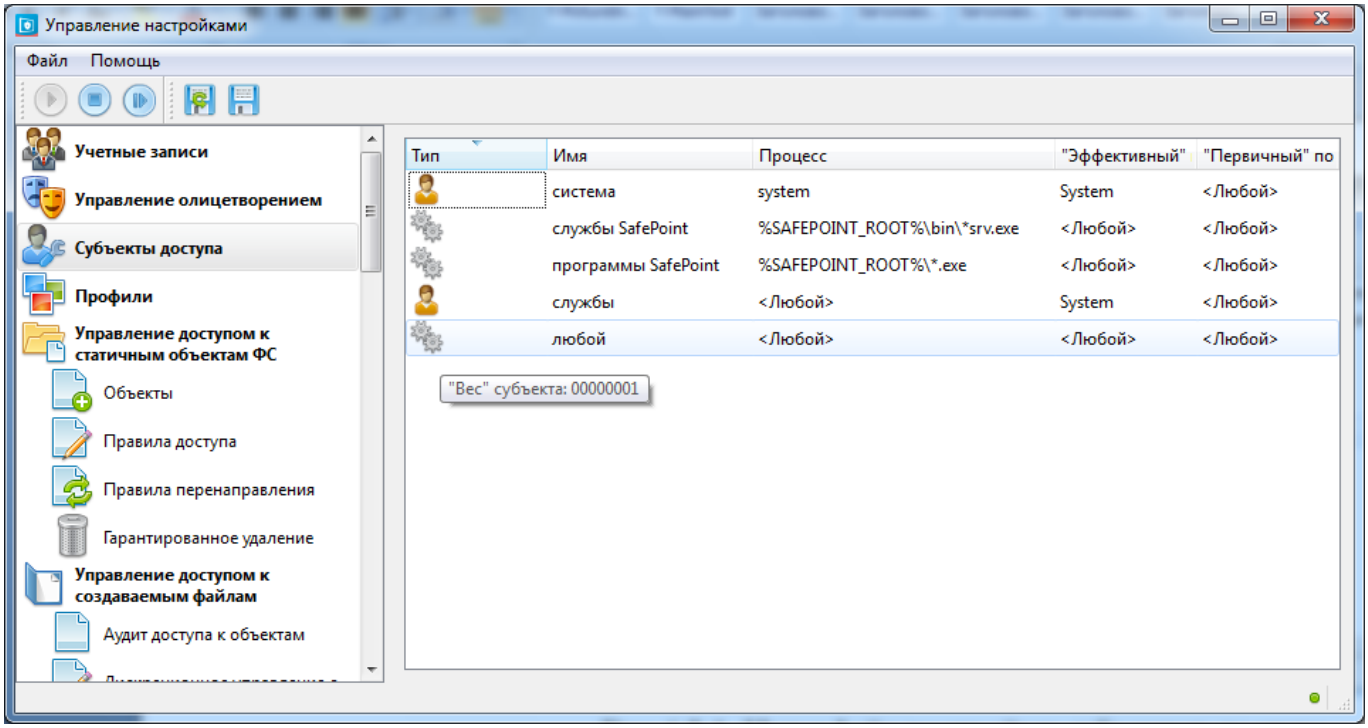


Рис.6.2.1. Интерфейс настройки субъектов доступа

Для создания субъекта доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Субъекты доступа».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Субъекты доступа» и в контекстном меню (рис.6.2.2) выбрать «Добавить субъект».

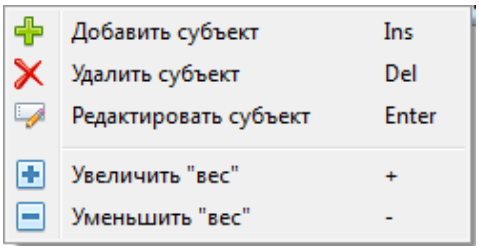


Рис.6.2.2. Контекстное меню окна «Субъекты доступа»

3. В окне «Добавление нового субъекта доступа» (рис.6.2.3) произвести следующие настройки:

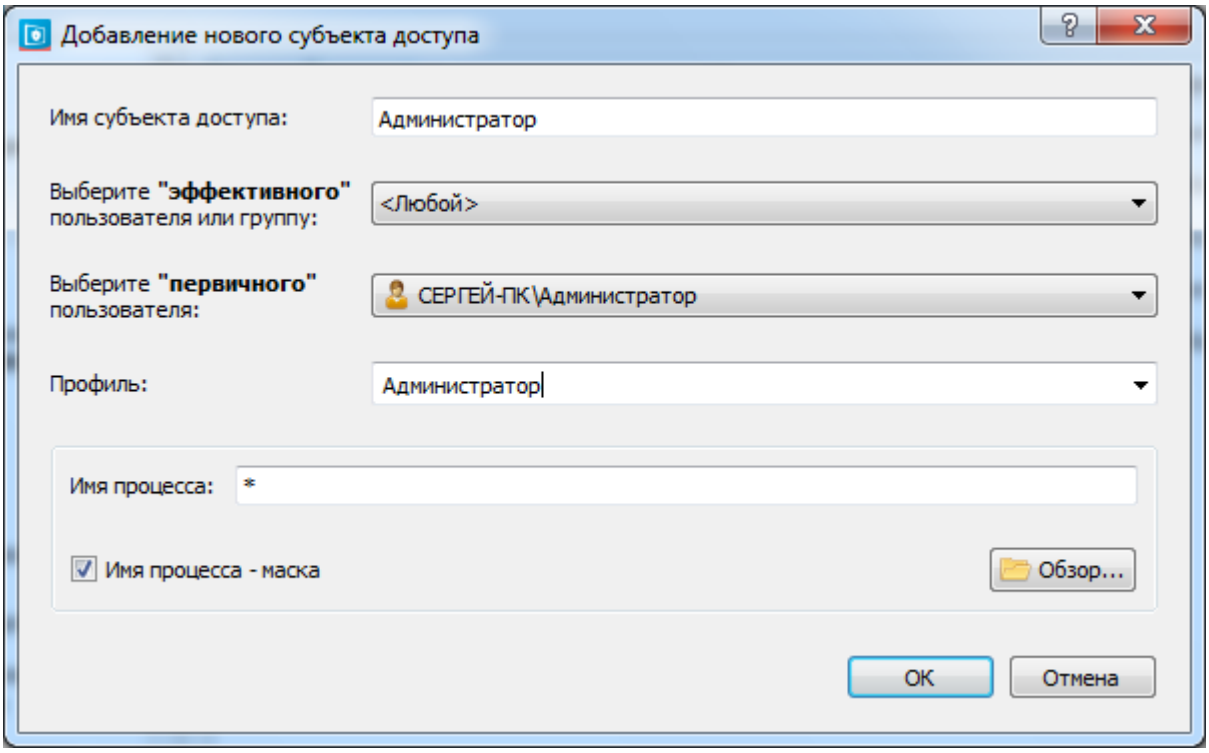


Рис.6.2.3. Окно добавления нового субъекта доступа

1) Задать «Имя субъекта доступа».
2) Выбрать «эффективного» пользователя или группу пользователей (группы пользователей операционной системы Microsoft Windows) из выпадающего списка или выбрать любого пользователя, задаваемого маской (в выпадающем списке - «Любой»).

Некоторые механизмы СЗИ «ViPNet SafePoint» могут быть настроены не только для отдельных субъектов, но и для групп пользователей.

При задании в качестве эффективного пользователя группы пользователей, автоматически в качестве первичного пользователя будет задан «Любой» и в качестве процесса также будет задан любой процесс («*»).

3) Выбрать «первичного» пользователя из выпадающего списка или выбрать любого пользователя (в выпадающем списке – «Любой»).
4) Выбрать «Профиль» из выпадающего списка или создать новый профиль, задав имя профиля.
5) Задать имя процесса (полнопутевое имя исполняемого файла процесса) вручную или используя «Обзор». Имя процесса можно задавать масками и переменными среды окружения. Если имя процесса задано маской, то следует установить флаг «Имя процесса – маска».
6) Нажать кнопку «ОК».

4. В случае если создается новый профиль в появившемся окне с вопросом «Профиль с указанным именем не существует. Создать новый?» следует выбрать «Да», в следующем появившемся окне с вопросом «Хотите скопировать правила из существующего профиля в создаваемый?» выбрать необходимый вариант. При нажатии «Да» появится окно «Выберите профиль источник», в котором необходимо выбрать профиль источник и нажать кнопку «ОК», в этом случае в новый профиль будут скопированы настройки из профиля источника; при нажатии «Нет» создастся новый профиль без настроек.
5. Если субъект будет включен в один из уже существующих профилей, субъект сразу создастся при нажатии кнопки «ОК» в окне «Добавление нового субъекта доступа» (рис.6.2.3).

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6.2.2. Изменение субъекта доступа

Существует возможность редактирования уже существующего субъекта доступа. Для этого необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Субъекты доступа».
2. Выбрать субъект.
3. Нажать правой кнопкой мыши по субъекту доступа.
4. В контекстном меню выбрать «Редактировать субъект» (рис.6.2.2).
5. В появившемся окне «Редактирование параметров субъекта доступа» внести необходимые изменения (окно повторяет окно «Добавление нового субъекта доступа» рис.6.2.3).

Включение или исключение субъекта доступа из профиля упрощает процесс администрирования системы в случае, когда:

1. Требуется включить субъект в профиль для распространения на него правил доступа, назначенных для профиля;
2. Требуется исключить субъект из профиля для задания субъекту правил доступа, отличающихся от правил, назначенных для профиля.

6. Нажать кнопку «ОК».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6.2.3. Удаление субъекта доступа

Для того чтобы удалить субъект доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Субъекты доступа».
2. Выбрать субъект.
3. Нажать правой кнопкой мыши по субъекту доступа.
4. В контекстном меню выбрать «Удалить субъект» (рис.6.2.2).
5. В появившемся окне «Подтверждение удаления» нажать «Да».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Просмотр заведенных в СЗИ «ViPNet SafePoint» субъектов осуществляется из окна интерфейса «Субъекты доступа» (рис.6.2.4). В интерфейсе отражаются тип (пиктограмма), имя субъекта, процесс, «Эффективный» и «Первичный» пользователи. При наведении курсора на имя, процесс, «Эффективного» и «Первичного» пользователей субъекта, появится всплывающее окно с уточнением. При наведении курсора на тип объекта, появится всплывающее окно, отражающее «вес» субъекта (см. раздел 6.5).

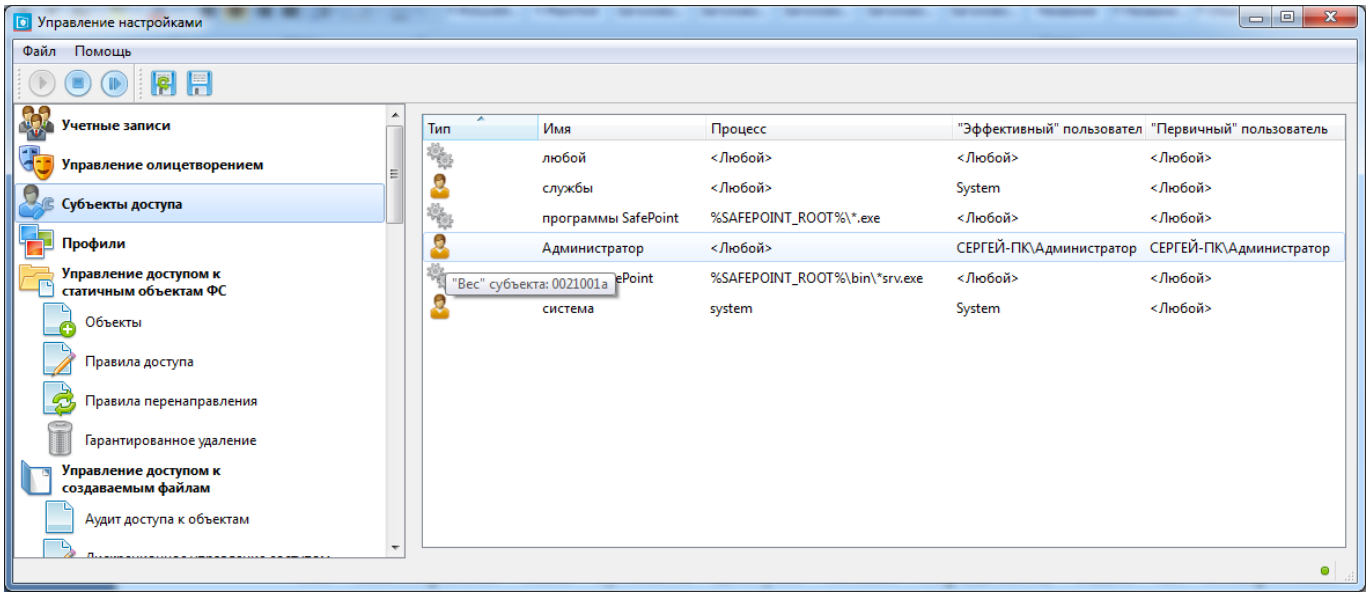


Рис.6.2.4. Просмотр заведенных субъектов доступа

По пиктограмме типа субъекта доступа можно определить, задан ли конкретный «Эффективный» пользователь –  , не задан –  , является ли субъект группой пользователей –  .

6.2.4. Использование масок при задании субъекта доступа

При задании «Эффективного» и «Первичного» пользователей в выпадающем списке можно выбрать «Любой», это подразумевает использование маски «*». Маска «*» обозначает любую последовательность символов. Задав таким образом «эффективного» и «первичного» пользователей при создании субъекта доступа, правила для этого субъекта будут распространяться на всех пользователей (учетных записей), заведенных на используемой системе, т.е. будет реализовываться контроль (разграничение прав) доступа к защищаемым ресурсам исключительно для процессов (приложений).

При создании или редактировании элемента субъекта доступа «процесс» возможно использование масок и переменных среды окружения, это позволяет упростить настройки правил разграничения доступа и задавать процессы, как из определенного каталога, так и процессы определенного типа.

Примеры масок:

- Использование маски «*» подразумевает все процессы (системные и прикладные). Если процесс в настройках определен маской «*», то разграничительная политика доступа к ресурсам реализуется исключительно для пользователей (учетных записей).

- Использование масок типа «C:\Program Files*» подразумевает все процессы из заданного каталога.
- Использование маски типа «*.exe» подразумевает все файлы с указанным расширением (тип файла).
- Маска «*iexplore.*» подразумевает все файлы с названием «iexplore» с любым расширением, находящиеся в любом каталоге.

При задании каталогов существует возможность использования переменных среды для указания, например, системного каталога. Пример задания процессов из системного каталога Program Files:

- %PROGRAMFILES%* подразумевает все файлы из каталога Program Files с установленными программами, запущенной операционной системы.

Существует возможность использования других спецсимволов и конструкций:

? – обозначает любой символ (символ в имени ресурса должен присутствовать на месте спецсимвола в маске);

+ – обозначает один и более символов (символ в имени ресурса должен присутствовать на месте спецсимвола в маске);

[набор символов] – обозначает любой символ, входящий в набор (символ в имени ресурса должен присутствовать на месте конструкции в маске);

[!набор символов] или [^набор символов] – обозначает любой символ, не входящий в набор (символ в имени ресурса должен присутствовать на месте конструкции в маске).

Набор символов может задаваться как последовательностью (например, [abcdefg]), так и диапазоном (например, [a-g]), а также комбинацией последовательности и диапазона (например, [bde-hxyz]).

Например, маска «text?.doc» покрывает все имена ресурсов с именами «text1.doc», «text2.doc», «texta.doc» и т.п.

6.2.5. «Вес» субъекта доступа в разграничительной политике. Задание и изменение

В результате использования масок, при задании элемента субъекта доступа «процесс», запрос доступа к ресурсу (в запросе процесс идентифицируется полнопутевым именем его исполняемого файла) одновременно может подпасть под несколько правил разграничительной политики. Возникает задача выбора наиболее подходящего правила при анализе корректности запроса доступа.

Пример. Пусть «процесс» в разграничительной политике доступа для разных правил задается следующими двумя способами: «*.exe» и «C:\Program Files*». Пусть доступ к ресурсу

запрашивается процессом с исполняемым файлом с расширением «exe» из каталога «C:\Program Files». Какое правило выбрать – от этого зависит реализация принципиально различных разграничительных политик. Если выбрать правило «*.exe», считая, что именно им более точно описывается субъект доступа, то все процессы с исполняемым файлом с расширением «exe» подпадут под это правило, в том числе и те из них, исполняемые файлы которых хранятся в каталоге «C:\Program Files». Для всех же иных исполняемых файлов из каталога «C:\Program Files» (с расширением не «exe») будет действовать правило для субъекта доступа «C:\Program Files*». В противном случае - если выбрать правило «C:\Program Files*», считая, что именно им более точно описывается субъект доступа – процесс, исполняемый из каталога C:\Program Files, при любом расширении его исполняемого файла, подпадет под действие правила для субъекта «C:\Program Files*», любой же процесс, исполняемый файл которого имеет расширение «exe», запускаемый не из каталога C:\Program Files, подпадет под правила разграничения доступа, заданные маской «*.exe»

При создании субъекта доступа, СЗИ «ViPNet SafePoint» субъекту автоматически (по реализованным в СЗИ «по умолчанию» правилам) присваивается его «вес». Чем более точно, с точки зрения этих правил, заданы параметры субъекта доступа (точнее описатель субъекта доступа в разграничительной политике), тем больше «вес» субъекту присваивается СЗИ «ViPNet SafePoint». При выборе между несколькими правилами, под которые подпадает запрос доступа, для анализа корректности запроса доступа в силу вступит то правило (будет выбрано для анализа), у которого «вес» больше. При реализации конкретных разграничительных политик администратору может потребоваться изменить «вес» субъекта (изменить «вес» субъекта доступа, автоматически установленный СЗИ), определив тем самым иное правило, характеризуемое более точным описателем субъекта доступа.

Для увеличения или уменьшения «веса» субъекта необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Субъекты доступа».
2. Нажать правой кнопкой мыши по субъекту.
3. В контекстном меню выбрать «Уменьшить «вес»» либо «Увеличить «вес»» (рис.6.5.1).

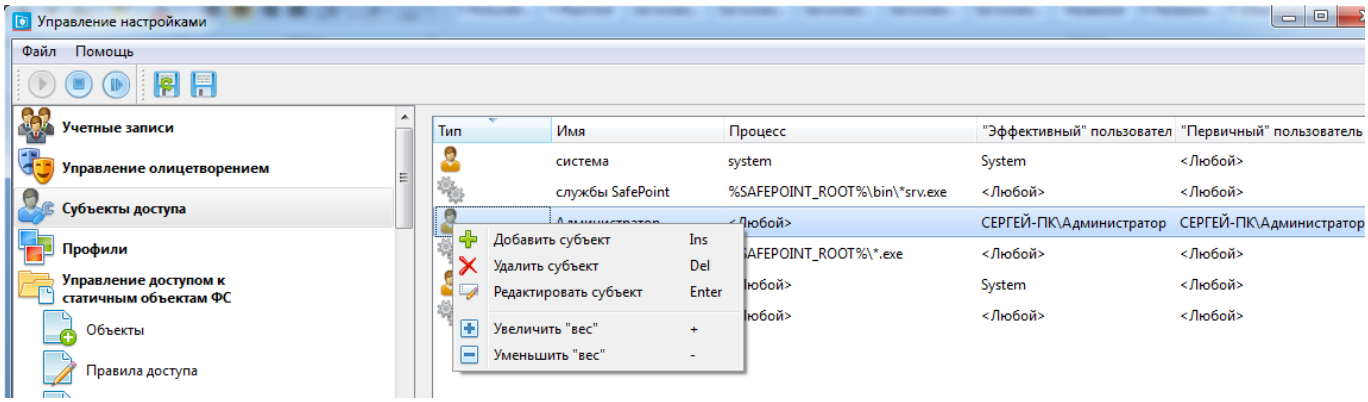


Рис.6.5.1. Контекстное меню окна «Субъекты доступа»

В интерфейсе «Субъекты доступа» субъекты представлены в порядке увеличения их «веса» (либо снизу вверх, либо сверху вниз). Для просмотра «веса» субъекта необходимо навести курсор на пиктограмму типа выбранного субъекта (рис.6.5.2). После изменения «веса» субъекта доступа, при увеличении он переместится на позицию выше, при уменьшении – ниже (или наоборот, при инверсном отображении) (рис.6.5.3).

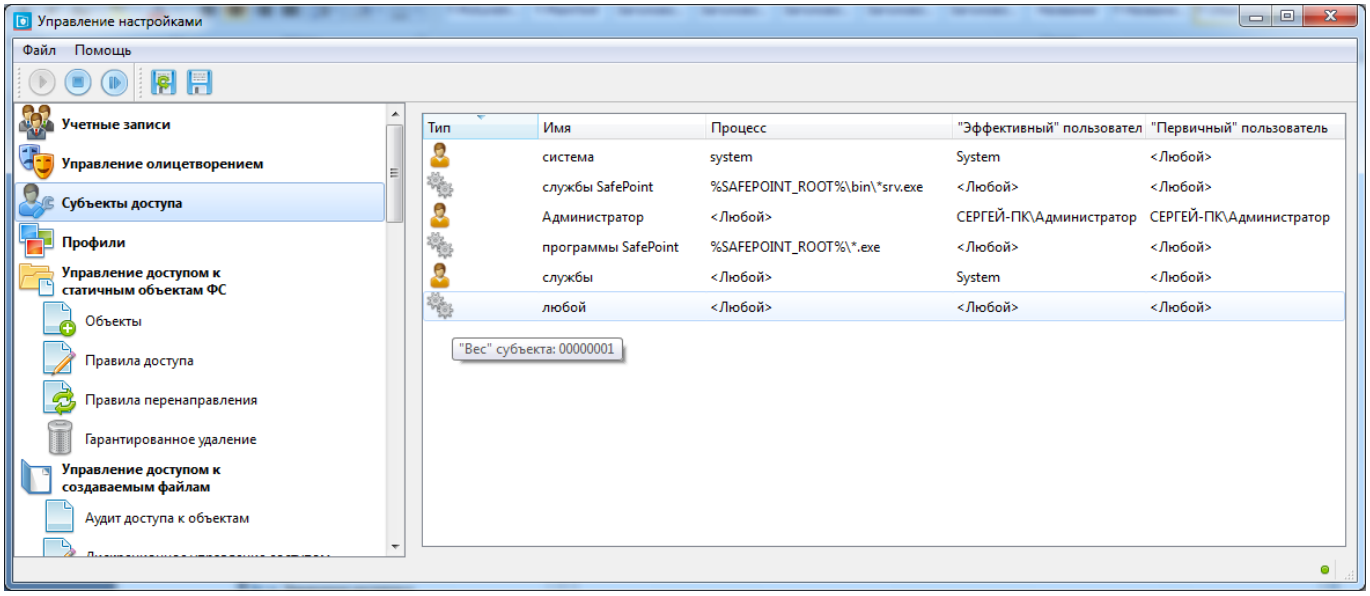


Рис.6.5.2. Просмотр субъектов доступа в порядке увеличения веса снизу вверх

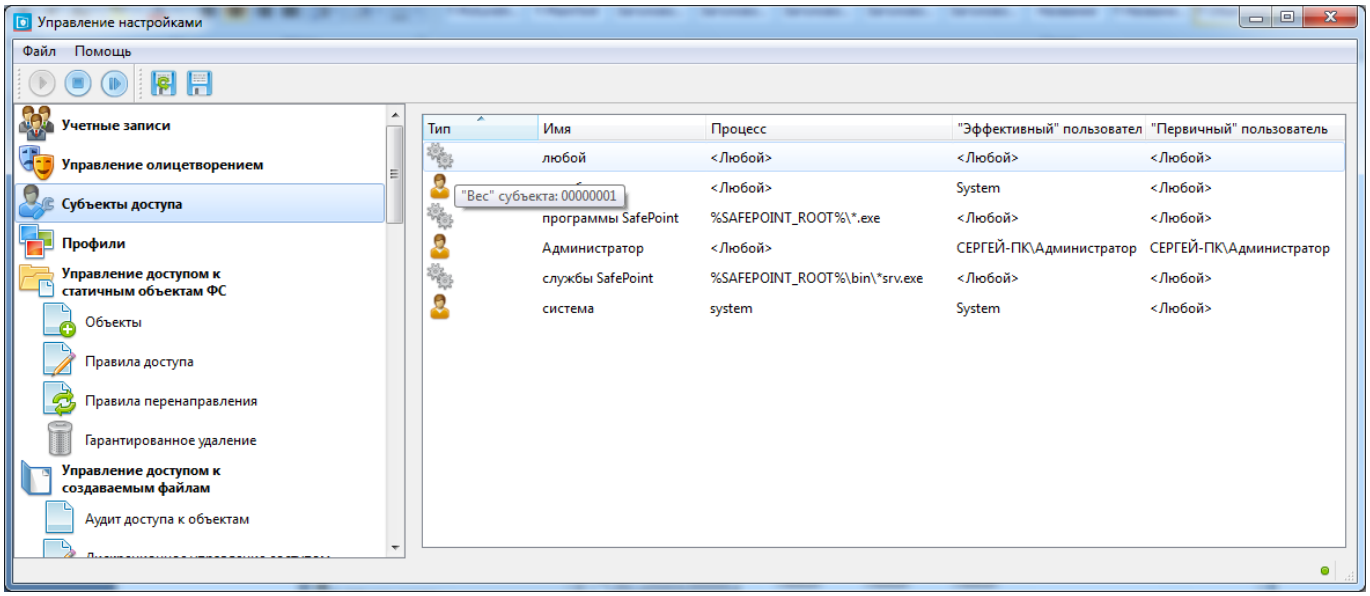


Рис.6.5.3. Просмотр субъектов доступа в порядке увеличения веса сверху вниз

«Вес» субъектов, находящихся в начале и конце списка, может быть изменен только в одну сторону. Т.к. субъекты представлены в порядке увеличения их «веса».

При достижении субъектом крайних положений в списке, «вес» не сможет быть уменьшен или увеличен, т.к. субъекты, находящиеся в этих положениях, обладают наименьшим или наибольшим «весом» соответственно (рис.6.5.4).

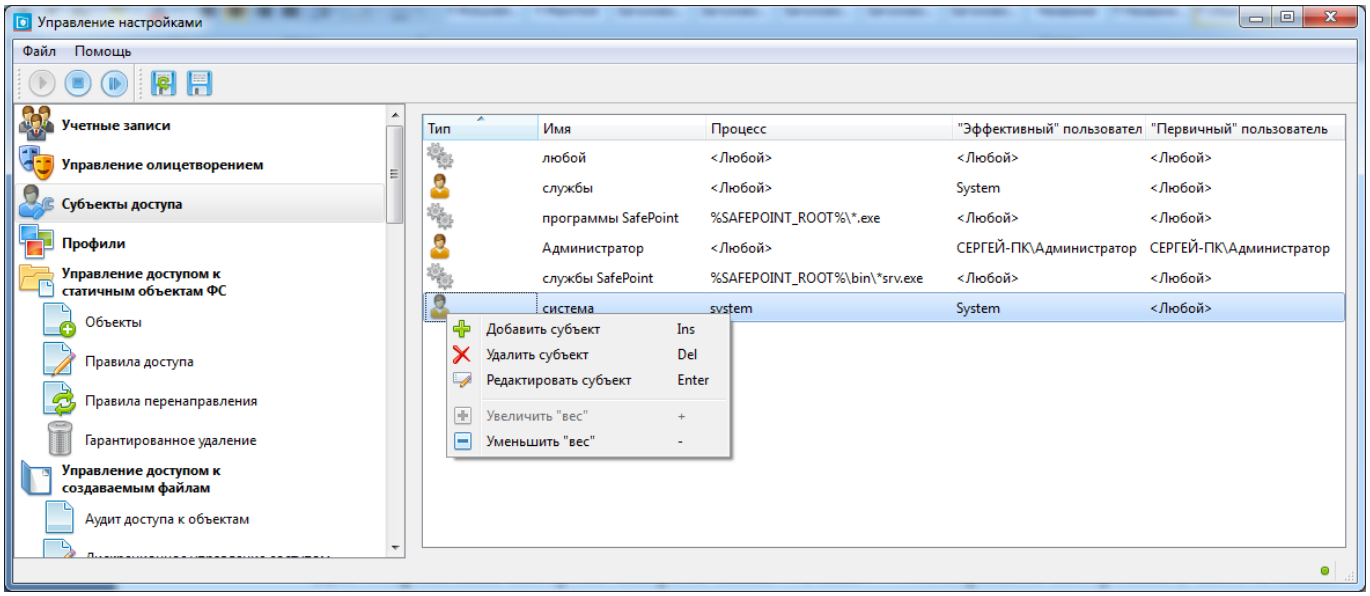


Рис.6.5.4. Изменение «веса» субъектов доступа в крайних положениях списка

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6.3. *СОЗДАНИЕ, РЕДАКТИРОВАНИЕ И УДАЛЕНИЕ ПРОФИЛЯ*

6.3.1. Создание профиля

Окно интерфейса «Профили» представлено на рис.6.3.1, рис.6.3.2. В окне отображается информация о созданном профиле. Существует два варианта отображения связи профилей и субъектов доступа. В первом случае отображаются: имя профиля и субъекты, принадлежащие к данному профилю (рис.6.3.1). Во втором случае отображаются субъект доступа и профили, в которые он входит (рис.6.3.2). Этот режим предназначен только для удобства просмотра всех субъектов и профилей, в которые они включены.

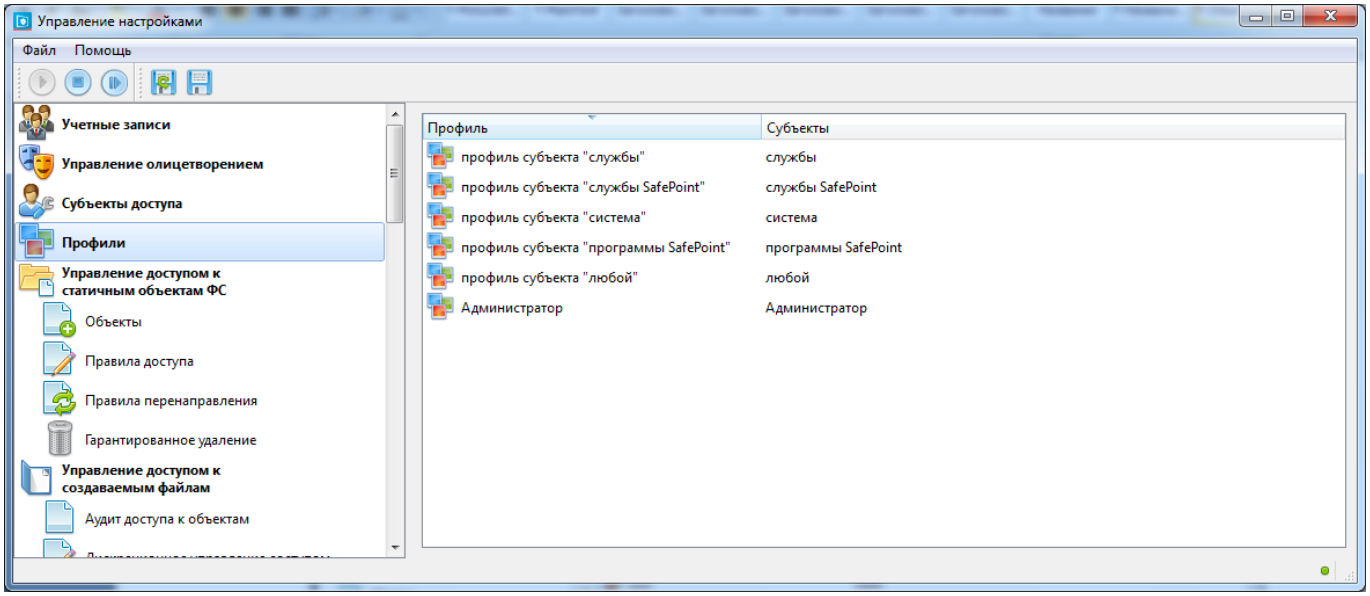


Рис.6.3.1. Интерфейс настройки профилей

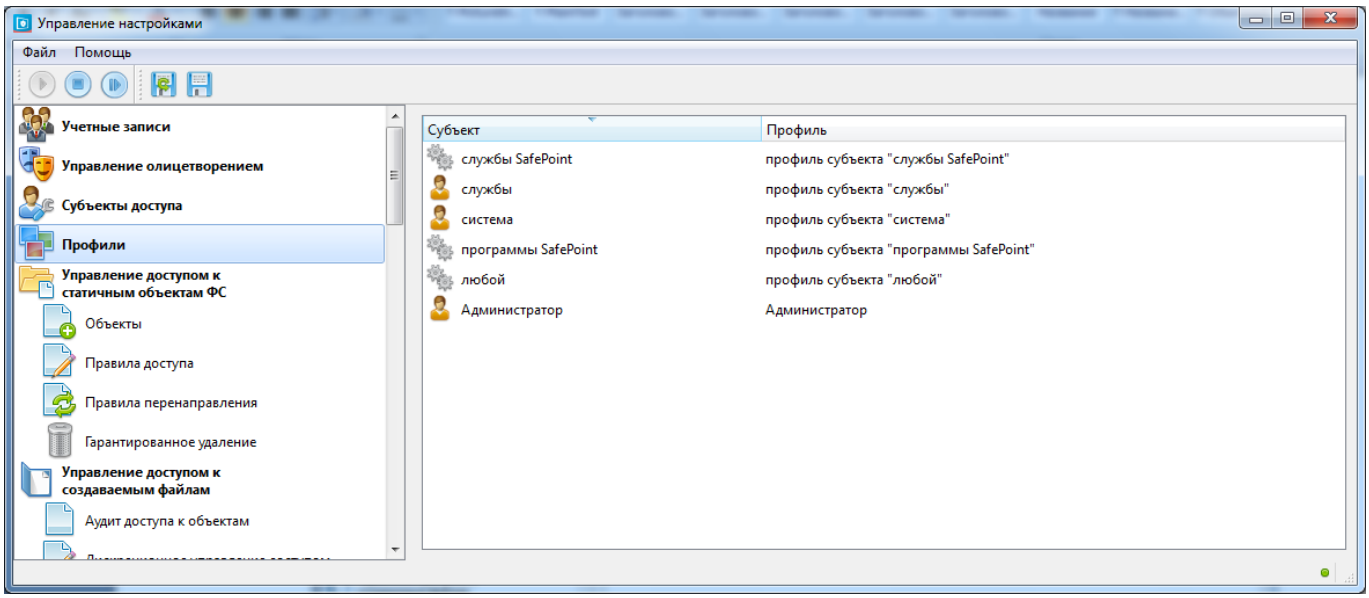


Рис.6.3.2. Интерфейс настройки профилей

По умолчанию в СЗИ «ViPNet SafePoint» созданы профили: профиль субъекта «любой», включающий субъект доступа «любой», профиль субъекта «система», включающий субъект доступа «система», профиль субъекта «службы», включающий субъект доступа «службы», профиль субъекта «службы СЗИ ViPNet SafePoint», включающий субъект доступа «службы СЗИ ViPNet SafePoint» и профиль субъекта «программы СЗИ ViPNet SafePoint», включающий субъект доступа «программы СЗИ ViPNet SafePoint».

Для переключения режима отображения вида списка следует:

1. Нажать правой кнопкой мыши по пустой области интерфейса «Профили».
2. В контекстном меню выбрать строку «Переключить режим отображения».

Создание профиля необходимо, для дальнейшего применения к нему правил и включения в него субъектов доступа. Для создания профиля необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт меню «Профили».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Профили» и в контекстном меню (рис.6.3.4) выбрать «Добавить профиль».

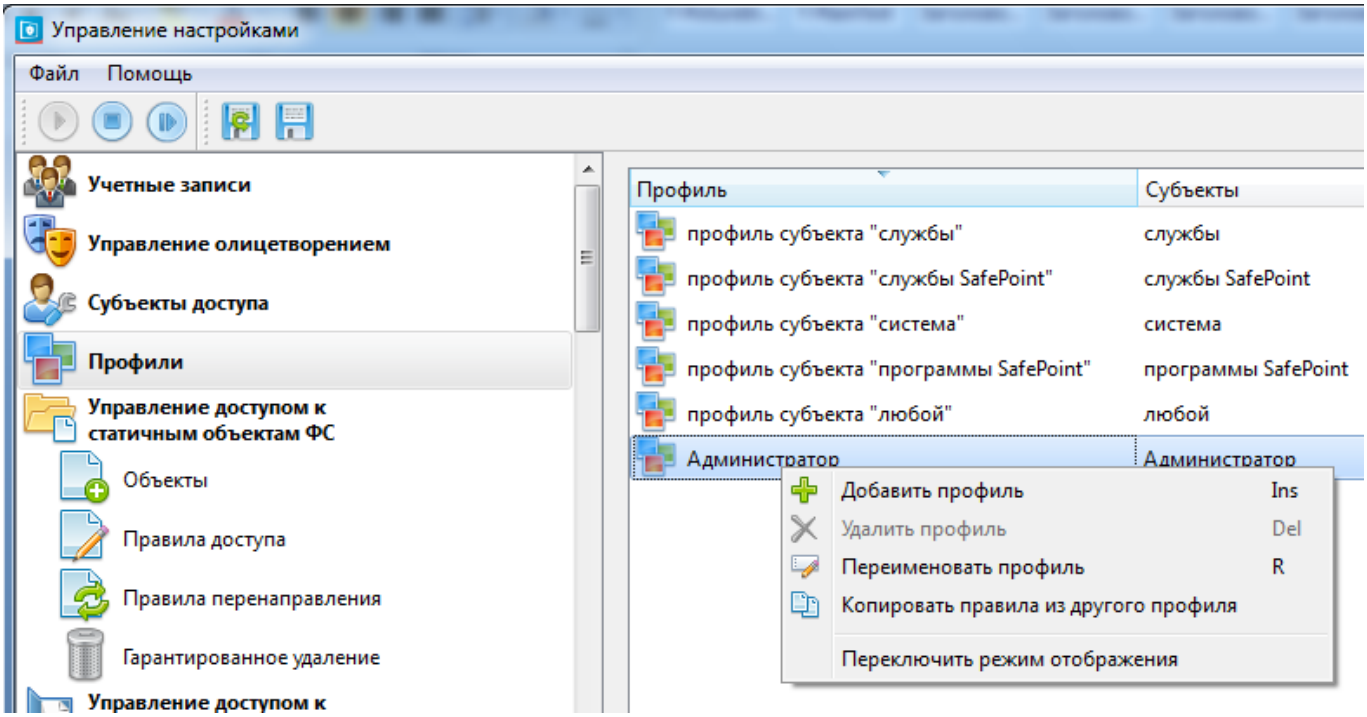


Рис.6.3.4. Контекстное меню окна «Профили»

3. В появившемся окне «Создание нового профиля» (рис.6.3.5) ввести нужное имя профиля и нажать кнопку «ОК».

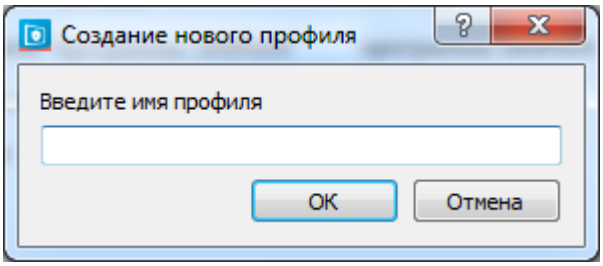


Рис.6.3.5. Окно создания нового профиля

4. Во всплывающем окне «Создан новый профиль» с вопросом «Хотите скопировать правила из существующего профиля в новый?» (рис.6.3.6) выбрать необходимый вариант. При нажатии «Да» появится окно «Выберите профиль источник» (рис.6.3.7), в котором необходимо выбрать профиль источник и нажать кнопку «ОК», в этом случае в новый профиль будут скопированы настройки из профиля источника, при нажатии «Нет» создастся новый профиль без настроек.

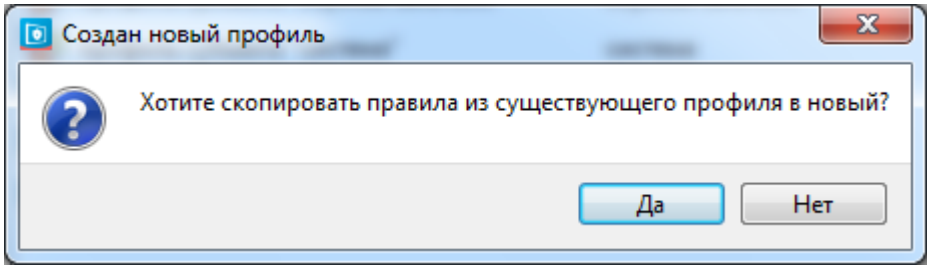


Рис.6.3.6. Окно «Создан новый профиль»

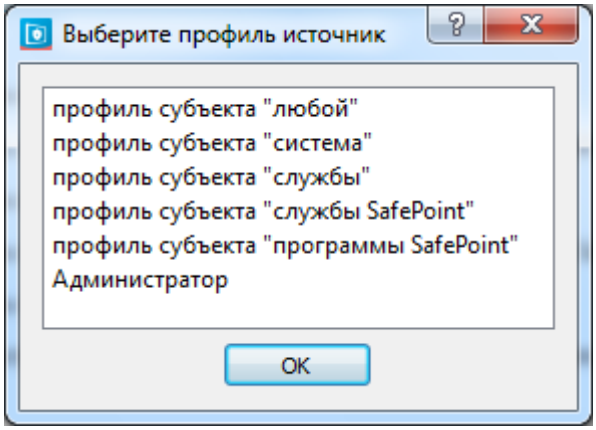


Рис.6.3.7. Окно выбора профиля источника

Использование при создании нового профиля источника позволяет упростить процесс администрирования системы. Например, если уже существует профиль с заданными основными правилами разграничения доступа и требуется создать новый профиль с похожими правилами, использование данной возможности СЗИ «ViPNet SafePoint» существенно сократит трудозатраты.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6.3.2. Переименование и изменение профиля

Переименование профиля возможно в режиме, отображающем имя профиля и субъекты, принадлежащие к данному профилю (рис.6.3.1). Для переименования профиля необходимо:

1. Выбрать профиль.
2. Нажать правой кнопкой мыши по выбранному профилю (рис.6.3.4).
3. В контекстном меню выбрать «Переименовать профиль» (рис.6.3.4).
4. В появившемся окне внести необходимые изменения, нажать «ОК» (окно аналогично окну «Создание нового профиля» рис.6.3.5).

Изменение профиля подразумевает изменение настроек, заданных для профиля. Это упрощает процесс администрирования, т.к. не потребуется настраивать каждый механизм заново, а потребуется лишь внести некоторые изменения. Для того чтобы добавить в профиль настройки из уже существующего профиля в режиме, отображающем имя профиля и субъекты, принадлежащие к данному профилю (рис.6.3.1) необходимо:

1. Выбрать профиль.
2. Нажать правой кнопкой мыши по выбранному профилю (рис.6.3.4).
3. В контекстном меню выбрать «Копировать правила из другого профиля».
4. В появившемся окне «Выберите профиль источник» необходимо выбрать профиль источника настроек и нажать «ОК».

Добавление в созданный профиль настроек из профиля источника позволяет упростить процесс администрирования системы. Например, если уже существует профиль с заданными правилами разграничения доступа и требуется применить похожие правила доступа к другому профилю использование данной возможности СЗИ «ViPNet SafePoint» существенно сокращает трудозатраты.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

6.3.3. Удаление профиля

Для удаления профиля необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт меню «Профили».
2. Выбрать профиль;
3. Нажать правой кнопкой мыши по выбранному профилю.
4. В контекстном меню выбрать «Удалить профиль» (рис.6.3.4).

5. В появившемся окне «Подтверждение удаления» нажать «Да».

Удаление профиля в СЗИ «ViPNet SafePoint» возможно только в случае, если в него не включен ни один субъект доступа.

Просмотр заведенных в СЗИ «ViPNet SafePoint» профилей осуществляется в окне интерфейса «Профили». Существует два варианта отображения связи профилей и субъектов доступа. В первом случае отображаются: имя профиля и субъекты, принадлежащие к данному профилю (рис.6.3.8). Во втором случае отображаются субъект доступа и профили, в которые он входит (рис.6.3.9). Этот режим предназначен только для удобства просмотра всех субъектов и профилей, в которые они включены.

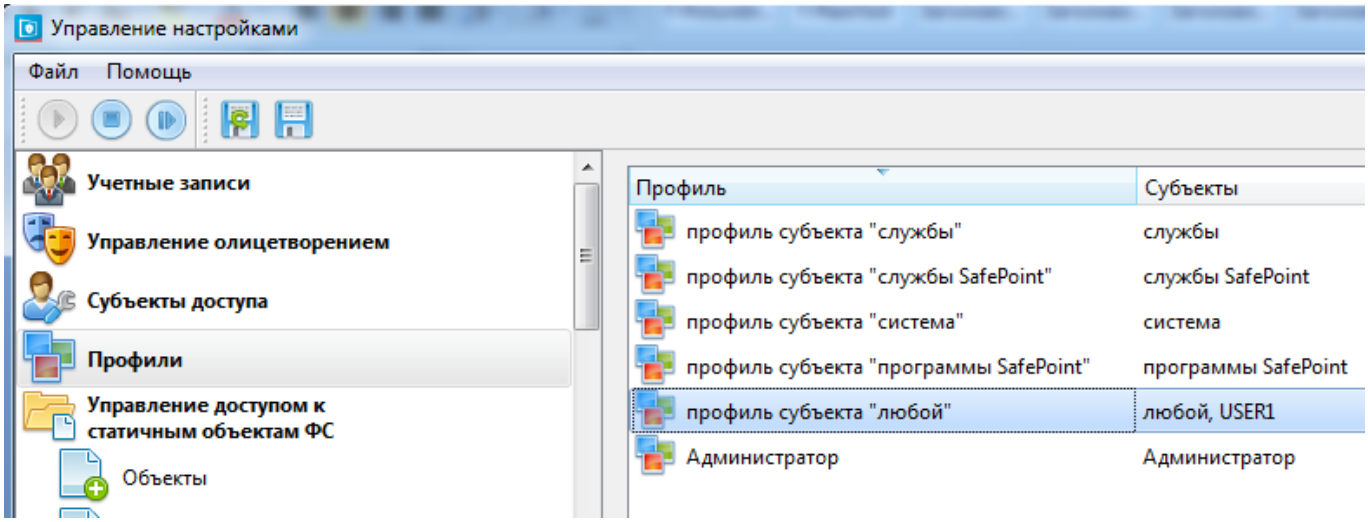


Рис.6.3.8. Просмотр созданных профилей и субъектов, входящих в эти профили

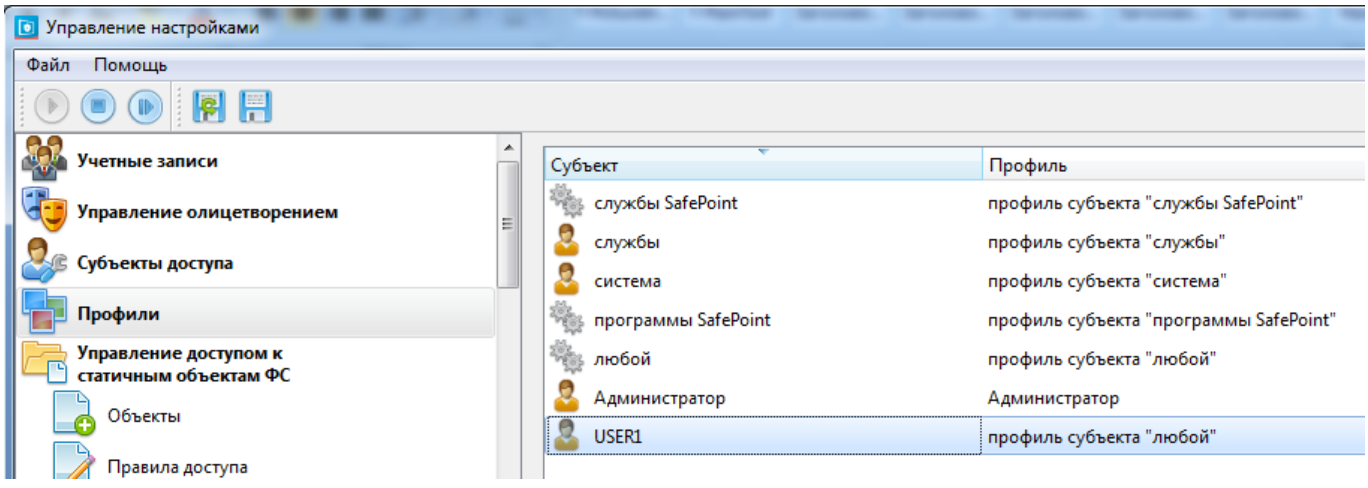


Рис.6.3.9. Просмотр субъектов и профилей, в которые включены субъекты

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку .

7. МЕХАНИЗМЫ КОНТРОЛЯ (РАЗГРАНИЧЕНИЯ) ПРАВ ДОСТУПА

7.1. МЕХАНИЗМ КОНТРОЛЯ ДОСТУПА К ОБЪЕКТАМ ФАЙЛОВОЙ СИСТЕМЫ

7.1.1. Статичные и создаваемые файловые объекты. Модель защиты СЗИ «ViPNet SafePoint»

Модель защиты СЗИ «ViPNet SafePoint», в части реализации контроля (разграничения прав) доступа к файловым объектам, предполагает разделение файловых объектов на статичные и создаваемые в процессе работы системы, с реализацией различных принципов контроля доступа к статичным и к создаваемым файловым объектам. Создаваемые файлы используются в вычислительной системе для хранения обрабатываемой информации, эти файлы отсутствуют на момент задания разграничительной политики доступа – создаются уже в процессе эксплуатации информационной системы, статичные – это, в первую очередь, системные файловые объекты, присутствующие в системе на момент задания правил доступа администратором.

Подобная классификация файловых объектов позволяет выявить все противоречия, возникающие при реализации контроля доступа к создаваемым файлам, средствами контроля доступа к статичным файловым объектам. При реализации подобной разграничительной политики доступа, ее сущностями выступают: субъект доступа, объект доступа, правила доступа.

Поскольку на момент задания разграничительной политики доступа создаваемых в процессе работы пользователей файлов еще не существует в системе, администратором при реализации разграничительной политики доступа заранее создаются хранилища – папки (своего рода «контейнеры») для последующего принудительного сохранения в них в процессе работы пользователями файлов. Т.е. администратором создаются папки (контейнеры), к которым и разграничивается доступ. Объект доступа «файл» в общем случае при этом исчезает из разграничительной политики доступа как таковой. Созданные файлы наследуют разграничения, установленные для папок. Задача реализации разграничительной политики доступа, состоящая в разграничении прав доступа субъектов к обрабатываемой в вычислительной системе информации, решается не напрямую, а опосредованно, чрез объекты доступа – папки.

Подобный метод контроля доступа в модели защиты СЗИ «ViPNet SafePoint» должен, в первую очередь, применяться для реализации контроля доступа к статичным (системным) файловым объектам. Естественно, что в данном случае имеет смысл применять дискреционный метод контроля доступа, предполагающий реализацию разграничительной политики на основе матрицы доступа (никак не метод, основанный на использовании меток безопасности, как правило, предполагающий категорирование информации по уровням конфиденциальности, что не имеет смысла в отношении системных файловых объектов). Применительно к реализации разграничительной политики доступа к создаваемым файлам, в модели защиты СЗИ «ViPNet

SafePoint» реализован принцип контроля доступа, основанный на исключении сущности «объект» доступа из разграничительной политики, как таковой. Все разграничения доступа задаются исключительно между субъектами, что принципиально упрощает реализацию разграничительной политики доступа к создаваемым файлам (или к обрабатываемой в системе информации), обеспечивая при этом реализацию корректной разграничительной политики доступа в общем случае.

Реализованные в СЗИ «ViPNet SafePoint» принципы контроля доступа к создаваемым файлам состоят в следующем:

1. Сущность «объект» исключается из схемы контроля доступа, при реализации разграничительной политики (при задании правил доступа) используются две сущности: идентификатор (учетная информация) субъекта, создавшего объект, и идентификатор субъекта, запрашивающего доступ к созданному объекту.

2. Правила доступа устанавливаются между сущностями: «субъект доступа (учетная информация), запрашивающий доступ к объекту» и «субъект доступа (учетная информация), создавший этот объект».

3. При создании субъектом доступа нового файла, создаваемый файл автоматически размечается СЗИ «ViPNet SafePoint» – файлом наследуется (записывается СЗИ «ViPNet SafePoint» в атрибуты создаваемого файла) учетная информация субъекта доступа (используется альтернативный поток), создавшего этот файл. Тоже происходит и при модификации неразмеченного ранее файла.

4. При запросе доступа к любому файлу, диспетчер доступа СЗИ «ViPNet SafePoint» анализирует наличие, а при наличии, содержимое унаследованной файлом учетной информации создавшего его субъекта доступа (разметки файла). При наличии, анализирует заданные правила доступа к создаваемым файлам, в результате чего предоставляет запрошенный субъектом доступ, либо отказывает в нем.

В отношении контроля доступа к создаваемым файлам, как к файлам, предназначенным для хранения обрабатываемой в информационной системе информации – может категорироваться по уровням конфиденциальности, уже имеет смысл реализация (реализованы в СЗИ «ViPNet SafePoint»), как дискреционного (на основе матрицы доступа) принципа контроля, так и принципа контроля доступа на основе меток безопасности.

Учетная информация субъекта при дискреционном контроле доступа, задается тремя сущностями: первичный идентификатор пользователя; эффективный идентификатор пользователя; процесс. Именно эта информация записывается в атрибуты файла при его создании.

Для реализации разграничительной политики доступа не требуется назначать правила доступа субъектов к объектам – все правила задаются исключительно для субъектов – задается то, какие права доступа имеет один субъект к файловым объектам, созданным другим субъектом.

В качестве учетной информации субъекта при контроле доступа на основе меток безопасности выступает назначаемая ему (в качестве субъекта доступа в данном случае выступает пользователь – учетная запись) метка безопасности. Метки безопасности требуется назначать только пользователям (учетным записям), никакого назначения меток безопасности объектам доступа не требуется.

Механизм контроля доступа на основе меток безопасности может применяться одновременно с механизмом дискреционного контроля доступа к создаваемым файлам, при этом доступ будет возможен, если он разрешен обоими этими механизмами защиты. При этом сначала анализируются правила контроля доступа на основе меток безопасности, затем дискреционного контроля доступа к создаваемым файлам. Контроль доступа к статичным файловым объектам может применяться одновременно с контролем доступа к создаваемым файлам – доступ будет возможен, если он разрешен обоими этими механизмами защиты. При этом сначала анализируется разграничительная политика доступа, заданная в отношении статичных файловых объектов.

Отдельно в модели защиты СЗИ «ViPNet SafePoint» выделены файловые накопители. К ним реализуется контроль доступа по аналогии с контролем доступа к статичным файловым объектам, с той лишь разницей, что объект доступа задается идентификатором устройства (включая его серийный номер). Задание файлового устройства в разграничительной политике доступа буквой диска, к которой оно примонтировано, не допустимо.

Если контроль доступа к создаваемым файловым объектам, как дискреционный, так и основанный на применении меток безопасности, позволяет реализовать корректную разграничительную политику доступа в общем случае (размечаются непосредственно файлы), то корректность реализации контроля доступа к статичным файловым объектам обеспечивается дополнительным механизмом защиты из состава СЗИ «ViPNet SafePoint» – механизмом перенаправления запросов. Некорректность разграничительной политики при контроле доступа к статичным файловым объектам без использования данного механизма, обусловливается наличием в системе неразделяемых ОС и приложениями каталогов (коллективно используемых ресурсов), например, папок хранения временных файлов. Механизм перенаправления запросов позволяет принудительно (средствами СЗИ «ViPNet SafePoint») разделить между субъектами доступа любой не разделяемый ОС и приложениями файловый объект.

В драйвер механизма контроля доступа к объектам файловой системы добавлена возможность отключать запрос параметров устройства для букв дисков «A:» и «B:» (дисководы гибких дисков, флоппи-дисковод). Для использования данной возможности необходимо создать параметр реестра «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\fileCtrl3\Parameters\ Determine Floppy Devices» типа DWORD со значением 0.

7.1.2. Механизм контроля доступа к статичным файловым объектам. Назначение и особенности реализации. Интерфейс

Модель защиты СЗИ «ViPNet SafePoint», в части реализации контроля (разграничения прав) доступа к статичным файловым объектам предполагает реализацию дискреционного контроля доступа (на основе матрицы доступа) субъектов к файловым объектам с принудительным управлением потоками информации (непривилегированный пользователь исключен из схемы администрирования – правила доступа могут задаваться/модифицироваться исключительно администратором).

Особенностью реализации является то, что правила доступа задаются для субъектов (а не назначаются в качестве атрибутов доступа объектам). Это позволяет при минимальных усилиях строить сложнейшие разграничительные политики доступа к статичным объектам, в том числе для процессов (приложений), за счет использования масок при задании объектов доступа, а также реализовать принципиально новые возможности защиты информации от несанкционированного доступа в информационной системе.

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к ресурсам.

Разграничительная политика реализуется для профилей.

Например, можно разрешить запуск файлов только из каталогов Windows и Program Files, запретив их модификацию интерактивным пользователям (возможно, отдельным критичным процессам), чем обеспечивается **замкнутость программной среды** – исполняемые файлы можно запустить только из этих каталогов, а сами эти каталоги, в которых также хранятся системные файлы настройки ОС и приложений, не могут быть несанкционированно модифицированы. Можно полностью изолировать доступ к системным файлам критичных приложений (обеспечить

им только необходимый для корректной работы доступ к системным файловым объектам). Поскольку в качестве субъектов доступа могут выступать системные процессы, данным механизмом защиты можно разграничивать права доступа к файловым объектам для системных процессов и сетевых служб, в том числе, в части защиты от атак на уязвимости системных процессов, направленных на реализацию несанкционированного доступа к обрабатываемой в информационной системе информации.

Использование масок при задании файловых объектов предоставляет принципиально новые возможности защиты, в частности, позволяет реализовать контроль доступа к файлам по их расширениям. Пример задания маской исполняемого файла «*.exe». Подобным образом в разграничительной политике могут задаваться файлы, разрешенные к исполнению, при этом они запрещаются к переименованию, модификации, кроме того, «по умолчанию» (установлено в разграничительной политике – соответствующие правила не включены в интерфейс механизма защиты) СЗИ «ViPNet SafePoint» не позволит создать новый файл с заданным расширением и переименовать любой файл в файл с заданным расширением. В результате реализации данной разграничительной политики доступа, на компьютер не смогут быть занесены вредоносные программы. Подобную же разграничительную политику доступа (на основании расширений файлов) можно реализовать и в отношении, например, скриптовых файлов, с целью предотвращения их создания интернет-браузерами.

Возможности практического использования данного механизма защиты крайне широки, для определения же актуальных правил доступа можно воспользоваться средствами инструментального аудита событий из состава СЗИ «ViPNet SafePoint».

Основное назначение данного механизма контроля доступа – защита системных ресурсов (исполняемых файлов и файлов настройки ОС и приложений), в том числе, защита от компрометации системы.

Механизм контроля доступа к статичным файловым объектам позволяет задавать правила, регламентирующие возможность создания файлов, т.е. производить контроль по созданию файлов:

- задать каталоги, в которых возможно создание файлов тем или иным субъектом доступа;
- задать какие файлы (с какими расширениями) могут быть созданы тем или иным субъектом доступа;
- задать какие файлы (с какими расширениями) из каких каталогов могут быть доступны тому или иному субъекту доступа.

Окно интерфейса механизма контроля доступа к статичным объектам представлено на рис.7.1.2.1. В данном, основном окне интерфейса, включаются или отключаются механизмы перенаправления и гарантированного управления.

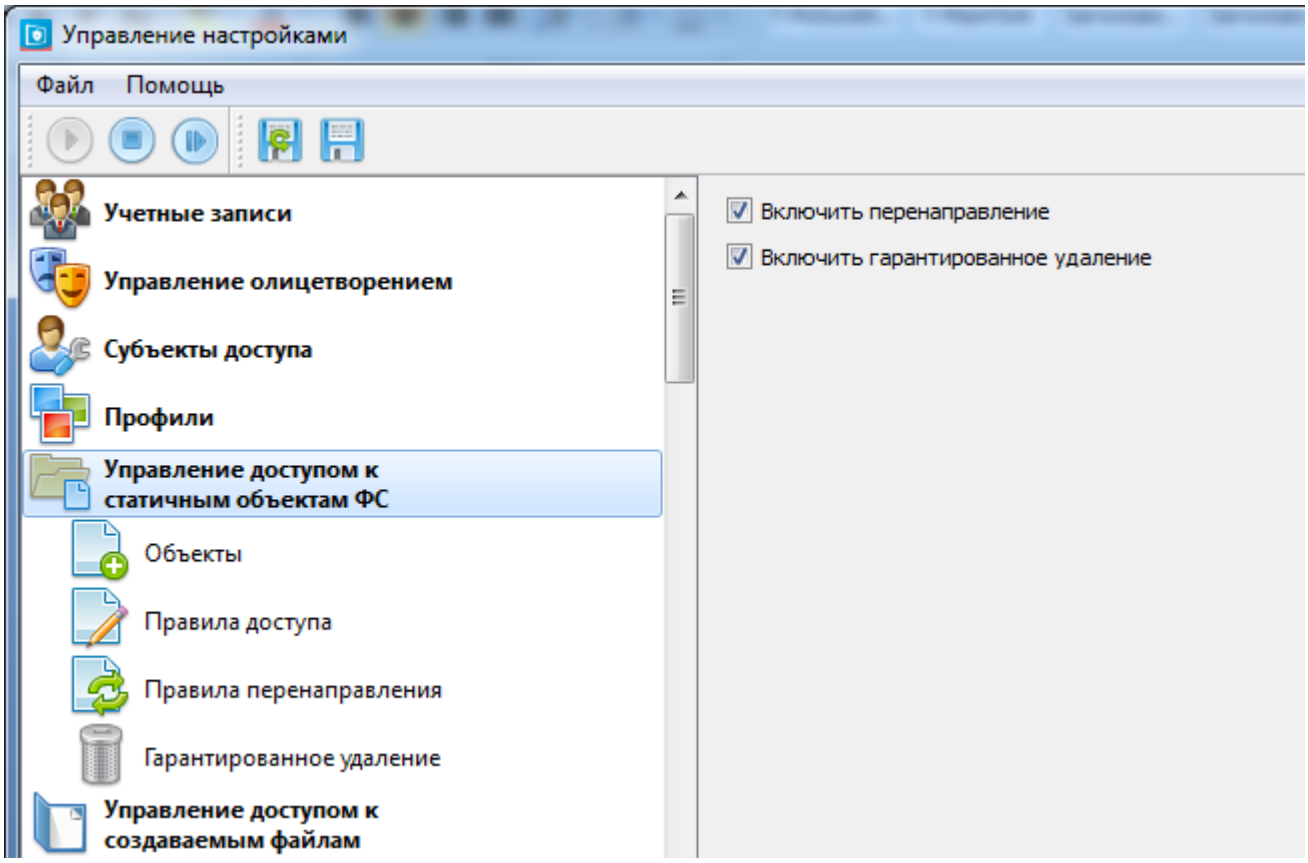


Рис.7.1.2.1. Окно интерфейса управления доступом к статичным объектам ФС

Настраивать правила доступа к статичным файловым объектам следует последовательно, сначала определить для каких профилей будут заданы правила (см. раздел 6. Профили и субъекты доступа), для каких объектов (задать объекты в СЗИ «ViPNet SafePoint»), далее уже собственно назначить правила доступа профилей к объектам.

7.1.2.1. Создание, редактирование и удаление объектов доступа

Выбор окна интерфейса создания объектов представлен на рис.7.1.2.1.1. Объекты задаются их полнопутевыми именами. Также при задании объектов могут быть использованы маски и переменные среды окружения.

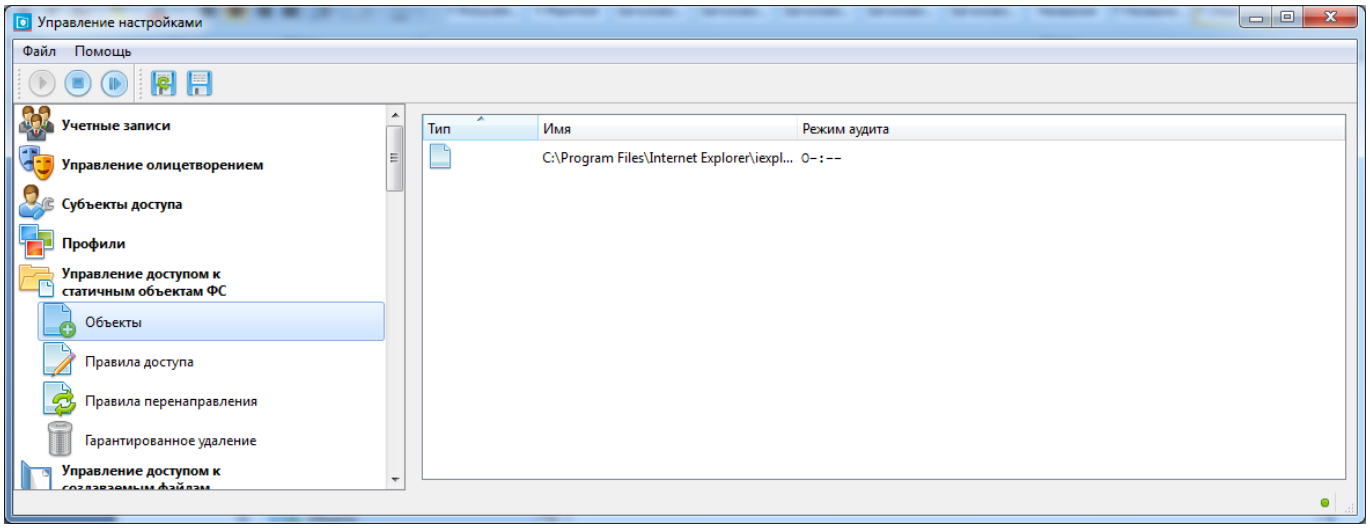


Рис.7.1.2.1.1. Окно интерфейса объекты доступа

При заведении объектов следует учитывать:

1) Объект необходимо задавать в соответствии с его типом (файл, маска файла, каталог, маска каталога, маска).

В СЗИ «ViPNet SafePoint» реализуется контроль доступа субъектов к объектам. При реализации разграничительной политики доступа к файловому объекту, для выбора требуемого для анализа правила доступа из задаваемой таблицы (матрицы) правил диспетчер доступа выбирает объект по наиболее точному его соответствию полнопутевому имени объекта, к которому запрашивается доступ (имя которого получается диспетчером из запроса доступа).

С учетом возможности использования масок, одновременно несколько объектов, заведенных в СЗИ «ViPNet SafePoint» в том числе с использованием масок и переменных среды окружения, могут соответствовать реальному объекту, определяемому его полнопутевым именем, к которому запрашивается доступ. Для выбора правила доступа введен следующий приоритет обработки объектов, заданных в СЗИ «ViPNet SafePoint», исходя из их типа: файл, маска файла, каталог, маска каталога, маска. Заданные в СЗИ «ViPNet SafePoint» объекты сравниваются с реальными объектами в заданном порядке обработки (файл, маска файла, каталог, маска каталога, маска) и выбирается правило доступа для первого из подошедших объектов.

В СЗИ «ViPNet SafePoint» тип объекта (файл, маска файла, каталог, маска каталога, маска) задается автоматически, но при реализации конкретной разграничительной политики, пользователю может понадобиться установить тип объекта вручную, для изменения порядка его обработки (сравнения объекта, заведенного в СЗИ «ViPNet SafePoint», с реальным объектом, к которому запрашивается доступ).

В СЗИ «ViPNet SafePoint» если задан тип объекта файл или каталог, т.е. выбраны конкретные объекты, специальные символы не учитываются как маски, а считаются именем объекта.

2) При задании разграничений на каталог, разграничения накладываются непосредственно на сам каталог и на все его содержимое.
3) При задании объектов типа «полнопутевое имя каталога*» разграничения действуют только на содержимое каталога, на сам каталог разграничения не действуют.

При указании «полнопутевое имя каталога*», во избежание отмены разграничений на содержимое в каталоге в связи с доступными изменениями самого каталога (переименование, удаление), необходимо задавать отдельное правило на сам каталог. При указании после каталога «\», разграничения на каталог и его содержимое не действуют.

Создание объектов

Для создания объекта доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Объекты».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Объекты» в контекстном меню (рис.7.1.2.1.2) выбрать «Добавить объект ФС».

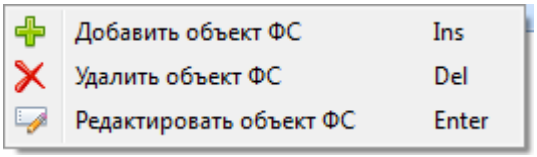


Рис.7.1.2.1.2. Контекстное меню окна управления доступом к статичным объектам ФС

3. В появившемся окне «Создание нового объекта файловой системы» (рис.7.1.2.1.3) произвести следующие настройки:

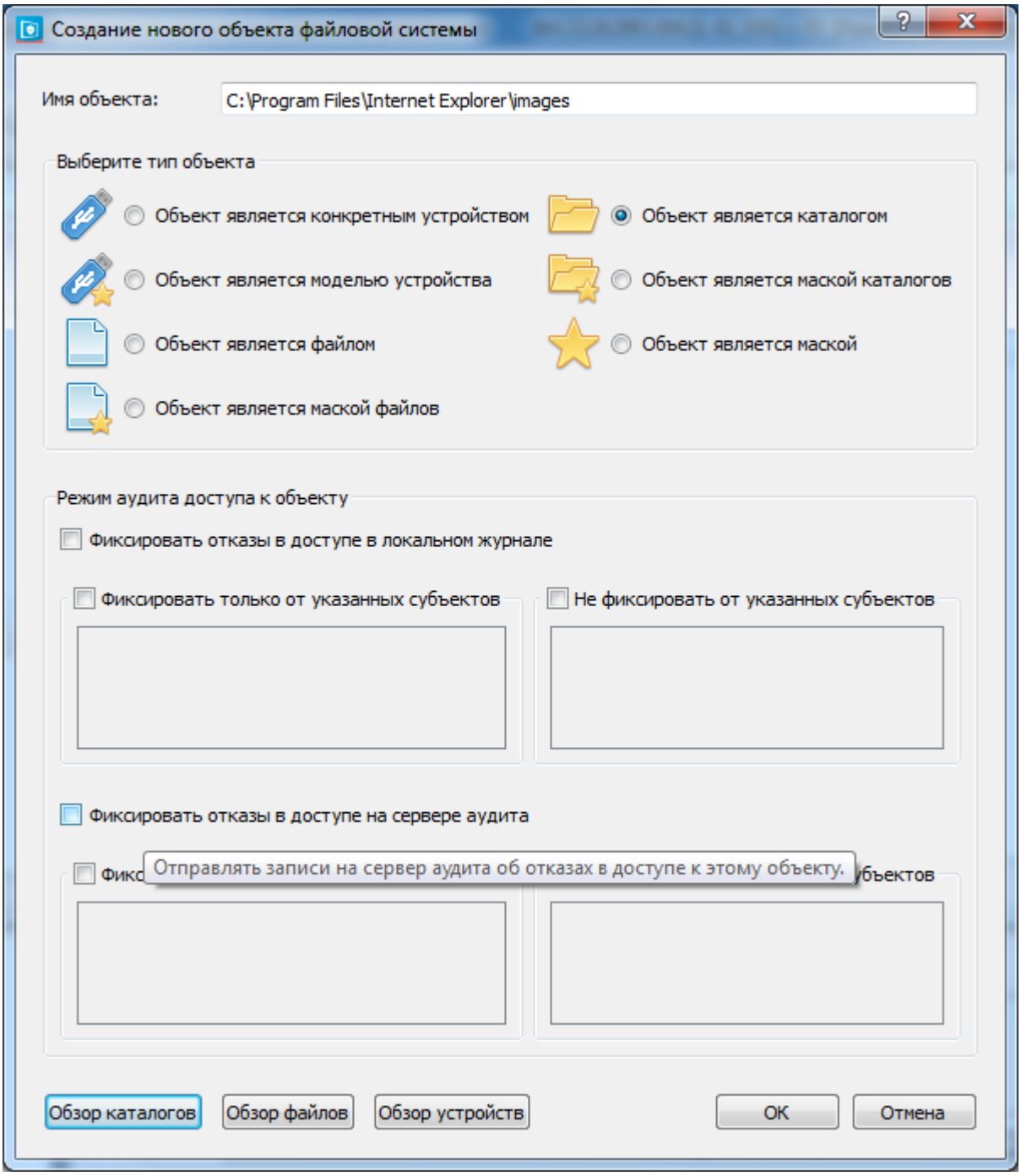


Рис.7.1.2.1.3. Окно создания нового объекта файловой системы»

1) Задать имя объекта, используя «Обзор каталогов», «Обзор файлов» в зависимости от типа объекта или задать имя объекта вручную, путем указания маски или полнопутевого имени.

Выбрав объект в «Обзоре каталогов» или «Обзоре файлов», в строке «имя объекта» вручную можно дополнить или изменить имя объекта, включив в него маску.

2) Выбрать тип объекта или оставить тип, выбранный автоматически.
3) Настроить режим аудита (раздел 15.2.2 Аудит доступа к объектам).

4. Нажать кнопку «ОК».

В качестве объектов могут быть использованы разделенные в сети файловые объекты. Такие объекты возможно задавать, используя символьное имя удаленной машины (например, *\\ТАТЬЯНА-ПК\doc new, \\TEST7-PK\test\текстовый документ.txt*) или IP адрес (например, \\192.168.0.52*, \\192.168.0.66\test.txt).

Обращение к разделенным в сети файловым объектам по IP адресу машины (например, *\\192.168.0.43\test.txt, \\192.168.0.66\)* запрещено по умолчанию. При попытке такого обращения в «Журнале управления доступом к файловой системе» в Просмотрщике журналов аудита будут появляться записи запрета доступа с уточнением «Доступ к сетевому ресурсу по IP запрещен по умолчанию».

Для разрешения данных действий при установке СЗИ «ViPNet SafePoint» добавлено правило, разрешающее доступ к объекту *, который покрывает любые IP адреса. Рекомендуется далее в процессе эксплуатации выявить конкретные ресурсы, к которым необходим доступ, и, заведя соответствующие объекты доступа, разрешить к ним доступ, а доступ к остальным ресурсам по IP адресам запретить.

Кроме того, имеется возможность задавать статические объекты ФС по именам пространства NT.

Любой том на дисковых носителях, к которому Windows может обратиться, имеет имя «\Device\HarddiskVolume?», где «?» – монотонно возрастающее число, начинающееся с 1. Данные имена фиксированы до перезагрузки, но могут меняться, например, в случае если на диске, где расположен том, были созданы еще тома. Привычные имена вида «C:\...» существуют по причине совместимости с DOS и фактически являются доступом по символической ссылке. Т.е. в пространстве имен NT существует ссылка, например, вида «C: -> \Device\HarddiskVolume2». И обращение «C:\Windows\notepad.exe» превращается в «Device\HarddiskVolume2\Windows\ notepad.exe». Ссылки с буквой на том может и не быть. Примером такого тома размером около 100 Мб, создаваемого ОС Windows автоматически при установке, является том, в котором располагается загрузчик ОС. Этому загрузчику BIOS передает управление для загрузки ОС.

СЗИ «ViPNet SafePoint» позволяет контролировать и разграничивать права доступа к «скрытым» подобным образом объектам, в том числе, к загрузчику ОС.

Обзор объектов файловой системы по NT именам возможен локально и удаленно при добавлении объекта файловой системы.

Для создания такого объекта доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Объекты».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Объекты» в контекстном меню (рис. 7.1.2.1.4) выбрать «Добавить объект ФС».

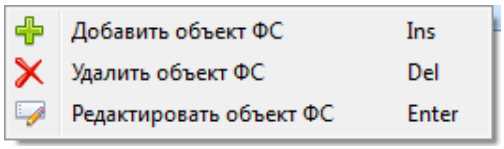


Рис.7.1.2.1.4. Контекстное меню окна управления доступом к статичным объектам ФС

3. В появившемся окне «Создание нового объекта файловой системы» (рис.7.1.2.1.5) произвести следующие настройки:

1) Задать имя объекта, используя «Обзор каталогов», «Обзор файлов» в зависимости от типа объекта, правой клавишей мыши вызвав контекстное меню на соответствующей кнопке: «Обзор папок» или «Обзор файлов» для открытия диалога обзора по именам NT (рис.7.1.2.1.6).

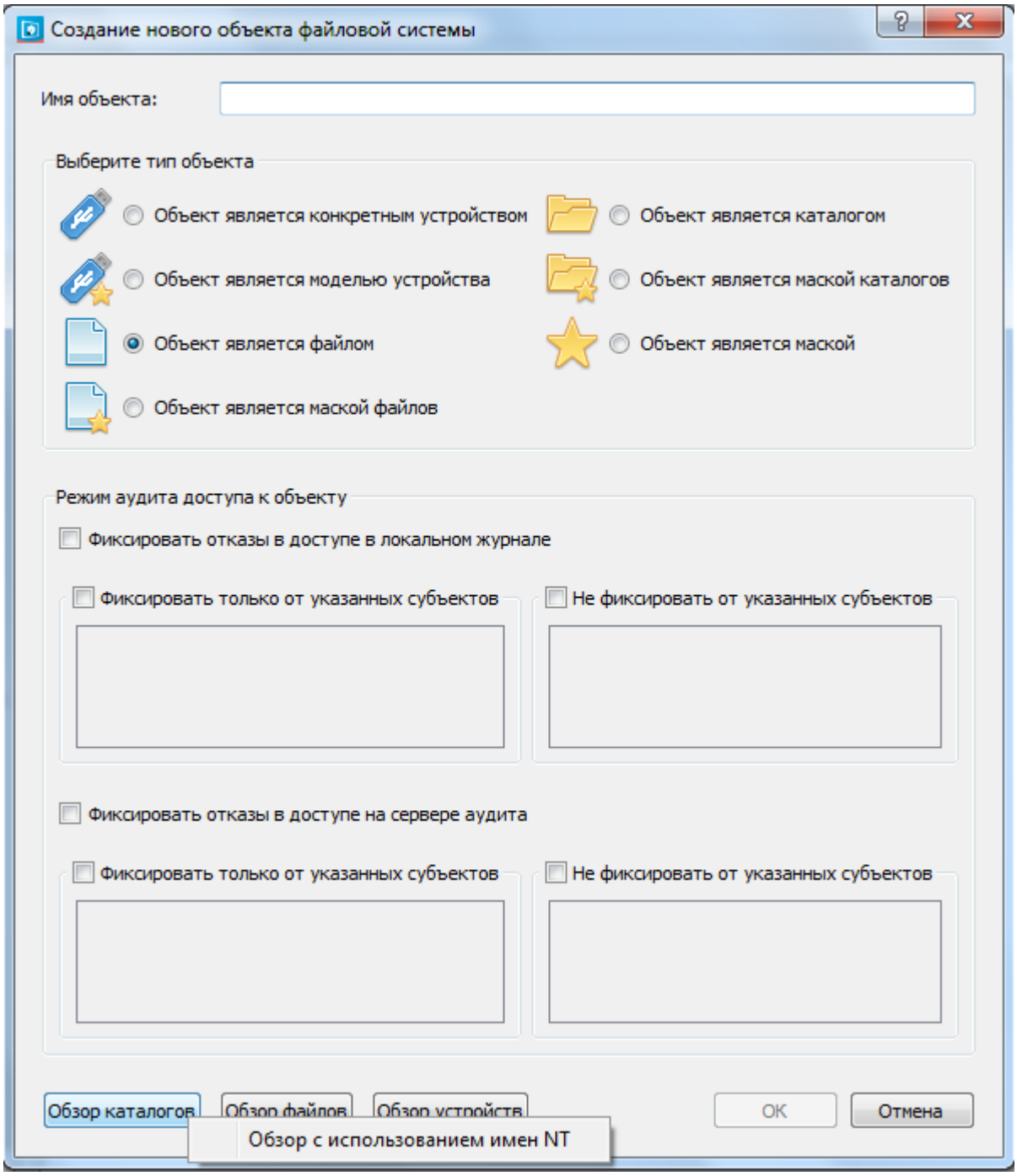


Рис.7.1.2.1.5. Окно создания нового объекта файловой системы»

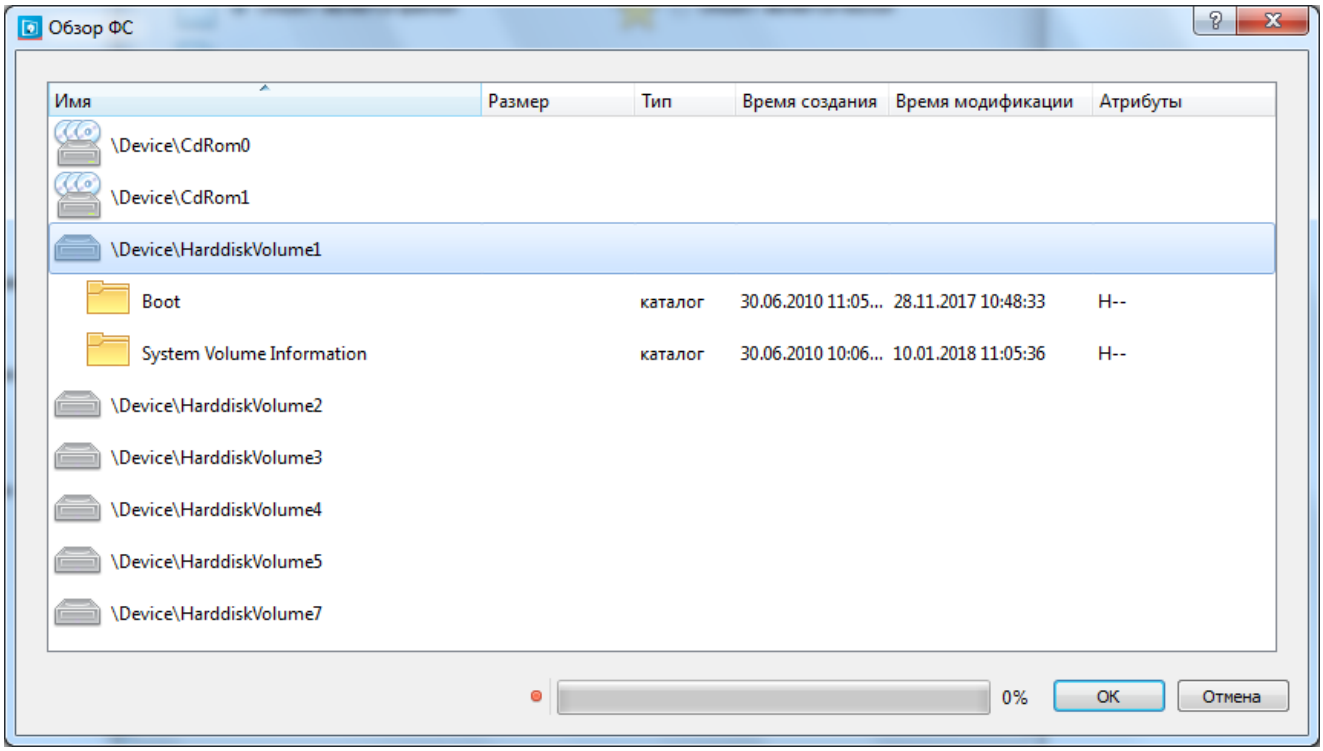


Рис.7.1.2.1.6. Окно создания нового объекта файловой системы»

Выбрав объект в «Обзоре каталогов» или «Обзоре файлов», в строке «имя объекта» вручную можно дополнить или изменить имя объекта, включив в него маску.

2) Выбрать тип объекта или оставить тип, выбранный автоматически.

3) Настроить режим аудита (раздел 15.2.2 Аудит доступа к объектам).

4. Нажать кнопку «ОК».

NT-имена не поддерживаются механизмом перенаправления.

Контроль NT-имен можно отключить, отредактировав параметр реестра HKLM\System\CurrentControlSet\fileCtrl3\Parameters\Name Options (по умолчанию все биты этого числа установлены (0xffffffff) – необходимо убрать 5й бит.

Для **просмотра** созданных объектов необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Объекты» (рис.7.1.2.1.1). Объекты отображаются в интерфейсе (рис.7.1.2.1.7), в котором указаны: тип объекта (пиктограмма), его имя, и режим аудита. Выделив объект левой кнопкой мыши, и, при наведении курсора на тип, имя или режим аудита объекта, появится всплывающее окно с пояснением.

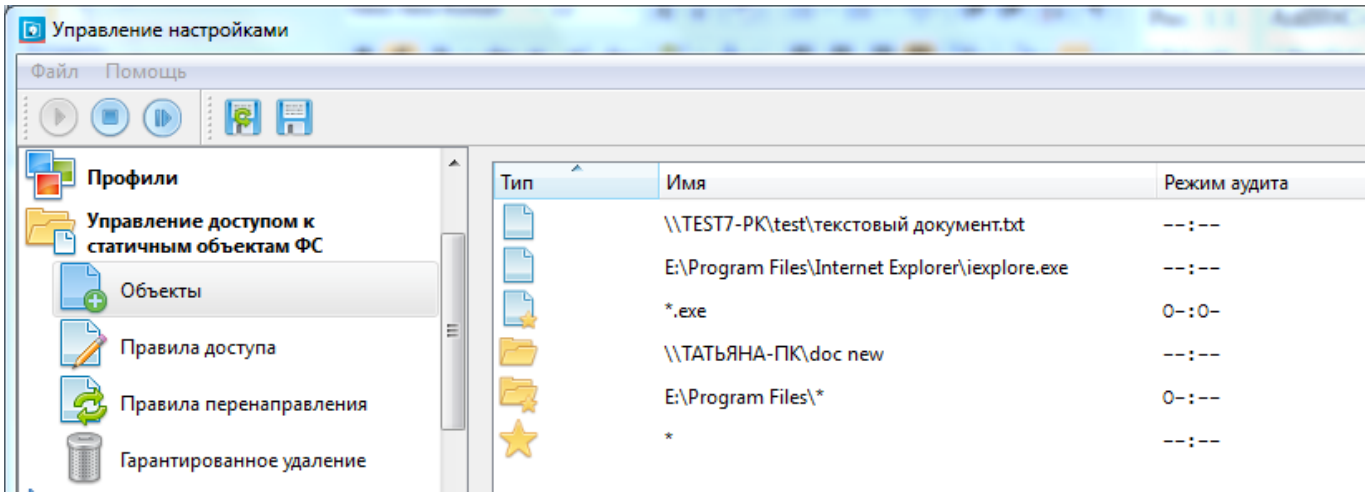


Рис.7.1.2.1.7. Интерфейс просмотра созданных объектов

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Для **редактирования** уже созданного объекта следует нажать правой кнопкой мыши по объекту в интерфейсе «Объекты» (рис.7.1.2.1.7) и в контекстном меню выбрать «Редактировать объект ФС», после чего внести необходимые изменения.

Для **удаления** объекта следует нажать правой кнопкой мыши по объекту в интерфейсе «Объекты» (рис.7.1.2.1.7) и в контекстном меню выбрать «Удалить объект ФС».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.2.2. Возможности использования масок и переменных среды окружения

При задании объекта доступа возможно использование масок, которые являются строками, содержащими в себе вместе с частями имени ресурса также специальные символы и конструкции. Эти спецсимволы управляют процессом сравнения двух строк: маски и имени ресурса. При создании или редактировании объекта доступа использование масок позволяет упростить настройки разграничения доступа и задавать объекты, как из определенного каталога, так и объекты определенного типа.

Примеры масок:

- Использование маски «*» подразумевает все объекты системы;
- Использование масок типа «C:\Program Files*» подразумевает все файлы из заданного каталога;
- Использование маски типа «*.txt» подразумевает все файлы с указанным расширением (тип файла);

- Маска «*iexplore.*» подразумевает все файлы с названием «iexplore» с любым расширением, находящиеся в любом каталоге.

При задании каталогов существует возможность использования переменных среды для указания, например, системного каталога. Пример задания процессов из системного каталога Program Files:

- %PROGRAMFILES%* подразумевает все файлы из каталога Program Files, содержащего установленные программы загруженной операционной системы.

Существует возможность использования других спецсимволов и конструкций:

? – обозначает любой символ (символ в имени ресурса должен присутствовать на месте спецсимвола в маске);

+ – обозначает один и более символов (символ в имени ресурса должен присутствовать на месте спецсимвола в маске);

[набор символов] – обозначает любой символ, входящий в набор (символ в имени ресурса должен присутствовать на месте конструкции в маске);

[!набор символов] или [^набор символов] – обозначает любой символ, не входящий в набор (символ в имени ресурса должен присутствовать на месте конструкции в маске).

Набор символов может задаваться как последовательностью (например, [abcdefg]), так и диапазоном (например, [a-g]), а также комбинацией последовательности и диапазона (например, [bde-hxyz]).

Например, маска «*text?.doc*» покрывает все имена ресурсов с именами *«text1.doc», «text2.doc», «texta.doc»* и т.п.

7.1.2.3. Назначение правил доступа

При реализации разграничительной политики доступа возможно использование запретительной политики доступа или разрешительной политики доступа. Запретительная политика подразумевает, что, по умолчанию все действия субъектов над объектами разрешены, но для «определенных» субъектов доступ к «определенным» объектам запрещен. При реализации разрешительной разграничительной политики, по умолчанию, доступ всех субъектов ко всем объектам запрещен, но для «определенных» субъектов назначены правила, разрешающие доступ к «определенным» объектам. «Определенные» это субъекты и объекты, задаваемые администратором, исходя из задач реализуемой политики разграничения доступа.

Разрешительная или запретительная разграничительная политика может быть реализована как для системы в целом, так и для отдельных субъектов.

В СЗИ «ViPNet SafePoint» при назначении правил доступа режимы доступа сгруппированы для упрощения процесса администрирования в:

1. Чтение.
2. Запись.
3. Исполнение.
4. Удаление.
5. Переименование.

Под «**Чтением**» подразумевается любой доступ к объекту, не изменяющий объект, т.е. это чтение содержимого файла, атрибутов файла, владельца, разрешений, для каталогов это еще и чтение их содержимого (обзор).

«**Запись**» – это доступ изменяющий объект. К записи относятся такие действия (флаги, установленные при открытии объекта файловой системы (далее ФС) и обозначающие запрашиваемые виды доступа), как: удаление, переименование, запись разрешений (в операционных системах Microsoft Windows (далее ОС Windows) «смена разрешений»), запись владельца (в ОС Windows «смена владельца»), запись данных (создание файлов), добавление данных (создание папок), запись атрибутов (только чтение, архивный, скрытый, системный), запись расширенных атрибутов (в ОС Windows «запись дополнительных атрибутов»), удаление дочернего объекта (для каталогов), создание файла при открытии, перезапись файла при открытии, замена файла при открытии.

«**Исполнение**» – это открытие файла с флагом FILE_EXECUTE.

Проверка доступа типа «Чтение/Запись» происходит при открытии объекта, а не при доступе к нему. Поэтому даже если программа собиралась только читать файл, но открывает его, указав хотя бы один флаг, относящийся к записи, – проверка доступа будет проведена как при попытке записи.

«**Удаление**» – это доступ к файлу на удаление.

«**Переименование**» – это доступ к файлу на переименование.

Проверка доступа типа «Переименование» и «Удаление» происходит во время собственно самой операции. Переименование и удаление являются операциями записи. Если не указаны разграничения для конкретного вида доступа (удаление, переименование) то проверяются более общие правила доступа. Например, программой открывается файл для удаления. Далее следует проверка назначенных правил по порядку – от более конкретных к общим:

1. «Удаление» – разрешено, тогда доступ будет разрешен, невзирая на возможные запреты записи или чтения объекта.

2. «Удаление» – нет разграничений, «Запись» – разрешена, тогда доступ будет разрешен, невзирая на возможный запрет чтения объекта.

3. «Удаление» – нет разграничений, «Запись» – нет разграничений, «Чтение» - запрещено, в этом случае доступ будет запрещен.

Таким образом, приоритетны всегда более точные правила.

В СЗИ «ViPNet SafePoint» правила доступа назначаются для профилей относительно объектов. Для назначения правила доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Правила доступа».
2. В выпадающей строке «Профиль» выбрать профиль, для которого будут назначены правила доступа.
3. Нажать правой кнопкой мыши по пустой области интерфейса «Правила доступа для выбранного профиля» и в контекстном меню (рис.7.1.2.3.1) выбрать «Добавить правило».

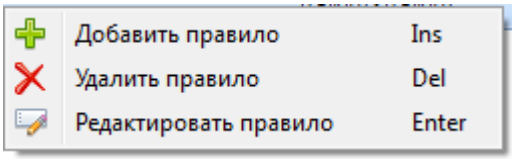


Рис.7.1.2.3.1. Контекстное меню окна «Правила доступа»

4. Произвести следующие настройки в появившемся окне «Добавление нового правила» (рис.7.1.2.3.2):

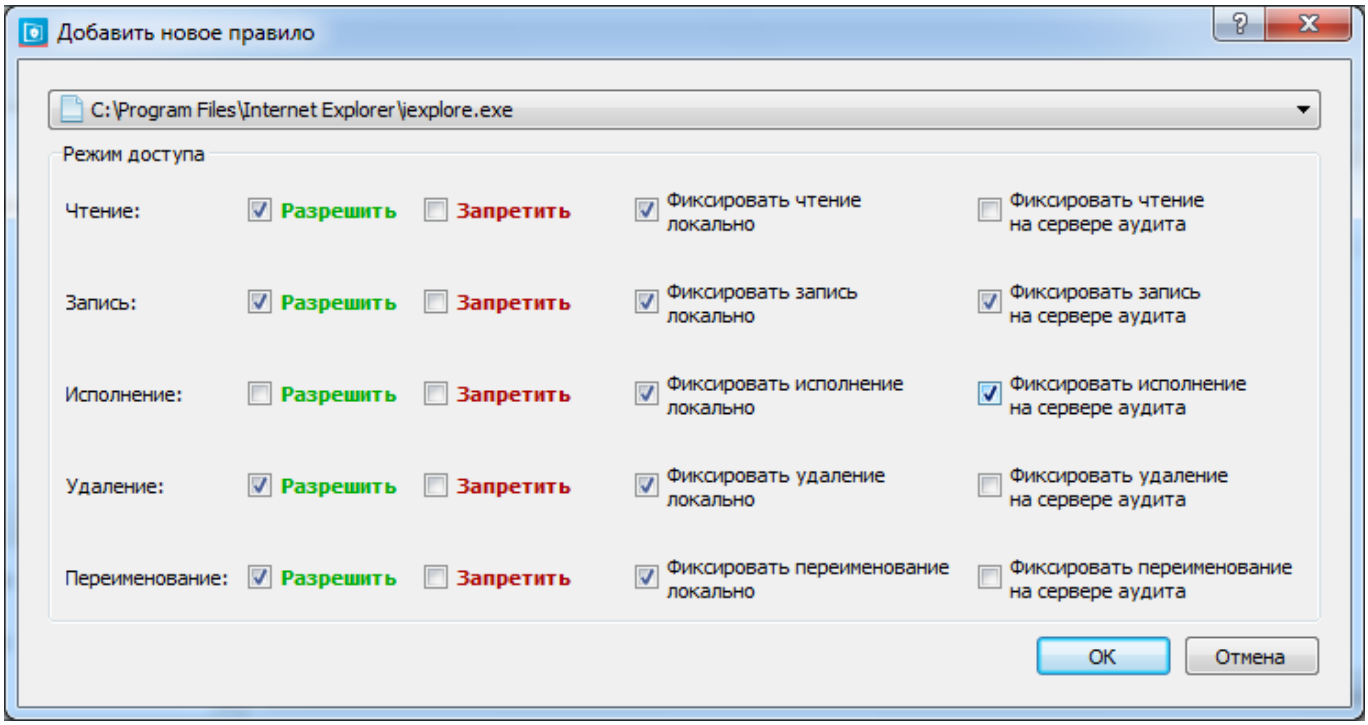


Рис.7.1.2.3.2. Окно «Добавить новое правило»

1) Выбрать из выпадающего списка объект доступа.
2) Установить необходимые флаги «Разрешить» или «Запретить» для режимов доступа: чтение, запись, исполнение, удаление и переименование.
3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Правила доступа» (рис.7.1.2.3.3). Назначенные правила представлены в интерфейсе, в котором указаны тип объекта (пиктограмма), имя объекта, режим доступа и режим аудита. Выделив правило левой кнопкой мыши, и, при наведении курсора на тип, имя объекта, режим доступа или режим аудита, появится всплывающее окно с пояснением.

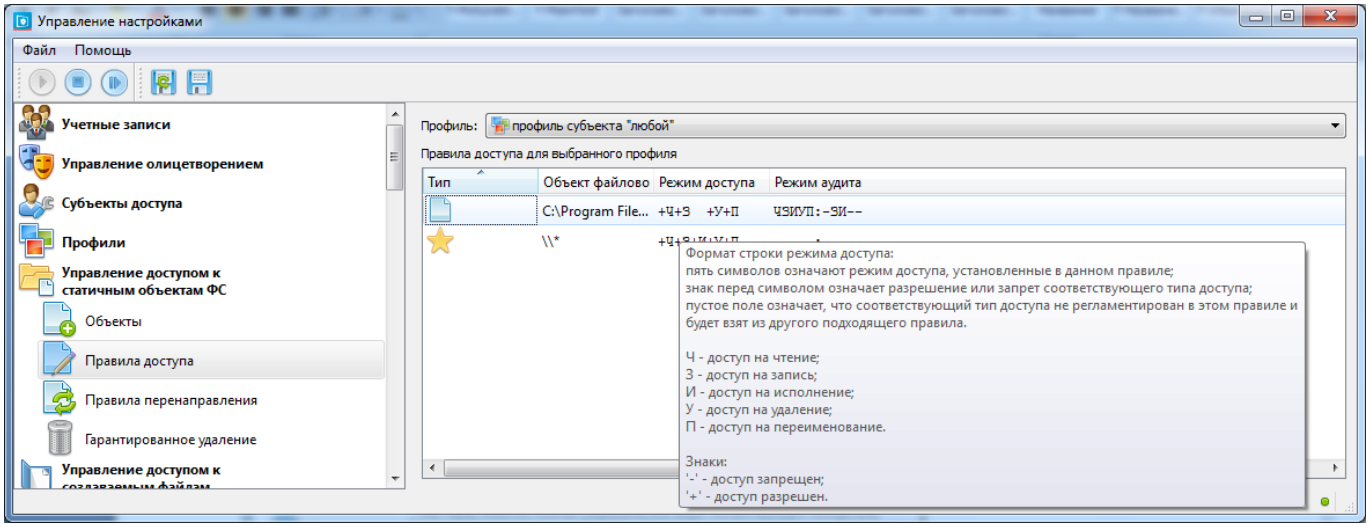


Рис.7.1.2.3.3. Интерфейс просмотра назначенных правил доступа

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Для **редактирования** уже созданных правил следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» (рис.7.1.2.3.3) и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» (рис.7.1.2.3.3) и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.2.4. Механизм контроля доступа к файловым накопителям. Назначение и особенности реализации. Интерфейс

Данный механизм защиты, предназначенный для реализации разграничительной политики доступа в отношении внешних накопителей и файловых объектов, располагаемых на внешних накопителях, реализуется по полной аналогии с механизмом контроля доступа к статичным файловым объектам, с той лишь разницей, что устройство задается в разграничительной политике доступа не как файловый объект (не буквой диска, к которой монтируется устройства), а идентификатором модели устройств, либо конкретного устройства, включая его серийный номер (если он есть у данного устройства).

Разграничительная политика реализуется для профилей.

Не каждое устройство, которое может использоваться в качестве внешнего накопителя, рассматривается в качестве файлового накопителя ОС Microsoft Windows (т.е. в отношение которого данным механизмом защиты СЗИ «ViPNet SafePoint» может быть реализован контроль доступа). Существуют устройства (например, смартфоны), которые «видны» в системе, как файловые устройства, но при этом, в которых функции файлового накопителя реализуются не ОС, а собственным драйвером устройства. Такие устройства, которые не будут идентифицироваться в качестве файловых накопителей механизмом защиты СЗИ «ViPNet SafePoint» (не видны при обзоре из СЗИ «ViPNet SafePoint» файловых накопителей), лучше не использовать (т.к. в отношении них не может быть в полном объеме реализована разграничительная политика доступа), предусмотрев невозможность их монтирования к системе соответствующим механизмом защиты из состава СЗИ «ViPNet SafePoint».

Основное назначение данного механизма контроля доступа – обеспечение регламента предприятия по работе с внешними файловыми накопителями – позволяет использовать только конкретные файловые накопители (с учетом их серийных номеров), для хранения на них информации, создаваемой конкретными субъектами (при использовании контроля доступа на основе меток безопасности к создаваемым файлам, см. ниже – для хранения на внешних накопителях информации конкретных уровней конфиденциальности).

Выбор окна интерфейса создания объектов - файловых накопителей представлен на рис.7.1.2.4.1. Файловым накопителем будем считать устройство, которое идентифицируется операционной системой Microsoft Windows (далее ОС Windows) как устройство хранения информации, и монтирующееся к букве диска.

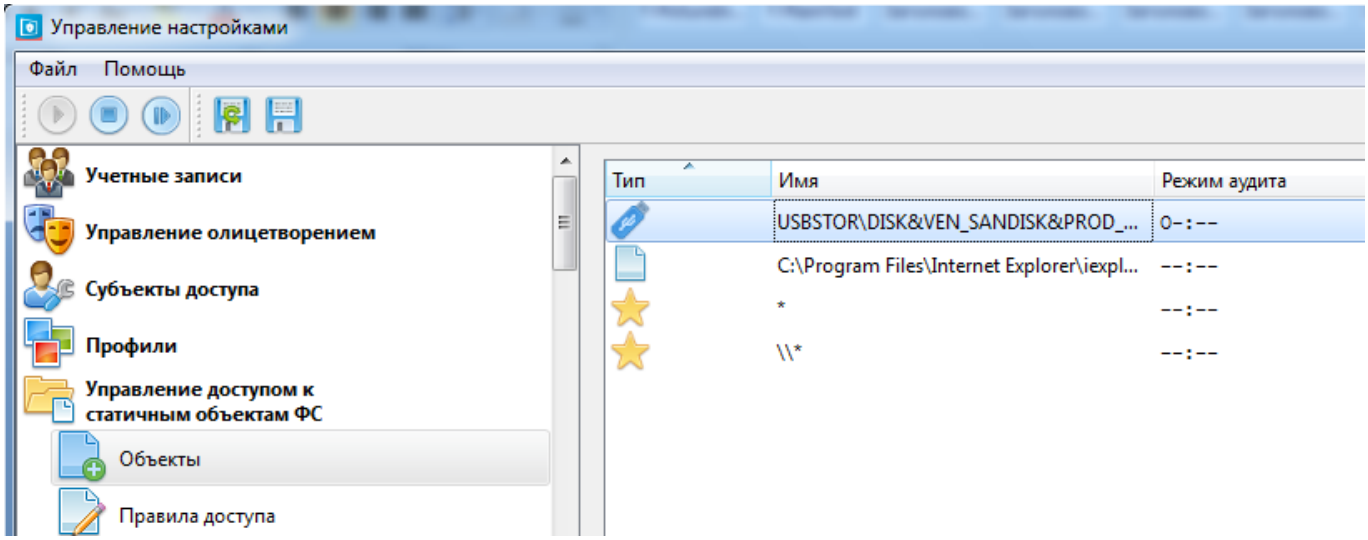


Рис.7.1.2.4.1. Окно интерфейса объекты доступа

Механизм настраивается для профилей, аналогично механизму контроля доступа к статичным объектам файловой системы. Прежде всего, необходимо задать соответствующий объект. Для этого необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Объекты».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Объекты» в контекстном меню (рис.7.1.2.4.1) выбрать «Добавить объект ФС».

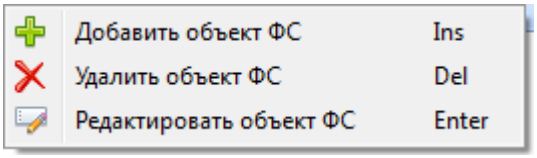


Рис.7.1.2.4.1. Контекстное меню окна управления доступом к статичным объектам ФС

3. В появившемся окне «Создание нового объекта файловой системы» (рис.7.1.2.4.2) произвести следующие настройки:

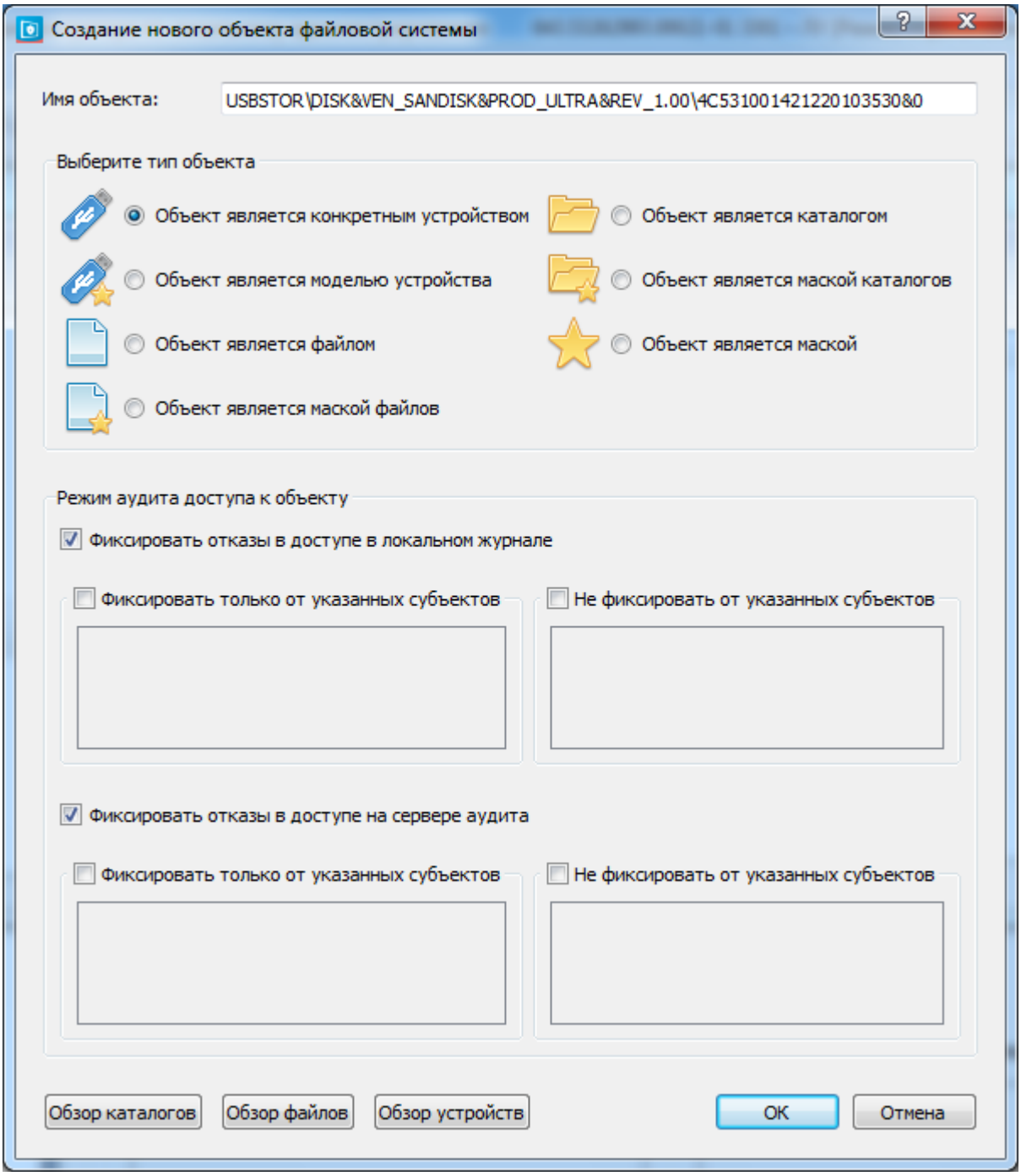


Рис.7.1.2.4.2. Окно создания нового файлового накопителя

1) Задать имя объекта, используя «Обзор устройств» или задать имя объекта вручную.

После нажатия кнопки «Обзор устройств», откроется окно «Выберите устройство», в котором зеленым подсвечиваются устройства, подключенные к системе в данный момент, а черным – устройства, которые когда-либо были подключены к системе.

В строке «Имя объекта», в результате использования обзора устройств, появляется идентификатор устройства. В этой строке можно дополнить имя файлового объекта на устройстве вручную или скопировав имя каталога или файла, расположенных на устройстве, из строки «Имя объекта», полученного путем использования обзора каталогов или файлов на этом устройстве.

2) Выбрать тип объекта либо «Объект является конкретным устройством», либо «Объект является моделью устройства» (*при выборе данного типа отсутствует возможность указания объектов, находящихся на накопителе*) или оставить тип, выбранный автоматически.
3) Настроить режим аудита (см. раздел 15.2.2 Аудит доступа к объектам).

4. Нажать кнопку «ОК».

Просмотр заведенных файловых накопителей осуществляется, как и просмотр заведенных объектов файловой системы (рис.7.1.2.4.3). В интерфейсе файловые накопители отличаются пиктограммой типа объекта.

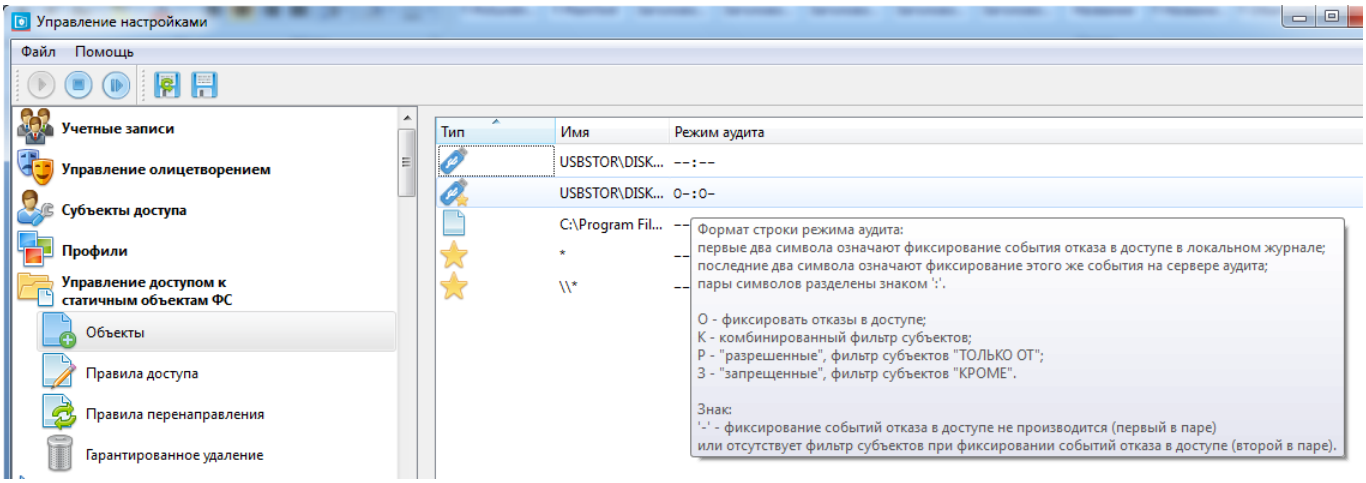


Рис.7.1.2.4.3. Интерфейс просмотра заданных файловых накопителей

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Существует возможность **редактировать** уже созданный объект. Для этого следует нажать правой кнопкой мыши по объекту в интерфейсе «Объекты» (рис.7.1.2.4.3) и в контекстном меню выбрать «Редактировать объект ФС», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка объект следует нажать правой кнопкой мыши по объекту в интерфейсе «Объекты» (рис.7.1.2.4.3) и в контекстном меню выбрать «Удалить объект ФС».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку .

Назначение правил доступа для файловых накопителей.

Правила доступа задаются для профилей относительно объектов. Правила доступа к файловым накопителям назначаются из интерфейса задания правил доступа для объектов файловой системы (далее ФС). Для назначения, редактирования или удаления правил доступа к файловым накопителям необходимо проделать аналогичные действия, как и при назначении, редактировании или удалении правил доступа к объектам ФС (см. раздел 7.1.2.3 Назначение правил доступа).

Просмотр назначенных правил доступа для файловых накопителей осуществляется из интерфейса просмотра правил доступа к статичным объектам ФС (рис.7.1.2.4.4).

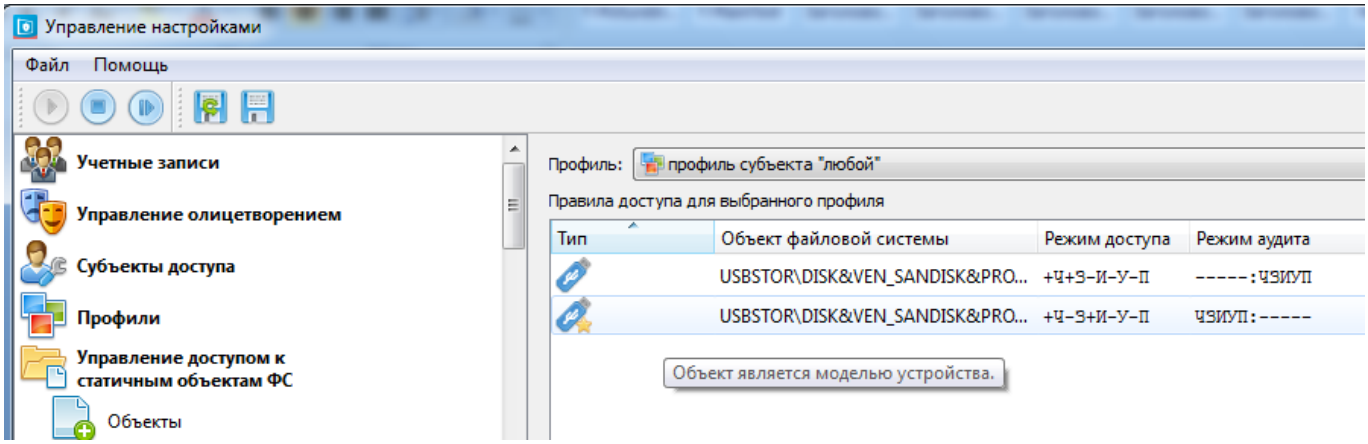


Рис.7.1.2.4.4. Интерфейс просмотра назначенных правил доступа

Существует возможность **редактировать** созданные правила. Для этого следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка правило доступа следует нажать правой кнопкой мыши по правилу и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку .

7.1.2.5. Механизм перенаправления запросов. Назначение и особенности реализации. Интерфейс

Реализация механизма переадресации запросов доступа к объектам файловой системы (папкам), не разделяемым системой и приложениями между субъектами доступа, (например, к каталогам Temp, не разделяемым между пользователями) предполагает принудительное

перенаправление СЗИ «ViPNet SafePoint» запросов доступа к подобным папкам коллективного использования. При этом для каждого субъекта доступа (например, пользователя) для неразделяемого между пользователями объекта администратором создается соответствующий собственный объект, например, для неразделяемого каталога «Общий ресурс», создается каталог «Общий ресурс 1» для первого пользователя, «Общий ресурс 2» для второго пользователя и т.д. При записи информации в неразделяемый каталог (соответственно, при чтении из этого каталога), диспетчер доступа СЗИ «ViPNet SafePoint» перенаправляет запрос доступа в соответствующий каталог пользователя, запросившего соответствующий доступ. Например, при сохранении информации в каталог «Общий ресурс» первым пользователем, данная информация будет перенаправлена диспетчером доступа и сохранена в каталоге «Общий ресурс 1».

Механизм перенаправления запросов к неразделяемым системой файловым объектам обрабатывает запрос перед механизмом контроля (разграничения прав) доступа к статичным файловым объектам, средствами которого уже могут разграничиваться права доступа к тем каталогам, в которые перенаправляется запрос доступа, например, доступ к каталогу «Общий ресурс 1» следует разрешить только первому пользователю, остальным – запретить. Данный механизм – это ключевой механизм в модели защиты СЗИ «ViPNet SafePoint» в части реализации контроля (разграничения прав) доступа к файловым объектам, позволяющий обеспечить отсутствие общих для субъектов ресурсов файловой системы, т.е. корректно реализовать разграничительную политику доступа к файловым объектам в общем случае. Без его применения в системе присутствуют неразделяемые между субъектами доступа файловые объекты, являющиеся «каналами» несанкционированного обмена информацией между субъектами, в том числе, между пользователями. Особенно это критично в том случае, когда реализуется обработка информации различных уровней конфиденциальности одним и тем же пользователем с различными правами доступа к ресурсам под различными учетными записями. Неразделяемый файловый объект при этом может быть использован для несанкционированного понижения уровня конфиденциальности обрабатываемой информации.

Разграничительная политика реализуется для профилей.

Выбор окна интерфейса назначения правил перенаправления представлен на рис.7.1.2.5.1.

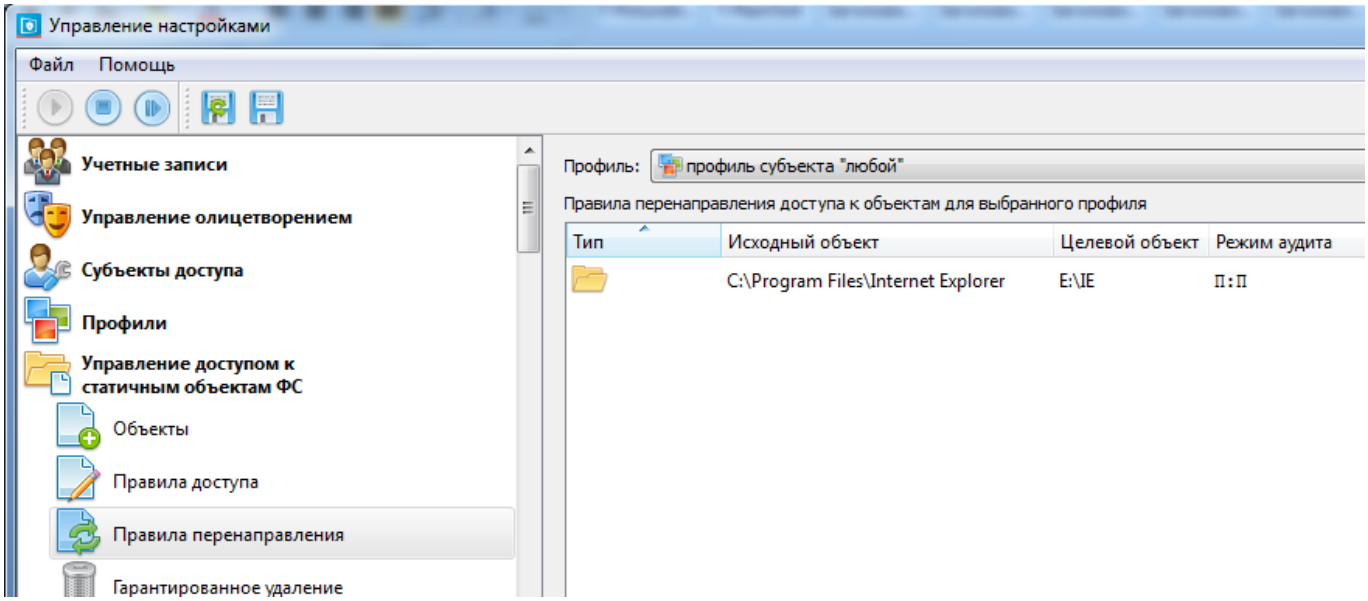


Рис.7.1.2.5.1. Интерфейс механизма перенаправления запросов

Для функционирования правил перенаправления запросов доступа необходимо, чтобы администратор для каждого субъекта создал в ОС объект, в который будет происходить перенаправление запроса доступа из исходного объекта. При необходимости, администратор должен скопировать содержимое исходного объекта в созданные им для перенаправления запросов объекты.

После создания объектов, в которые будут перенаправляться запросы доступа, необходимо создать эти объекты в разграничительной политике доступа (см. раздел 7.1.2.1 Создание, редактирование и удаление объектов доступа). Далее назначить правила перенаправления запросов. Назначить правила доступа к объектам, в которые происходит перенаправление запросов доступа.

Правила перенаправления запроса доступа срабатывают прежде, чем правила контроля доступа субъектов к объектам доступа.

Перенаправление запросов возможно только между конкретными объектами ФС, поэтому при задании исходного объекта и объекта, в который происходит перенаправлении, недопустимо использование масок.

Перенаправление запросов возможно только между объектами ФС одного типа (например, между файлами или между каталогами).

Для включения механизм перенаправления запросов необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС».
2. Установить флаг «Включить перенаправление» (рис.7.1.2.5.2).

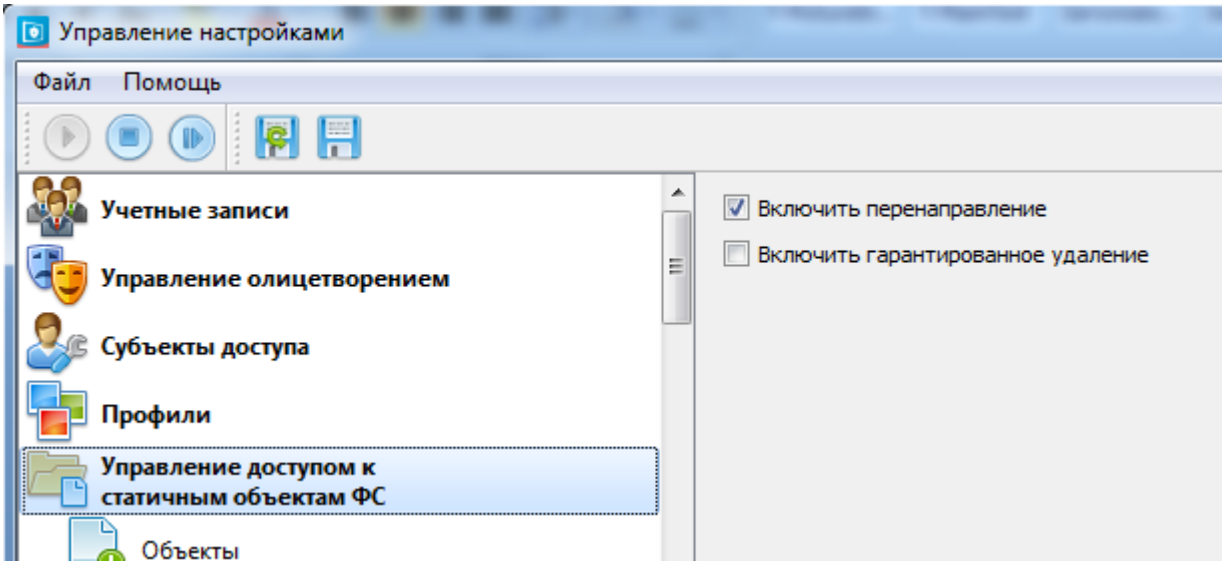


Рис.7.1.2.5.2. Интерфейс включения механизма перенаправления запросов

Для создания правила перенаправления запросов следует произвести следующие действия:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Правила перенаправления».
2. В выпадающем списке «Профиль» выбрать профиль, для которого будет назначено правило перенаправления.
3. Нажать правой кнопкой мыши по пустой области интерфейса «Правила перенаправления доступа к объектам для выбранного профиля» и в контекстном меню выбрать «Добавить правило» (рис.7.1.2.5.3).

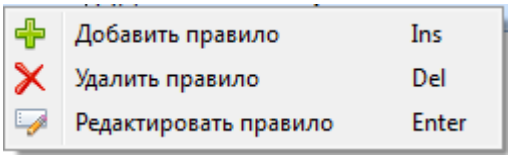


Рис.7.1.5.3. Контекстное меню окна «Правила перенаправления»

4. Произвести следующие настройки в появившемся окне «Добавление нового правила» (рис.7.1.2.5.4):

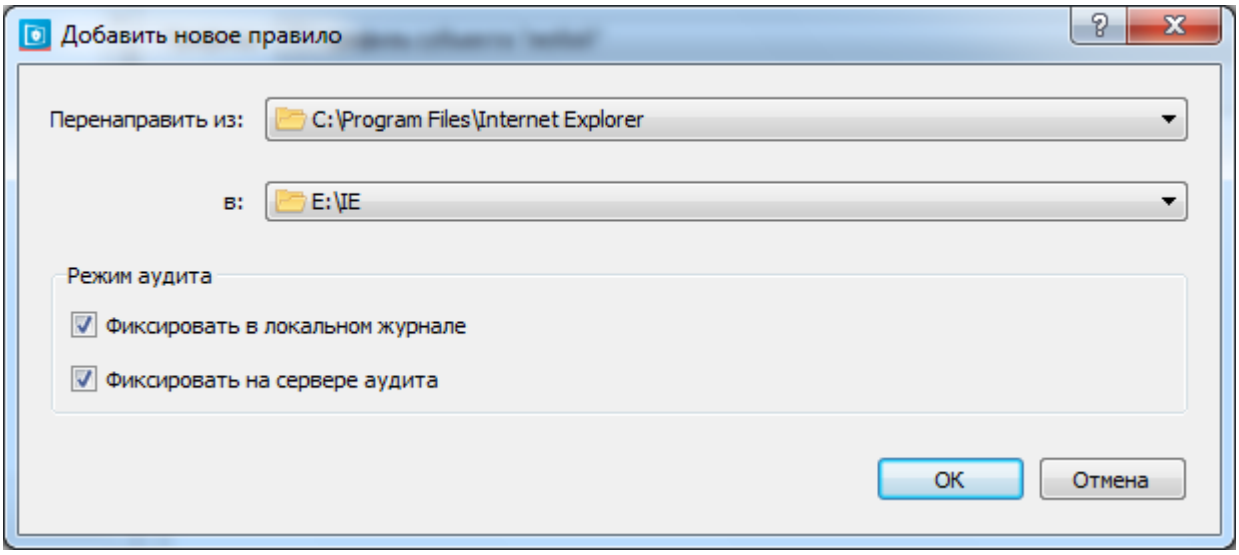


Рис.7.1.2.5.4. Окно добавления нового правила доступа

1) Выбрать из выпадающего списка «Перенаправить из» объект, из которого будет производиться перенаправление.
2) Выбрать из выпадающего списка строки «В» объект, в который будет производиться перенаправление.

Для корректной работы необходимо выбирать созданные объекты, учитывая типы объектов (однотипные), т.к. перенаправление возможно только между объектами одного типа (папка-папка или файл-файл).

3) Настроить режим аудита (см. раздел 15.2.2 Аудит доступа к объектам).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил перенаправления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Правила перенаправления». Назначенные правила представлены в интерфейсе, в котором указаны типы объектов (пиктограммы), исходный объект, целевой объект и режим аудита. Выделив правило левой кнопкой мыши, и, при наведении курсора на тип, объекты или режим аудита, появится всплывающее окно с пояснением.

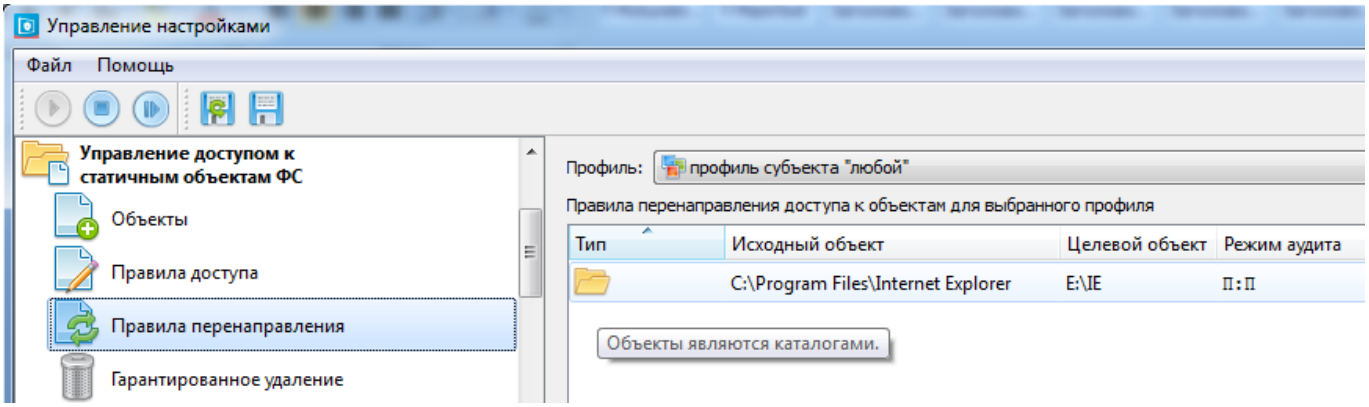


Рис.7.1.2.5.5. Интерфейс просмотра назначенных правил перенаправления

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Существует возможность **редактировать** созданные правила перенаправления запросов. Для этого следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила перенаправления» (рис.7.1.2.5.5) и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка правило перенаправления запросов доступа в интерфейсе «Правила перенаправления» (рис.7.1.2.5.5) следует нажать правой кнопкой мыши по правилу и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.3. Механизм контроля доступа к создаваемым файлам. Назначение и особенности реализации. Интерфейс

Механизм контроля доступа к создаваемым файлам может использоваться только с файловой системой NTFS.

Моделью защиты СЗИ «ViPNet SafePoint», в части реализации контроля (разграничения прав) доступа к обрабатываемой в информационной системе информации, в качестве основного механизма защиты регламентируется использование механизма контроля доступа к создаваемым файлам, по следующим причинам:

- именно для этих целей и предназначен этот механизм защиты (обрабатываемая в информационной системе информация хранится именно в создаваемых в процессе ее работы файлах);

– при использовании данного механизма защиты кардинально упрощается задача администрирования;

– данный механизм защиты позволяет реализовать корректную разграничительную политику доступа к создаваемым файлам (к обрабатываемой информации) в общем случае, в том числе, вне зависимости от наличия в системе неразделяемых ОС и приложений файловых объектов и иных условий.

Создаваемый файл однозначно размечается СЗИ «ViPNet SafePoint» при создании (вне зависимости от того, в разделяемых ли системой и приложениями папках он создается – в его атрибуты помещается учетная информация создавшего файл пользователя). Доступ к этому файлу возможен только в рамках реализуемой разграничительной политики.

Особенность реализации состоит в том, что права доступа назначаются между субъектами, а не задаются права доступа субъектов к объектам, и применяются для любых файлов, создаваемых субъектом (в том числе, в неразделяемых папках), в отношении создаваемых файлов которого реализуется контроль доступа.

При использовании данного механизма защиты не контролируется (не разграничиваются права) доступ по созданию файлов – контролируется доступ к файлам, создаваемым в процессе работы пользователя. Для контроля доступа по созданию файлов должен применяться механизм контроля доступа к статичным файловым объектам и/или механизм контроля доступа к файловым накопителям.

При настройке механизма защиты контроль доступа к создаваемым файлам можно реализовывать, как в отношении всех, так и в отношении только определенных субъектов доступа.

Поскольку обрабатываемая информация, в отличие от системных ресурсов, в общем случае может быть категорирована по уровням конфиденциальности, в СЗИ «ViPNet SafePoint» реализованы механизмы дискреционного и основанного на метках безопасности контроля доступа к создаваемым файлам, которые могут использоваться совместно. В общем случае данные механизмы контроля доступа имеют различное функциональное назначение.

Механизм контроля доступа к создаваемым файлам настраивается для субъектов, поэтому, прежде всего, следует определить для каких субъектов (см. раздел 6. Профили и субъекты доступа) будут назначены правила доступа.

Окно интерфейса механизма контроля доступа к создаваемым файлам представлено на рис.7.1.3.1. В основном окне механизма контроля доступа к создаваемым файлам существует возможность:

- включить механизм маркировки файлов при создании – флаг «Использовать маркировку файлов при создании»;
- включить механизм дискреционного управления доступом – флаг «Включить дискреционное управление доступом»;
- включить механизм контроля доступа на основе меток безопасности – флаг «Включить мандатное управление доступом»;
- создать список исключений, т.е. задать файловые объекты, файлы, сохраняемые в которых, не будут размечаться.

Для включения механизма контроля доступа к создаваемым файлам необходимо в обязательном порядке устанавливать флаг «Маркировать файлы при создании».

Для того чтобы создаваемый файл был размечен, необходимо, чтобы его объем был не менее 1 Кб.

Файлы, создаваемые пользователем SYSTEM и системными процессами, автоматически не размечаются, при этом, для них может быть разграничен доступ к файлам, создаваемым интерактивными пользователями.

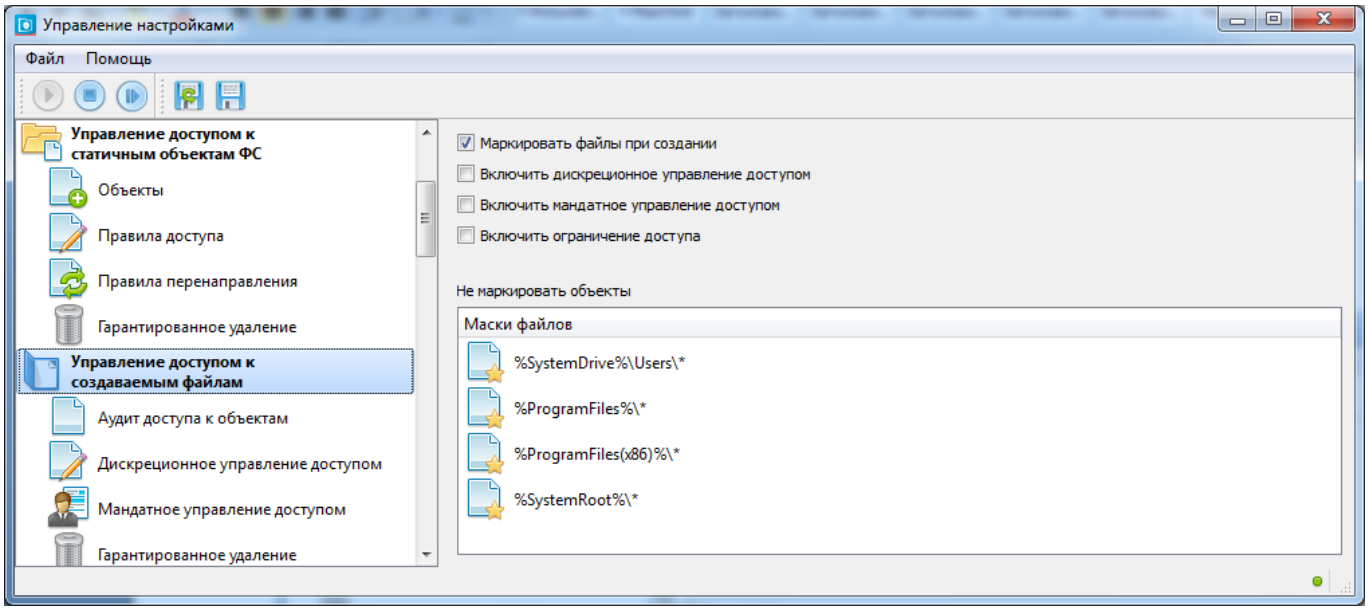


Рис.7.1.3.1. Интерфейс настройки механизма управления доступом к создаваемым файлам

7.1.3.1. Создание списка исключений

Список исключений представляет собой список объектов, при сохранении файлов в которые, файлы не будут размечаться.

По умолчанию, в СЗИ «ViPNet SafePoint» заведены следующие объекты, при сохранении файлов в которые, эти файлы не будут размечаться: %SystemDrive%\Users*, %ProgramFiles%*, %ProgramFiles(x86)%*, %SystemRoot%*. При необходимости эти объекты можно изменить или удалить.

Для создания списка объектов, при сохранении файлов в которые, файлы не будут размечаться, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Управление доступом к создаваемым файлам» в контекстном меню (рис.7.1.3.2.1) выбрать «Добавить».

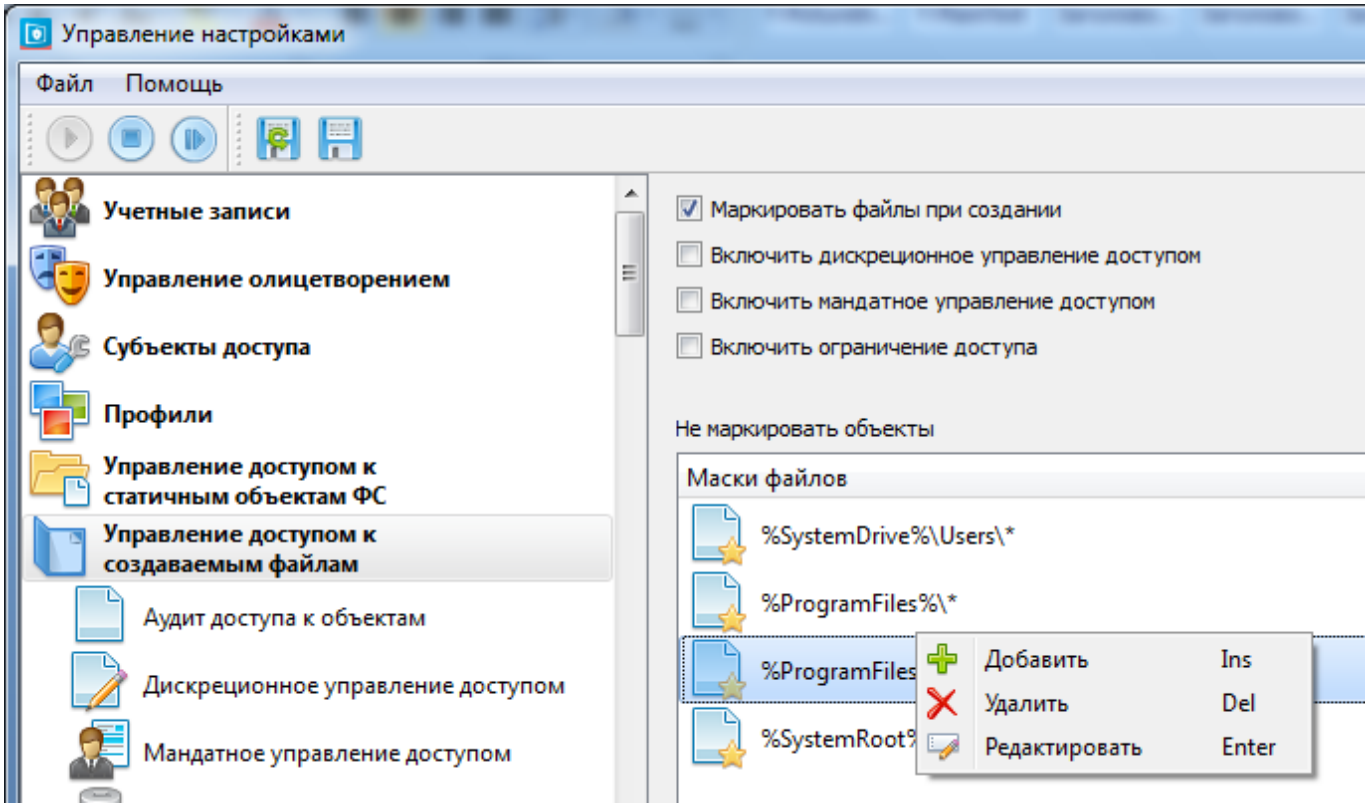


Рис.7.1.3.1.1. Контекстное меню окна управления доступом к создаваемым файлам

3. В появившемся окне «Добавление новой маски файлов» (рис.7.1.3.1.2) задать маску файлов вручную или используя «Обзор каталогов» или «Обзор файлов». Возможно использование обзоров с последующим редактированием объектов вручную, используя маски и переменные среды окружения.

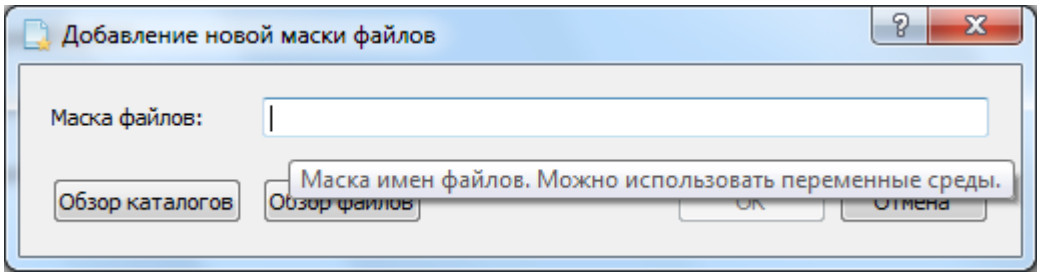


Рис.7.1.3.1.2. Окно добавления новой маски файлов

4. Нажать кнопку «ОК».

Просмотр созданного списка исключений объектов осуществляется в окне интерфейса настройки управления доступом к создаваемым файлам (рис.7.1.3.1).

Редактирование и **удаление** объектов из списка исключений осуществляется в окне интерфейса «Управление доступом к создаваемым файлам». Для этого необходимо нажать правой кнопкой мыши по объекту и в контекстном меню выбрать «Удалить» или «Редактировать». После чего внести необходимые изменения (при редактировании).

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.3.2. Механизм дискреционного контроля доступа. Назначение и особенности реализации. Интерфейс

Дискреционный принцип контроля доступа к создаваемым файлам реализует принудительное управление потоками информации (непривилегированный пользователь исключен из схемы администрирования). Соответствующими настройками может быть реализована, как разрешительная, так и запретительная политики разграничения доступа в отношении создаваемых файлов.

Основным назначением механизма контроля доступа является реализация изолированной между субъектами обработки информации в информационной системе.

Учетная информация субъекта при дискреционном контроле доступа, задается тремя сущностями: первичный идентификатор пользователя; эффективный идентификатор пользователя; процесс. Эта информация записывается в атрибуты файла диспетчером доступа СЗИ «ViPNet SafePoint», при создании файла.

При создании файлы не маркируются и, соответственно, к ним не контролируется доступ, если у субъекта создателя в качестве первичного пользователя выступает System и в качестве процесса – System.

В данном механизме защиты в разграничительной политике доступа используются не профили, а именно субъекты доступа, определяемые соответствующими тремя сущностями, т.к. именно в этом случае достигается принципиальное упрощение задачи администрирования.

Контроль доступа может быть реализован, в отношении файлов, создаваемых отдельными субъектами доступа, заданных, как «субъекты создатели» – это те субъекты, последующий доступ к файлам, создаваемым которыми, будет контролироваться (разграничиваться), так и в отношении всех создаваемых в информационной системе файлов. С использованием маски «Любой» можно реализовать контроль доступа в отношении всех создаваемых на компьютере интерактивными пользователями файлов, в этом случае все файлы, создаваемые интерактивными пользователями, будут размечаться. Для каждого заданного «субъекта создателя» задаются «субъекты, осуществляющие доступ» – те субъекты, доступ которых, к файлам, созданным соответствующим субъектом создателем, будет контролироваться (разграничиваться) и соответствующие разрешенные/запрещенные правила их доступа к этим файлам.

По умолчанию разрешены чтение, запись, удаление и переименование для субъектов к создаваемым ими же файлам.

Реализуется контроль доступа следующим образом. При создании субъектом нового файла, средством контроля доступа (диспетчером доступа СЗИ «ViPNet SafePoint») создаваемый файл автоматически размечается – файлом наследуется учетная информация субъекта доступа (определяемая соответствующими тремя сущностями), создавшего этот файл, если этот субъект задан в разграничительной политике, как «субъект создатель». Данная информация размещается диспетчером доступа в атрибутах созданного файла. Тоже происходит, если субъектом создателем модифицируется неразмеченный ранее файл.

При запросе же доступа к любому файлу, диспетчер доступа анализирует наличие, а при наличии, содержимое унаследованной файлом учетной информации создавшего его субъекта доступа. Это осуществляется, посредством считывания и анализа атрибутов файла, к которому запрошен доступ. С учетом этой информации и заданных правил доступа, диспетчер, либо разрешает запрошенный доступ, либо отказывает в нем, признавая тем самым запрошенный доступ несанкционированным.

Возможности защиты, основанной на применении данного механизма контроля доступа крайне широки, при этом сложность реализации разграничительной политики доступа минимальна, поскольку не требуется задавать правила доступа субъектов к объектам. Несколько простейших примеров реализации защиты, основанной на применении механизма контроля

доступа к создаваемым файлам. Защита от запуска на компьютере вредоносных программ. Угрозу внедрения на защищаемый компьютер и запуска вредоносных программ несут в себе именно создаваемые в процессе работы информационной системы файлы. Реализуется контроль доступ к файлам, создаваемым всеми субъектами, со стороны всех субъектов, для задания субъекта доступа «Любой» используется соответствующая маска «*». При этом «по умолчанию» разрешается чтение, запись, удаление и переименование всем субъектам ко всем создаваемым файлам, кроме исполнения создаваемых в процессе работы системы файлов – доступ на исполнение отдельно настраивается в интерфейсе. Другой пример, реализация защиты от атак на интернет-браузеры, эксплуатирующих уязвимости, обнаруживаемые в этих приложениях. Разграничительная политика простейшая. Задаются два субъекта доступа – «Все» (или «Любой») и «Интернет-браузер», определяемый соответствующим процессом интернет-браузера. Субъекту «Интернет-браузер» разрешается чтение и запись только созданных им же файлов (доступ к создаваемым остальными приложениями файлам при этом ему не разрешается), запрещается исполнять создаваемые им файлы, а всем остальным процессам (приложениям) запрещается исполнение файлов, созданным субъектом «Интернет-браузер». В результате работа потенциально уязвимого приложения в информационной системе полностью изолируется – в общем случае предотвращается возможность доступа этого приложения к обрабатываемой в информационной системе другими приложениями конфиденциальной информации.

С целью расширения функциональных возможностей механизма контроля доступа, в части реализации контроля доступа к статичным (системным) файлам, а также с целью упрощение внедрения механизма защиты в эксплуатируемую информационную систему (в которой пользователями уже созданы файлы, и они не размечены, как создаваемые), в механизме защиты предусмотрена возможность ручной разметки файлов администратором (может размечаться, как отдельный файл, так и все файлы (размечаются одинаково), располагаемые в одной папке. При этом администратором при ручной разметке также субъект доступа задается тремя сущностями: первичный идентификатор пользователя; эффективный идентификатор пользователя; процесс.

Например, администратором вручную могут быть размечены два каталога: Windows и Program Files (все файлы в этих каталогах), как созданные администратором. В разграничительной политике доступа для всех интерактивных пользователей (при необходимости, администратор может быть исключен из этого списка) должна предотвращаться возможность модификации и удаления этих файлов (устанавливается разрешение только на чтение и исполнение). В результате получим те же возможности разграничительной политики доступа, что и для случая применения механизма контроля доступа к статичным файловым объектам (соответствующий пример рассмотрен ранее).

Основное назначение данного механизма контроля доступа – разграничение прав доступа между субъектами доступа к обрабатываемой на компьютере информации. Может эффективно использоваться для реализации разграничительной политики доступа процессов к обрабатываемой на компьютере информации, в том числе, для реализации изолированных режимов обработки информации процессами (приложениями).

Выбор интерфейса механизма дискреционного контроля доступа представлен на рис.7.1.3.2.1.

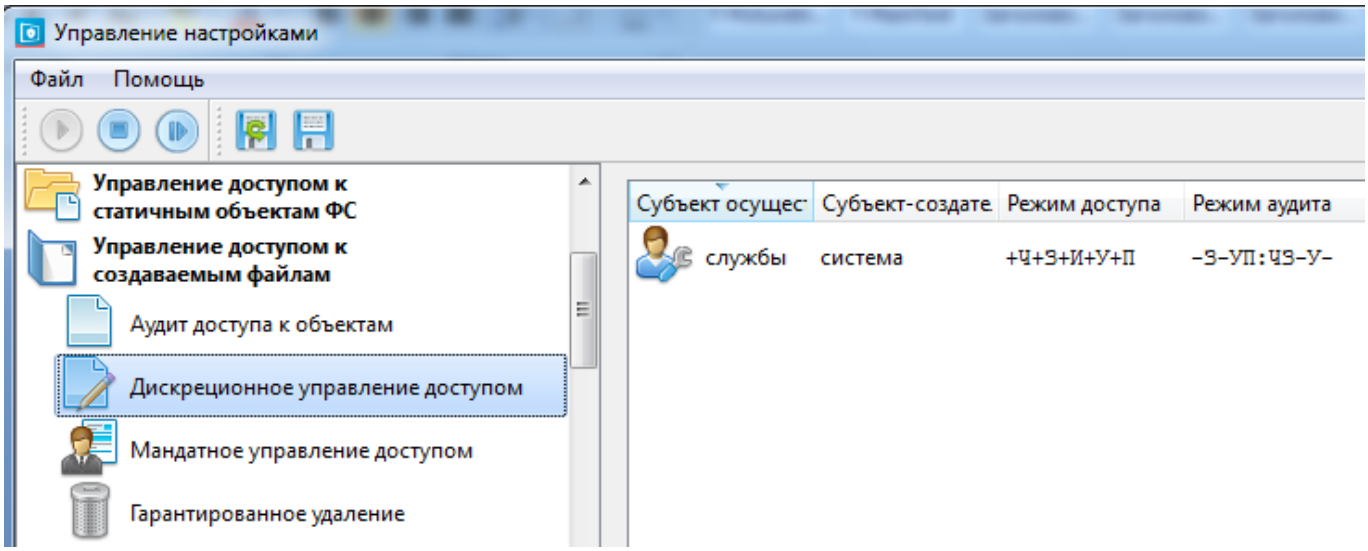


Рис.7.1.3.2.1. Интерфейс механизма дискреционного контроля доступа

Для включения данного механизма следует в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» и установить флаги «Включить дискреционное управление доступом» и «Маркировать файлы при создании».

При назначении правил дискреционного управления доступом к создаваемым файлам задаются два субъекта:

1. «Субъект-создатель» – субъект, который создает файлы в процессе работы системы.
2. «Субъект, осуществляющий доступ» – субъект, для которого устанавливаются разграничения на доступ к созданным субъектом – создателем файлам.

По умолчанию разрешены чтение, запись, удаление и переименование субъектов к создаваемым ими же файлам. Поэтому при выборе одноименных субъекта создателя и субъекта, осуществляющего доступ, откроется интерфейс с усеченными возможностями настройки, предоставляющий возможность установить режим аудита и разрешить либо запретить исполнение файлов.

Для назначения правила необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Дискреционное управление доступом».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Дискреционное управление доступом» в контекстном меню (рис.7.1.3.2.2) выбрать «Добавить правило».

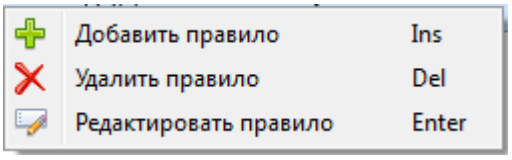


Рис.7.1.3.2.2. Контекстное меню окна дискреционного управления доступом

3. В появившемся окне «Добавление нового правила» (рис.7.1.3.2.3) произведите следующие настройки:

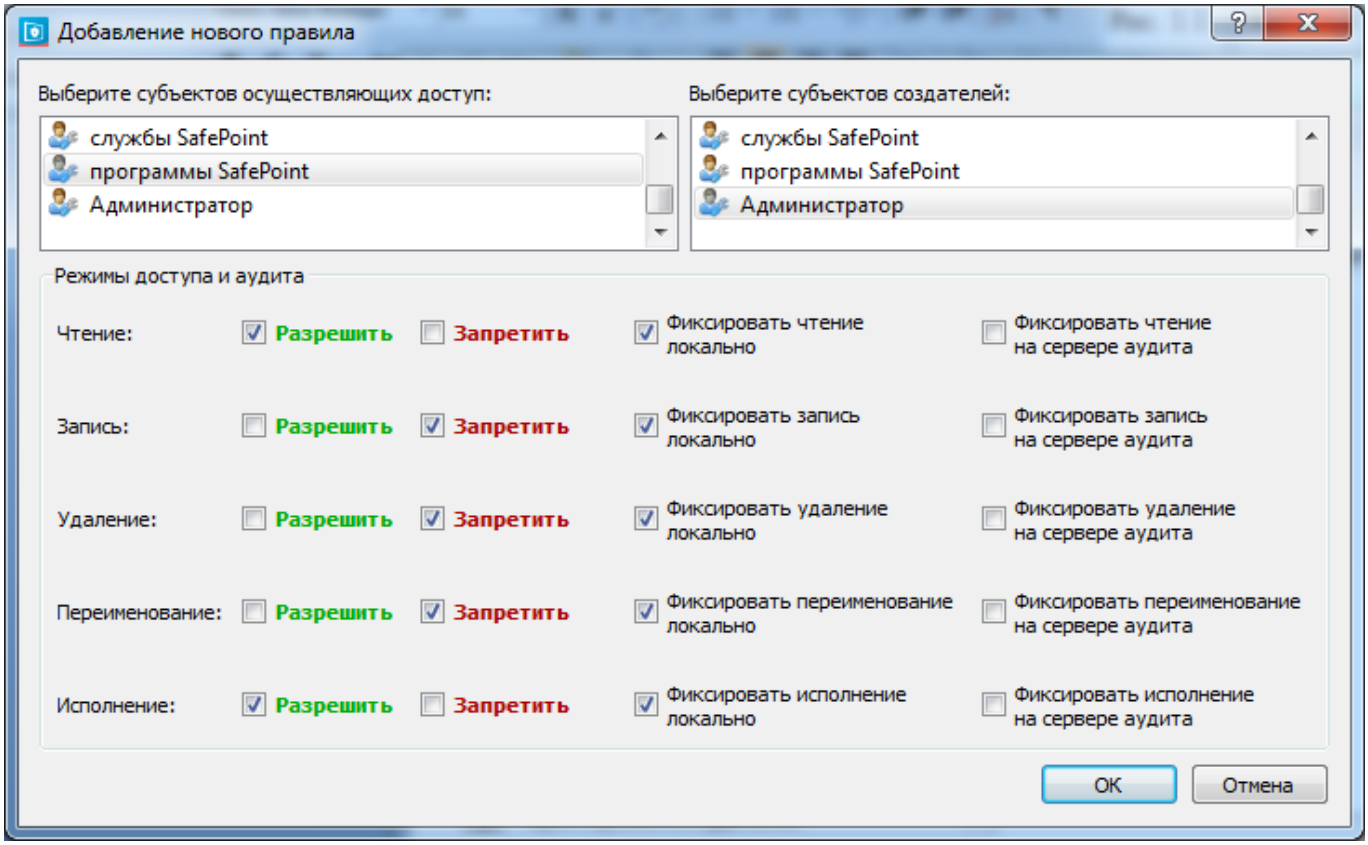


Рис.7.1.3.2.3. Окно добавления нового правила

1) Выбрать из списка субъекты, осуществляющие доступ и субъекты-создатели, существует возможность выбрать несколько субъектов.
2) Установить необходимые флаги «Разрешить» или «Запретить» для режимов доступа: чтение, запись, удаление, переименование и исполнение.
3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Дискреционное управление доступом» (рис.7.1.3.2.4). Назначенные правила представлены в интерфейсе, в котором указаны: субъект осуществляющий доступ, субъект-создатель файла, режим доступа и режим аудита. Выделив правило левой кнопкой мыши, и, при наведении курсора на субъект, режим доступа или режим аудита, появится всплывающее окно с пояснением.

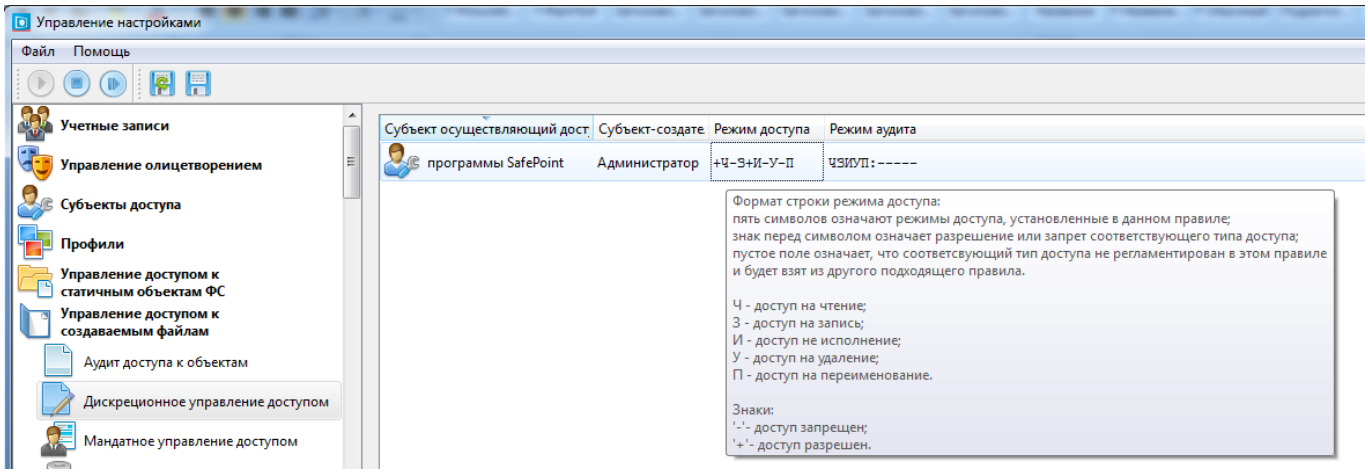
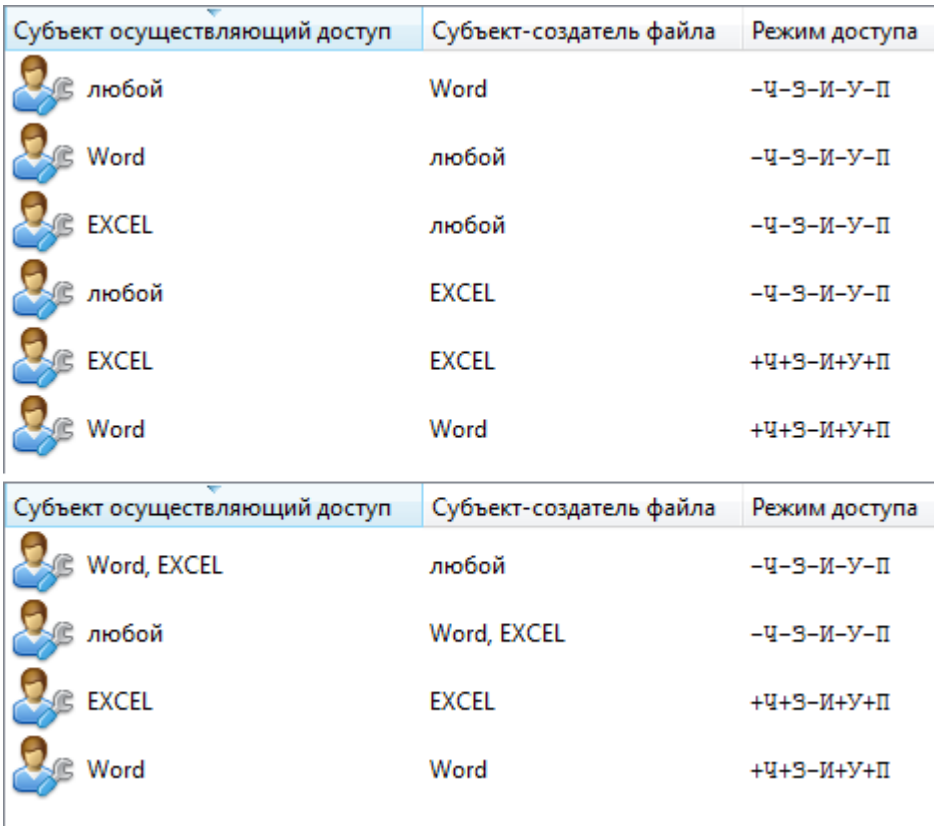


Рис.7.1.3.2.4. Интерфейс просмотра назначенных правил дискреционного управления доступом к создаваемым файлам

Правила доступа могут быть заданы как для отдельных субъектов доступа, так и путем перечисления нескольких субъектов доступа в одном правиле (рис.7.1.3.2.5).



Субъект осуществляющий доступ	Субъект-создатель файла	Режим доступа
любой	Word	-Ч-З-И-У-П
Word	любой	-Ч-З-И-У-П
EXCEL	любой	-Ч-З-И-У-П
любой	EXCEL	-Ч-З-И-У-П
EXCEL	EXCEL	+Ч+З-И+У+П
Word	Word	+Ч+З-И+У+П

Субъект осуществляющий доступ	Субъект-создатель файла	Режим доступа
Word, EXCEL	любой	-Ч-З-И-У-П
любой	Word, EXCEL	-Ч-З-И-У-П
EXCEL	EXCEL	+Ч+З-И+У+П
Word	Word	+Ч+З-И+У+П

Рис.7.1.3.2.5. Пример задания правил дискреционного управления доступом к создаваемым файлам

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Для **редактирования** назначенного правила следует нажать правой кнопкой мыши по правилу в интерфейсе «Дискреционное управление доступом» (рис.7.1.3.2.1) и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для **удаления** из списка правила следует нажать правой кнопкой мыши по правилу в интерфейсе «Дискреционное управление доступом» (рис.7.1.3.3.1) и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.3.3. Механизм контроля доступа на основе меток безопасности. Назначение и особенности реализации. Интерфейс

В первую очередь, данный механизм контроля доступа предназначен для реализации контроля доступа к категорированной информации, которая сохраняется именно в создаваемых в процессе функционирования системы файлах. Как следствие, при его использовании отсутствуют

противоречия, связанные с разметкой системных объектов и иерархических файловых объектов (размечаются непосредственно создаваемые файлы).

В качестве контролируемого объекта здесь рассматривается создаваемый файл (какого-либо контроля папок, равно как и их создания администратором, не требуется), как объект, непосредственно содержащий защищаемую информацию.

В качестве субъекта доступа в схеме контроля доступа на основе меток безопасности к создаваемым файлам выступает **метка безопасности (уровень доступа)**, присваиваемая пользователю (учетной записи).

Задание разграничительной политики доступа состоит исключительно в назначении меток безопасности субъектам (пользователям) Мс (что кардинально упрощает задачу администрирования – присваивать метки безопасности объектам не требуется). При создании субъектом нового файла (при модификации неразмеченного ранее файла), файлом наследуется учетная информация субъекта доступа – его метка безопасности Мс (обозначим унаследованную метку Мсо, при этом Мсо = Мс).

При запросе доступа к любому файлу, диспетчер доступа анализирует наличие, а при наличии, собственно значение метки безопасности Мсо, унаследованной данным файлом. При наличии метки у файла - Мсо, диспетчер сравнивает эту метку с меткой субъекта, запросившего доступ к файлу, Мс – анализирует выполнение заданных правил контроля доступа. В результате анализа данной информации, с учетом реализуемых правил контроля доступа, диспетчер либо разрешает запрошенный субъектом доступ к файлу, либо отказывает в нем. При модификации неразмеченного файла (создан субъект, для которого не задана метка безопасности), субъектом, для которого задана метка безопасности, данный файл наследует метку безопасности Мсо модифицирующего его субъекта. Доступ к неразмеченным файлам не контролируется.

Контроль доступа реализуется в отношении только тех создаваемых файлов, которые создаются субъектами с присвоенной им меткой безопасности Мс.

Данный механизм защиты позволяет задавать (из интерфейса) различные правила доступа (правила сравнения меток безопасности Мсо и Мс) при запросах доступа к файлам.

Механизмом контроля доступа на основе меток безопасности к создаваемым файлам не контролируется доступ на исполнение файлов. Для контроля исполнения файлов необходимо включить и настроить дискреционный механизм контроля доступа к создаваемым файлам.

При назначении правил доступа используются два типа доступа - режимы доступа на чтение и запись.

Режим доступа «**Чтение**» подразумевает любой доступ к объекту, не изменяющий объект, т.е. это чтение содержимого файла, атрибутов файла, владельца, разрешений, для каталогов это еще и чтение их содержимого (обзор).

Режим доступа «**Запись**» – это любой доступ изменяющий объект. К записи относятся такие действия, как: удаление, переименование, запись разрешений (в операционных системах Microsoft Windows (далее ОС Windows) «смена разрешений»), запись владельца (в ОС Windows «смена владельца»), запись данных (создание файлов), добавление данных (создание папок), запись атрибутов (только чтение, архивный, скрытый, системный), запись расширенных атрибутов (в ОС Windows «запись дополнительных атрибутов»), удаление дочернего объекта (для каталогов), создание файла при открытии, перезапись файла при открытии, замена файла при открытии.

Правила, направленные на защиту от понижения категории обрабатываемой информации (модель Белла-Лападулы):

1. Субъект С имеет доступ к объекту О в режиме “Чтения” в случае, если выполняется условие: Мс ≥ Мсо.

2. Субъект С имеет доступ к объекту О в режиме “Записи” в случае, если выполняется условие: Мс = Мсо.

Правила, определяющие «непротиворечивую модель контроля доступа на основе меток безопасности»:

1. Субъект С имеет доступ к объекту О в режиме «Чтения» и «Записи» в случае, если выполняется условие: Мс = Мсо.

2. Субъект С не имеет доступ к объекту О в случае, если выполняется условие: Мс ≠ Мсо.

Противоречие модели Белла-Лападулы состоит в следующем. Ею осуществляется защита от понижения категории обрабатываемой информации, с целью защиты от нарушения ее конфиденциальности. При этом ставится под угрозу доступность и целостность обрабатываемой конфиденциальной информации, что обусловливается следующим. Чем меньше категория конфиденциальности обрабатываемой информации (например, это открытая информация), тем менее жесткие условия ее обработки, как следствие, тем с большей вероятностью файлы, используемые для ее хранения, могут подвергаться заражению вирусами. При прочтении подобного файла приложением, это приложение наделяется вредоносными свойствами, при этом данное приложение имеет права доступа пользователя. Если этот пользователь, в рамках

реализации модели Белла-Лападулы, имеет право доступа на запись (модификацию) конфиденциальных файлов и чтения открытых данных, то с большой вероятностью зараженное (в результате прочтения файла с открытой информацией), приложение получает доступ на запись/модификацию к файлам, используемым для хранения конфиденциальной информации, в результате чего велика вероятность осуществления атаки на ее целостность и доступность.

Поскольку «непротиворечивая модель контроля доступа на основе меток безопасности», реализуемая СЗИ «ViPNet SafePoint», обеспечивает полную изолированность обработки информации пользователями, которым присвоены различные метки безопасности, при реализации разграничительной политики доступа могут быть использованы неиерархические метки (реализуется сравнение значений уровней только на совпадение/несовпадение). Это позволяет реализовать схему ролевого контроля доступа, при котором различные метки безопасности будут присваиваться пользователям, выполняющим в информационной системе различные роли (роль задается меткой безопасности, число которых, а также их смысловые транскрипции в СЗИ «ViPNet SafePoint» не ограничены).

При реализации необходимости предоставления права одному и тому же пользователю работать в одной информационной системе с информацией различных категорий конфиденциальности, для него должны быть заведены различные учетные записи для работы с информацией различных категорий конфиденциальности (число учетных записей соответствует числу категорий конфиденциальности информации, к обработке которых допущен пользователь). Простота реализации подобной разграничительной политики доступа обусловливается простотой администрирования механизма контроля доступа на основе меток безопасности к создаваемым файлам.

Разрешение доступа к информации различных уровней конфиденциальности под одной и той же учетной записью в различных режимах (сессиях – с заданием разграничительной политики между сущностями «сессия») не допустимо, т.к. в этом случае невозможна практическая реализация корректной разграничительной политики доступа к категорированной информации.

Ранее рассматривали механизм из состава СЗИ «ViPNet SafePoint», реализующий разделение файловых объектов, не разделяемых между учетными записями системой и приложениями. Подобных объектов в системе не так уж и много, поэтому их разделение средством защиты достаточно просто решаемая на практике задача.

В данном же случае речь идет о разделении между сессиями файлов, записываемых приложениями в процессе их работы под одной и той же учетной записью. Основу разграничительной политики доступа к файловым объектам для современных ОС составляет

реализация разграничений прав доступа именно между учетными записями. Сколько, и каких файлов создается и модифицируется в процессе работы приложениями, и какими приложениями, под одной учетной записью пользователя, трудно даже определить на практике. А ведь каждый подобный файл – это «канал» утечки информации – не должно быть в системе файлов, в которые разрешена запись приложениям, не разделенных между сессиями!

Проиллюстрируем сказанное простым, но достаточно показательным примером. Идентификационные данные доменов хранятся в файле cookies. Данный файл по умолчанию разделен между учетными записями. При работе в различных сессиях (открытая и конфиденциальная) одним и тем же пользователем – под одной учетной записью, интернет-браузером будет использоваться один и тот же файл cookies, формируемый приложением как в открытой, так и в конфиденциальной сессиях. Как следствие, при работе в открытой сессии становится возможным получить доступ к идентификационным данным доменов, созданных в конфиденциальной сессии. Подобных примеров масса, и все подобные файлы, с целью реализации корректной разграничительной политики доступа (не имеющей в своем составе каналов «утечки» информации), должны быть принудительно разделены между различными сессиями (т.к. именно сессия в данном случае выступает в качестве субъекта доступа).

Корректность выполнения запросом доступа правил контроля доступа на основе меток безопасности СЗИ «ViPNet SafePoint» анализируется перед анализом корректности выполнения правил дискреционного доступа к создаваемым файлам (при их совместном использовании), при этом доступ признается санкционированным, если он не противоречит правилам обоих механизмов контроля доступа к создаваемым файлам.

Основное назначение данного механизма контроля доступа, основанного на использовании меток безопасности – разграничение прав доступа к обрабатываемой на компьютере информации между пользователями. Может эффективно использоваться при реализации контроля доступа к категорированной по уровням конфиденциальности информации (иерархические метки безопасности) и для реализации изолированных режимов обработки информации пользователями, при реализации ролевой модели контроля доступа (неиерархические метки безопасности).

С целью расширения функциональных возможностей механизма контроля доступа на основе меток безопасности к создаваемым файлам, а также с целью упрощения внедрения механизма защиты в эксплуатируемую информационную систему (в которой пользователями уже созданы файлы, и они не размечены, как создаваемые), в механизме защиты предусмотрена возможность ручной разметки файлов администратором (может размечаться как отдельный файл, так и все файлы (размечаются одинаково), располагаемые в одной папке). При этом

администратором при ручной разметке в качестве учетной информации в атрибуты файлов записываются соответствующие метки безопасности.

Механизм контроля доступа на основе меток безопасности настраивается только для пользователей, которым присвоен уровень доступа. Выбор интерфейса механизма контроля доступа на основе меток безопасности – «Мандатное управление доступом» представлен на рис.7.1.3.3.1.

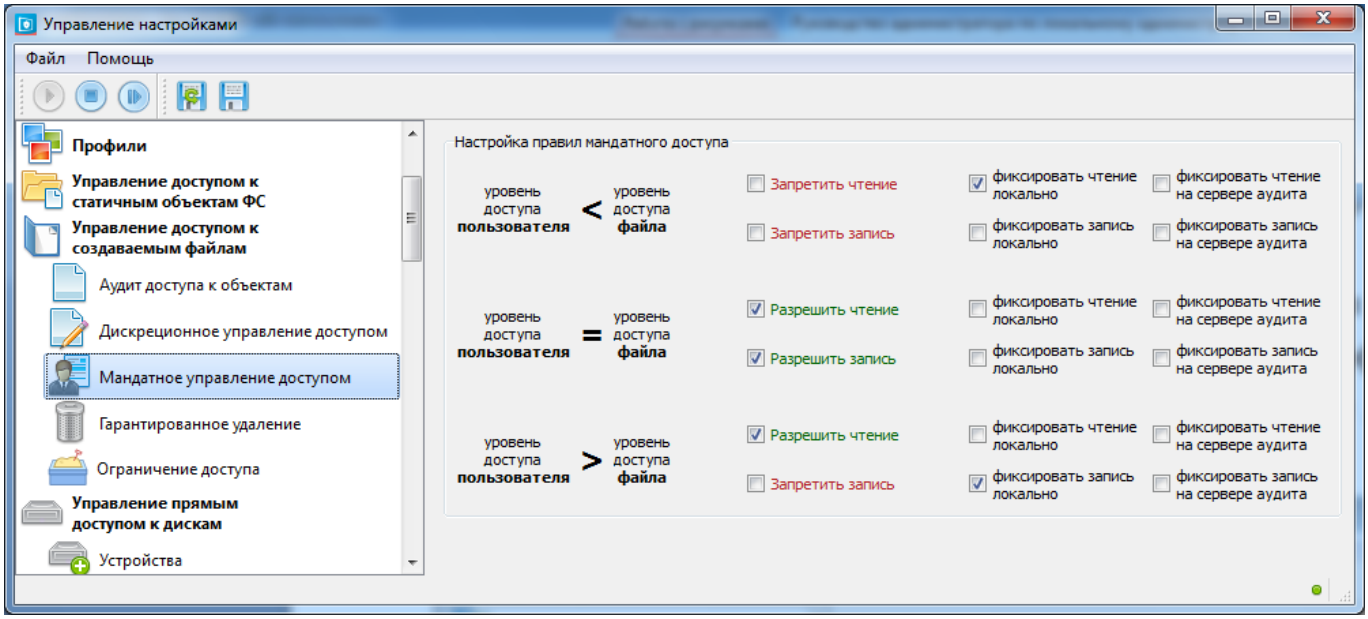


Рис.7.1.3.3.1. Интерфейс механизма контроля доступа на основе меток безопасности

Для включения данного механизма следует в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» и установить флаги «Включить мандатное управление доступом» и «Использовать маркировку файлов при создании».

7.1.3.3.1. Редактирование уровня доступа пользователя

Механизм контроля доступа на основе меток безопасности настраивается для пользователей, для которых задан уровень доступа. Для редактирования списка уровней доступа следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Учетные записи».
2. Нажать правой кнопкой мыши по пустому окну «Учетные записи» или по имени пользователя.
3. В появившемся всплывающем окне (рис.7.1.3.4.1.1) выбрать пункт «Редактировать список уровней доступа».

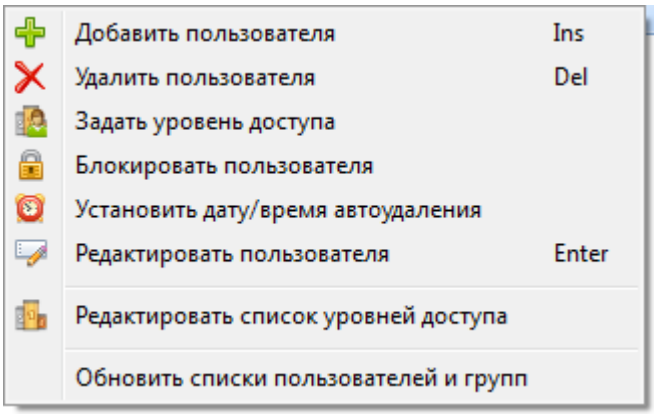


Рис.7.1.3.3.1.1. Контекстное меню окна «Учетные записи»

4. В появившемся окне (рис.7.1.3.4.1.2) следует:

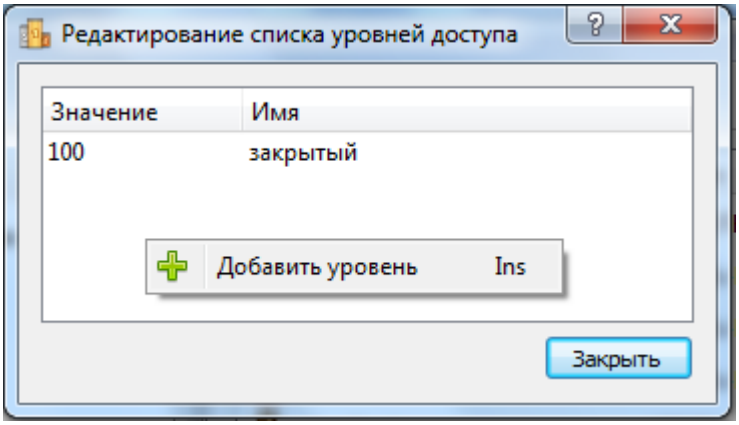


Рис.7.1.3.3.1.2. Окно «Редактирование списка уровней доступа»

1) Нажать правой кнопкой мыши по пустому окну «Редактирование списка уровней доступа».
2) В появившемся контекстном меню выбрать «Добавить уровень» (рис.7.1.3.3.1.2).
3) В появившемся окне «Добавление нового уровня доступа» (рис.7.1.3.3.1.3) ввести:
   - Имя уровня доступа;
   - Значение уровня доступа;

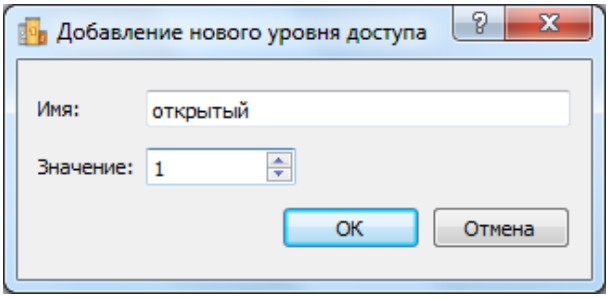


Рис.7.1.3.3.1.3. Окно добавления нового уровня доступа

4) Нажать кнопку «ОК».

Для того чтобы задать уровень доступа для пользователя необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Учетные записи».
2. Нажать правой кнопкой мыши по имени пользователя.
3. В появившемся окне (рис.7.1.3.3.1.4) выбрать уровень доступа пользователя.

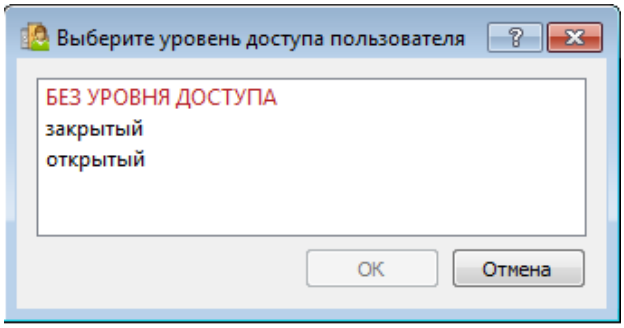


Рис.7.1.3.3.1.4. Окно «Выберите уровень доступа пользователя»

4. Нажать кнопку «ОК».

Для **просмотра** уровня доступа пользователя необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Учетные записи» (рис.7.1.3.3.1.5).

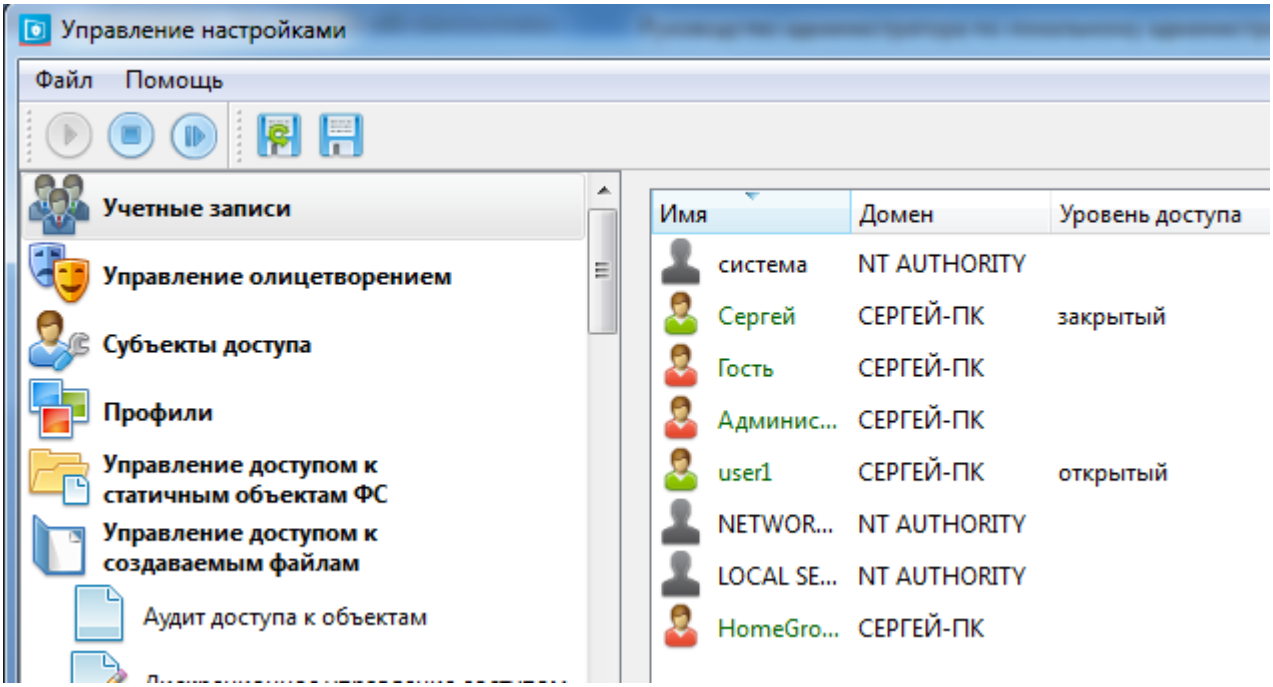


Рис.7.1.3.3.1.5. Интерфейс просмотра уровня доступа пользователей

Для **редактирования** уровня доступа пользователя необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Учетные записи» (рис.7.1.3.4.1.5). Выделить пользователя и, по двойному клику на уровень доступа, открыть окно «Выберите уровень доступа пользователя» (рис.7.1.3.4.1.6). Выбрать необходимый уровень доступа и нажать кнопку «ОК».

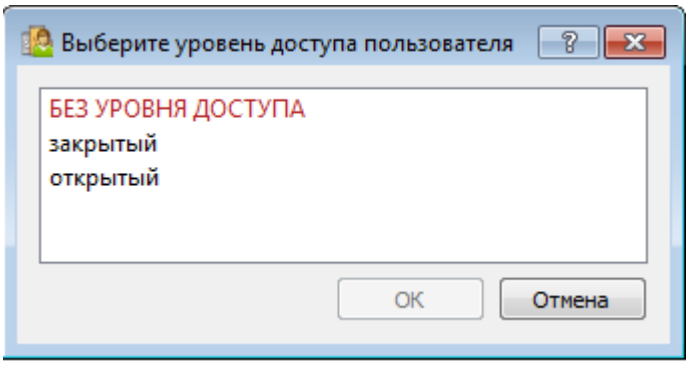


Рис.7.1.3.4.1.6. Окно выбора уровня доступа пользователя

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.1.3.3.2. Назначение правил доступа

Для настройки механизма контроля доступа на основе меток безопасности необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Мандатное управление доступом» (рис.7.1.3.3.2.1).

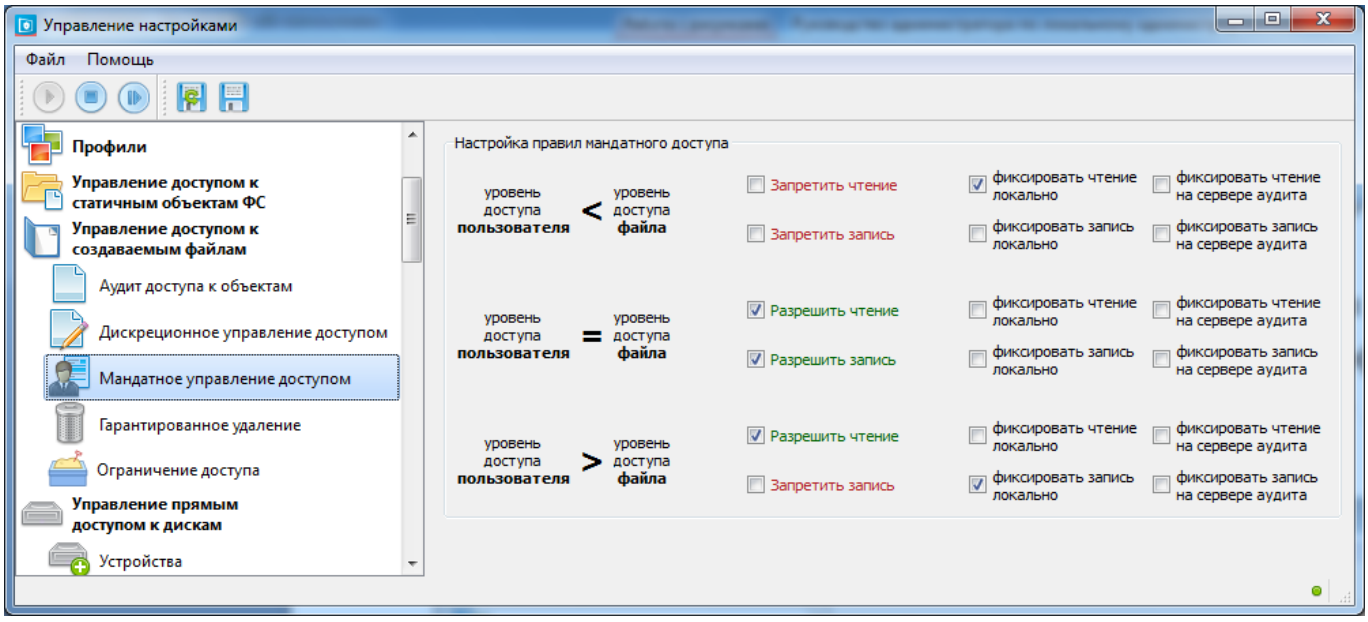


Рис.7.1.3.3.2.1. Интерфейс механизма управления доступом на основе меток безопасности

2. Установить необходимые флаги «Разрешить запись», «Разрешить чтение», «Запретить чтение», «Запретить запись».
3. Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).
4. Задать уровни доступа пользователей (см. раздел 7.1.3.3.1 «Редактирование уровня доступа пользователя»).

Просмотр назначенных правил доступа осуществляется в интерфейсе механизма контроля доступа на основе меток безопасности (рис.7.1.3.3.2.1).

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Для **редактирования** правил необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам»→ «Мандатное управление доступом» (рис.7.1.3.3.2.1). Внести необходимее изменения, поменяв флаги.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

По умолчанию в СЗИ «ViPNet SafePoint» принято, что чем меньше численное значение уровня доступа, тем выше уровень конфиденциальности. Соответственно правила по умолчанию задают, что пользователь с более высоким уровнем конфиденциальности (с меньшим числовым значением метки) имеет доступ на чтение к файлам, созданным пользователями с меньшим уровнем конфиденциальности (с большим числовым значением метки). При необходимости изменения данной конфигурации, необходимо внести изменения в правила контроля доступом на основе меток безопасности.

7.1.3.4. Утилита просмотра, создания и очистки информации о создателе

Утилита просмотра, создания и очистки информации о создателе (mdtexplore.exe) входит в состав дистрибутива СЗИ «ViPNet SafePoint». Она предоставляет администратору возможность просмотра, а также записи или очистки информации о создателях файлов (разметки).

Утилита mdtexplore.exe находится в каталоге, в которой производилась установка СЗИ. По умолчанию это каталог C:\Program Files\INFOTECS\VIPNET SAFEPOINT\bin.

Интерфейс утилиты имеет два режима отображения:

1. Режим отображения параметров субъекта создателя (Дискреционное управление доступом) (рис.7.1.3.4.1).
2. Режим отображения пользователя - создателя и его текущего уровня доступа (Контроль доступа на основе меток безопасности) (рис.7.1.3.4.2).

Для переключения режима отображения необходимо нажать правой кнопкой мышь по области строки сортировки и переключится на нужный режим.

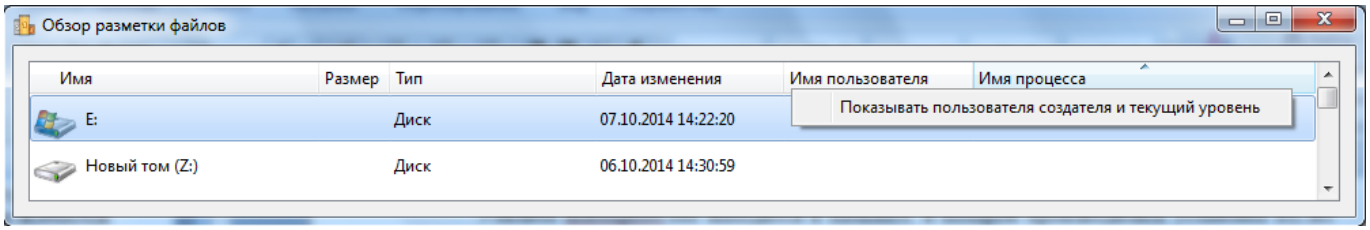


Рис.7.1.3.4.1. Интерфейс утилиты mdtexplore.exe

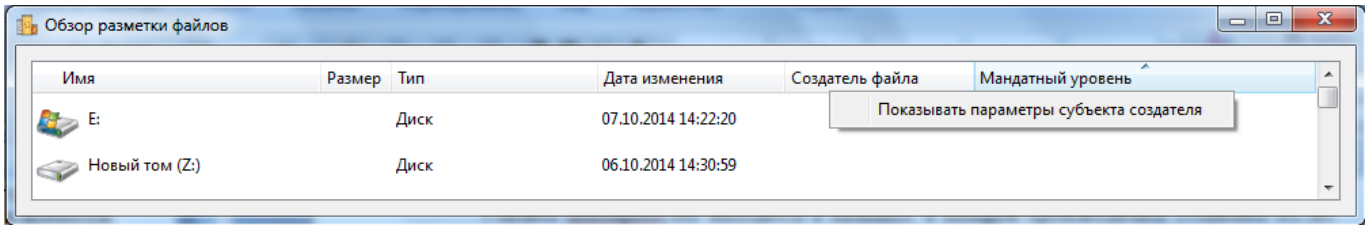


Рис.7.1.3.4.2. Интерфейс утилиты mdtexplore.exe

Использовать данную утилиту следует совместно с механизмами дискреционного контроля доступа и контроля доступа на основе меток безопасности**.**

Очистка информации о создателе конкретного файла

Для очистки информации о создателе конкретного файла, необходимо:

1. Нажать правой кнопкой мыши по необходимому файлу.
2. В контекстном меню выбрать «Стереть информацию о создателе».
3. В появившемся окне «Подтвердите очистку» нажать «Да».

Очистка информации о создателе файлов, входящих в каталоги и подкаталоги

Для очистки информации о создателе файлов, входящих в каталоги и подкаталоги, необходимо:

1. Нажать правой кнопкой мыши по необходимому каталогу.
2. В контекстном меню выбрать «Стереть информацию о создателе».
3. В появившемся окне «Очистка информации о создателе» выделить необходимого пользователя или пользователей путем комбинации «Ctrl + левая кнопка мыши».
4. Для очистки информации о создателе файлов в подкаталогах необходимо установить флаг «Рекурсивно» и нажать кнопку «ОК» (рис.7.1.3.4.3).

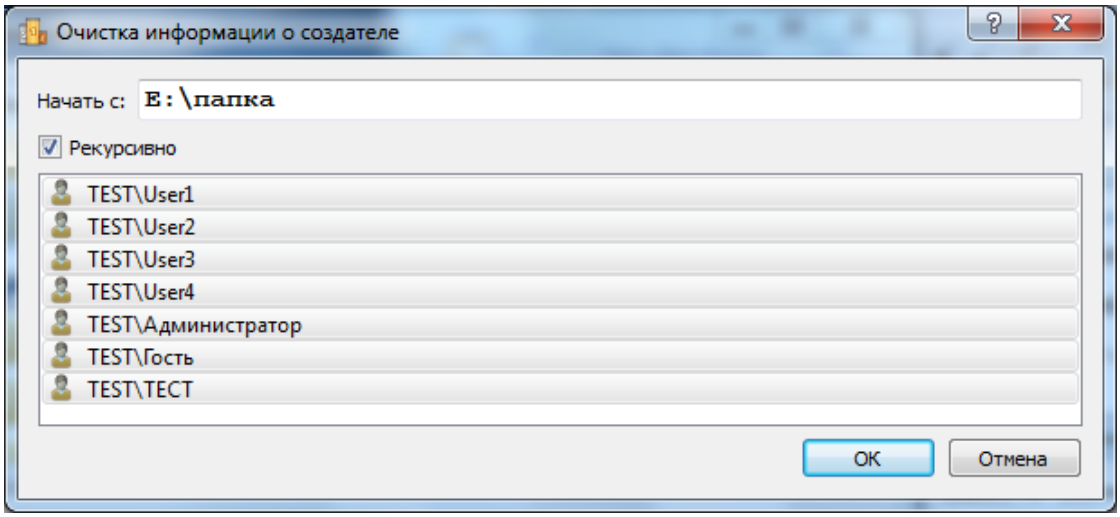


Рис.7.1.3.4.3. Окно очистки информации о создателе

Запись информации о создателе конкретного файла

Для записи информации о создателе конкретного файла, необходимо:

1. Нажать правой кнопкой мыши по необходимому файлу.
2. В контекстном меню выбрать «Запись информацию о создателе».
3. В появившемся окне выбрать «Первичного» и «Вторичного» пользователя, процесс (по умолчанию в качестве процесса назначается mdtexplore.exe) и нажать кнопку «ОК» (рис.7.1.3.4.3).

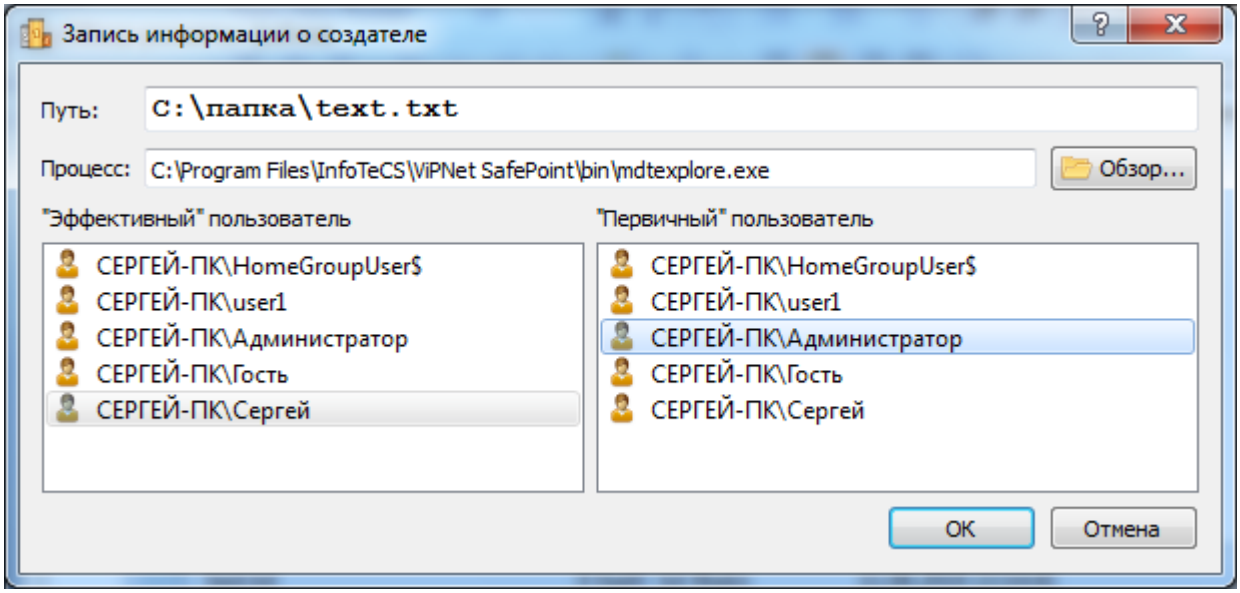


Рис.7.1.3.4.3. Окно записи информации о создателе

Запись информации о создателе файлов, входящих в каталоги и подкаталоги

Для записи информации о создателе файлов, входящих в каталоги и подкаталоги, необходимо:

1. Нажать правой кнопкой мыши по необходимому каталогу.
2. В контекстном меню выбрать «Запись информации о создателе».

3. В появившемся окне «Запись информации о создателе» произвести следующие действия:
   1) Установить флаг «Установить для всех файлов в дереве ФС, начиная с указанного каталога».
   2) Выбрать «Первичного», «Эффективного» пользователей и процесс (по умолчанию в качестве процесса назначается mdtexplore.exe), нажать кнопку «ОК» (рис.7.1.3.4.4).

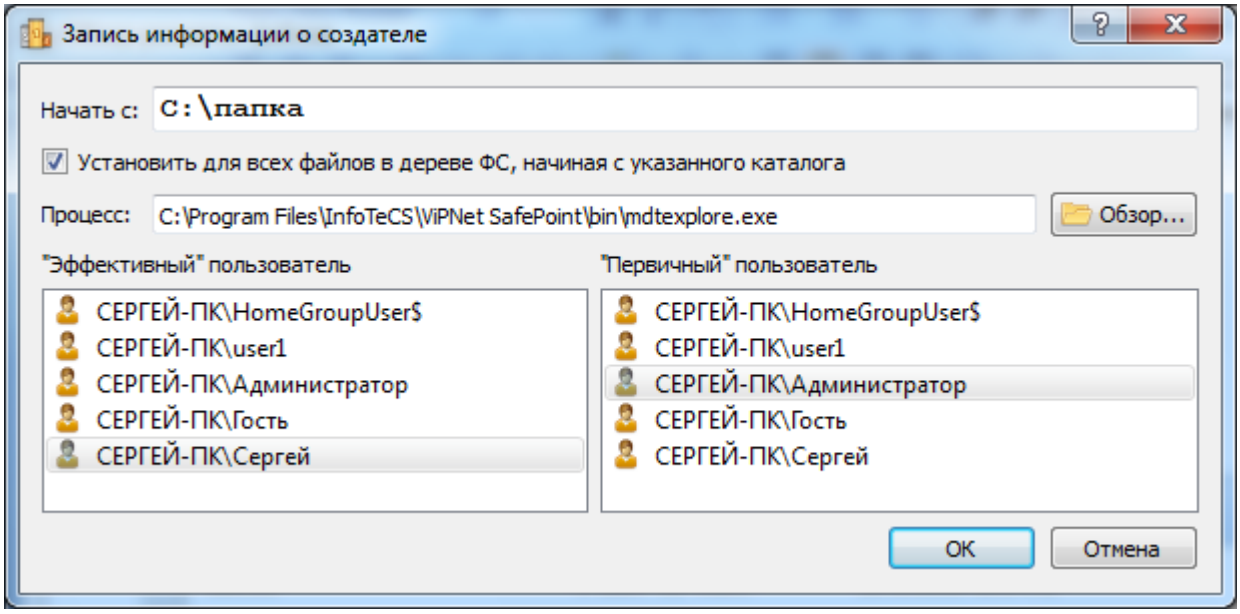
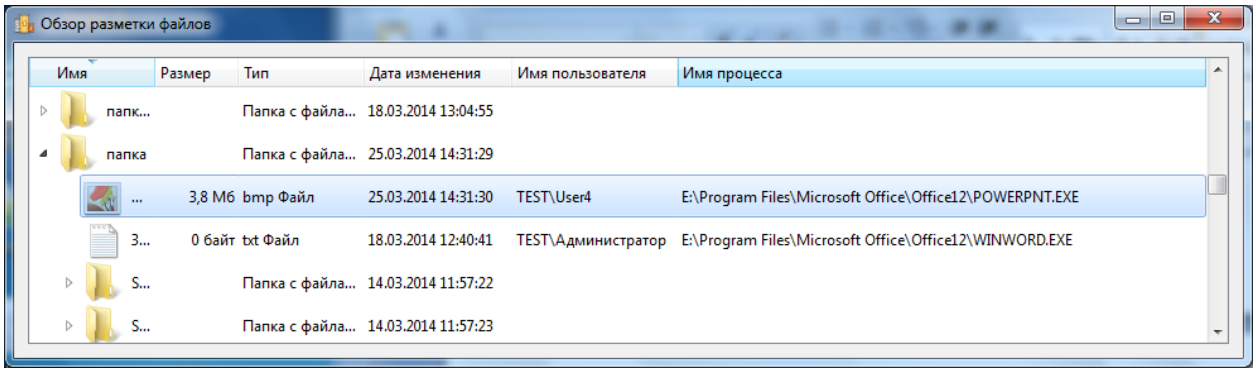


Рис.7.1.3.4.4. Окно записи информации о создателе

Для **просмотра** информации о создателе файла, необходимо в интерфейсе утилиты выбрать интересующий файл (рис.7.1.3.4.5). В интерфейсе утилиты отражается: имя, размер файла, тип, дата его изменения, имя пользователя и процесса (при использовании механизма дискреционного контроля доступа) или имя создателя файла и его «мандатный уровень» – уровень доступа (при использовании механизма контроля доступа на основе меток безопасности).



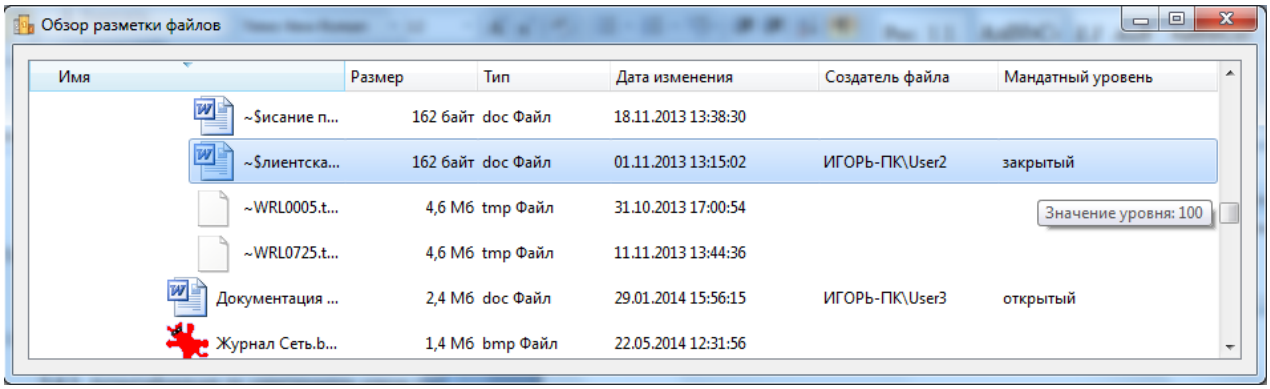


Рис.7.1.3.4.5. Просмотр информации о создателе

Просмотр при помощи утилиты сетевых дисков, внешних накопителей и CD-ROM не доступен, поскольку в большинстве случаев они имеют файловую систему FAT, для которой разметка файлов не возможна, в интерфейсе они будут отражаться другим цветом (рис.7.1.3.4.6).

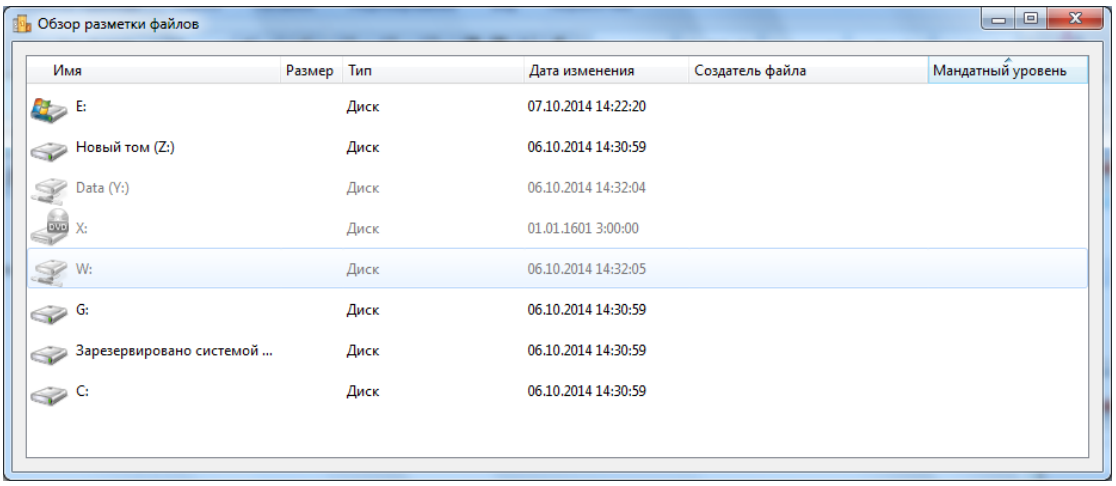


Рис.7.1.3.4.6. Интерфейс утилиты mdtexplore.exe

7.1.3.5. Механизм ограничения доступа. Назначение и особенности реализации. Интерфейс

Основным назначением механизма ограничения доступа является защита создаваемых файлов, полученных из доверенных источников, от атак, связанных с прочтением потенциально опасных (критичных) файлов, полученных из недоверенных источников (по сети, из интернета, в качестве почтового вложения).

При открытии файлов, полученных из недоверенных источников, процесс может быть наделен вредоносными свойствами. Следовательно, задачей является защита создаваемых доверенных файлов от атак со стороны процессов после прочтения ими файлов, источник получения которых является недоверенным.

Так можно задать, что любой процесс, осуществивший доступ к файлу, созданному, например, почтовым клиентом (к вложению), который автоматически размечается при его

создании, помещается в «песочницу» – его доступ к доверенным файлам при этом автоматически запрещается.

Приведем пример ограничения доступа. Пусть имеются файловые объекты, один из которых создан в Microsoft Word на рабочей станции и считается доверенным, а другой получен в качестве почтового вложения, т.е. считается критичным. Соответственно, разметка данных файлов показывает, что доверенный файл создан процессом «Winword.exe», а критичный – процессом «Outlook.exe».

При включенном механизме ограничения доступа и настроенном правиле фиксации параметров разметки для субъектов «Winword.exe» и «Outlook.exe» после открытия файла редактором Winword.exe, созданного «Outlook.exe» (т.е. критичного), невозможно будет открыть, удалить или переименовать файл, считающийся доверенным.

После открытия критичного файла, созданного «Outlook.exe» при уже открытом доверенном файле (т.е. созданном «Winword.exe»), работа с данным доверенным файлом возможна. Однако после редактирования данного доверенного файла будет предложено его сохранение как нового файла, запись, переименование и удаление иных доверенных файлов будет запрещена. При этом разметка созданного файла будет отражать, что данный файл был создан процессом «Outlook.exe». Таким образом, он также будет считаться файлом, полученным из недоверенного источника.

Разметка критичных файлов при работе с ними не изменяется. При каждом последующем доступе к ним будут работать правила ограничения доступа.

В данном механизме защиты в разграничительной политике доступа используются не профили, а именно субъекты доступа, определяемые соответствующими тремя сущностями, т.к. именно в этом случае достигается принципиальное упрощение задачи администрирования.

При указании субъекта-создателя файла определяется процесс, создающий файл, полученный из недоверенного источника.

Субъектом, осуществляющим доступ, является тот субъект, который будет помещен в «песочницу» при прочтении файла, полученного из недоверенного источника.

Реализуется ограничение доступа следующим образом. При создании субъектом нового файла, средством контроля доступа (диспетчером доступа СЗИ «ViPNet SafePoint») создаваемый файл автоматически размечается – файлом наследуется учетная информация субъекта доступа (определяемая соответствующими тремя сущностями), создавшего этот файл, если этот субъект задан в разграничительной политике, как «субъект создатель». Данная информация размещается

диспетчером доступа в атрибутах созданного файла. Тоже происходит, если субъектом создателем модифицируется неразмеченный ранее файл.

При запросе же доступа к любому файлу, диспетчер доступа анализирует наличие, а при наличии, содержимое унаследованной файлом учетной информации создавшего его субъекта доступа. Это осуществляется, посредством считывания и анализа атрибутов файла, к которому запрошен доступ.

При отсутствии разметки либо несоответствии разметки субъекту-создателю в правиле, ограничение в доступе не осуществляется. При открытии файла, разметка которого соответствует разметке субъекта-создателя, инициализируются заданные правила разграничения доступа.

Необходимо изолировать данные, полученные из недоверенных источников, для защиты доверенных данных.

Интерфейс механизма ограничения доступа представлен на рис. 7.1.3.5.1.

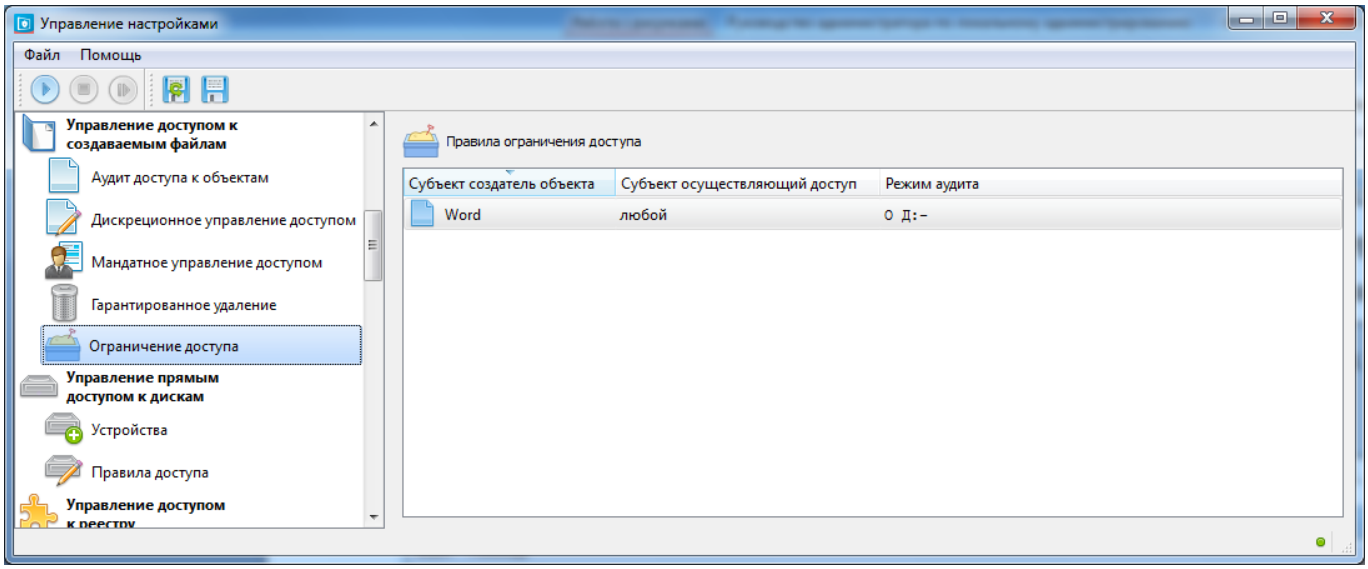


Рис. 7.1.3.5.1. Интерфейс механизма ограничения доступа

Для включения данного механизма следует в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» и установить флаги «Маркировать файлы при создании» и «Включить ограничение доступа».

При назначении правил ограничения доступа задаются два субъекта:

1. «Субъект-создатель» – субъект, который создает файлы в процессе работы системы.

2. «Субъект, осуществляющий доступ» – субъект, для которого устанавливаются ограничения на доступ к созданным субъектом-создателем файлам.

Для назначения правила необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Ограничение доступа».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Ограничение доступа» в контекстном меню (рис. 7.1.3.5.2) выбрать «Добавить правило».

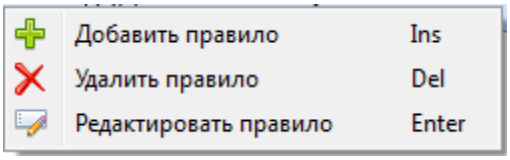


Рис.7.1.3.5.2. Контекстное меню окна ограничения доступа

3. В появившемся окне «Добавление нового правила» (рис.7.1.3.5.3) произвести следующие настройки:

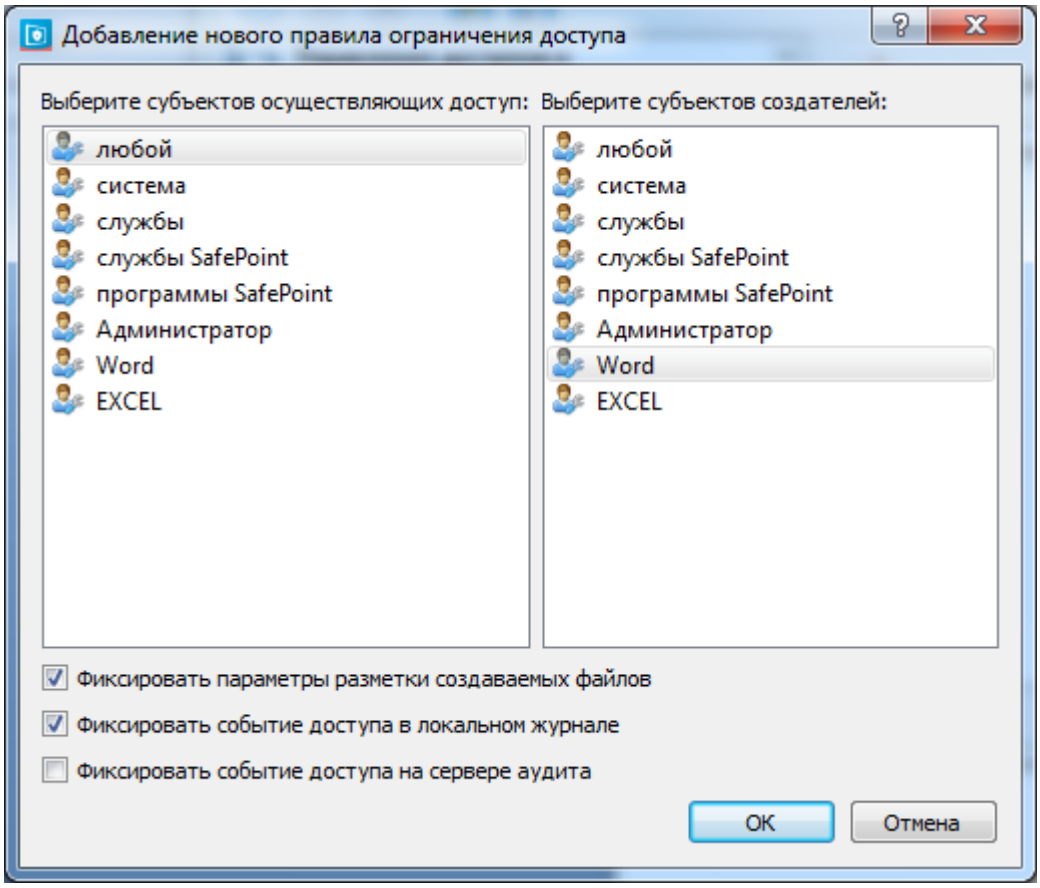


Рис.7.1.3.5.3. Окно добавления нового правила

1) Выбрать из списка субъект, осуществляющий доступ и субъект-создатель.
2) Установить флаг «Фиксировать параметры разметки создаваемых файлов».
3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Ограничение доступа» (рис.7.1.3.5.4). Назначенные правила представлены в интерфейсе, в котором указаны: субъект осуществляющий доступ, субъект-создатель файла и режим аудита.

Выделив правило левой кнопкой мыши, и, при наведении курсора на субъект или режим аудита, появится всплывающее окно с пояснением.

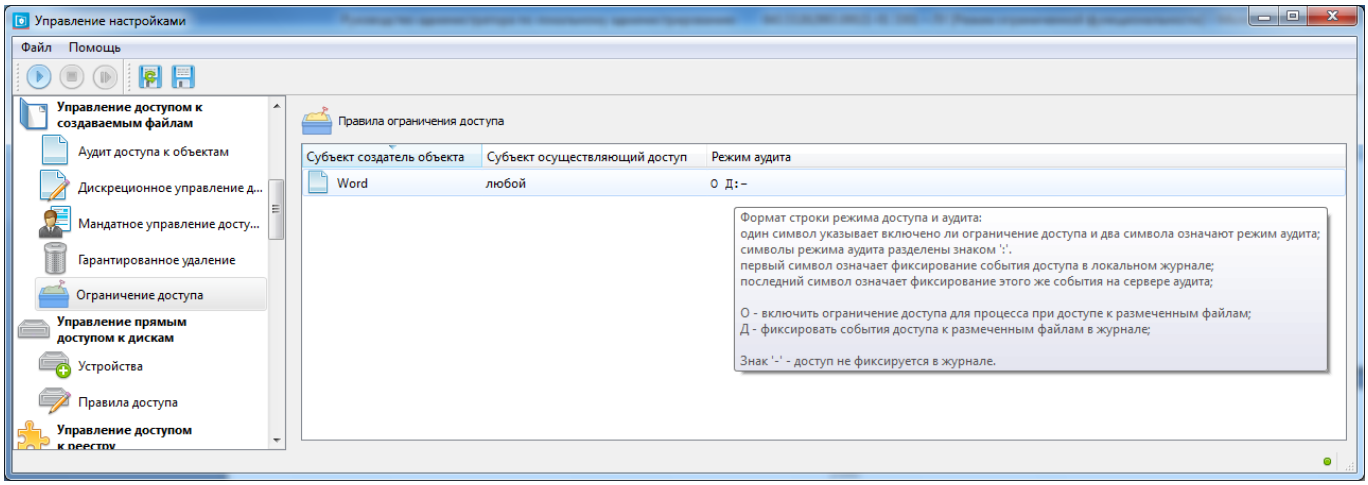


Рис.7.1.3.5.4. Интерфейс просмотра назначенных правил ограничения доступа

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к файловой системе».

Для **редактирования** назначенного правила следует нажать правой кнопкой мыши по правилу в интерфейсе «Ограничение доступа» (рис.7.1.3.5.1) и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для **удаления** из списка правила следует нажать правой кнопкой мыши по правилу в интерфейсе «Ограничение доступа» (рис.7.1.3.5.1) и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.2. МЕХАНИЗМ КОНТРОЛЯ ДОСТУПА К ОБЪЕКТАМ РЕЕСТРА. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Данный механизм защиты, предназначенный для реализации разграничительной политики доступа в отношении объектов (ветвей и ключей) реестра ОС, реализуется по полной аналогии с механизмом контроля доступа к статичным файловым объектам, с естественной поправкой, определяемой физическим смыслом данных объектов, в том числе, и при задании правил доступа (отсутствует исполнение).

Особенностью реализации опять же является то, что правила доступа задаются для субъектов (а не назначаются в качестве атрибутов доступа объектам). Это позволяет при минимальных усилиях строить сложнейшие разграничительные политики доступа к объектам реестра ОС, в том числе для процессов (приложений), за счет использования масок при задании

объектов доступа, а также реализовать принципиально новые возможности защиты информации от несанкционированного доступа в информационной системе.

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к объектам реестра.

Разграничительная политика реализуется для профилей.

Основное назначение данного механизма контроля доступа – защита от атак, направленных на системные объекты - объекты реестра ОС (атаки на отказ в обслуживании).

Выбор окна интерфейса механизма «Управление доступом к реестру» представлен на рис.7.2.1. Данный механизм следует настраивать последовательно, сначала задать объекты доступа, далее правила доступа.

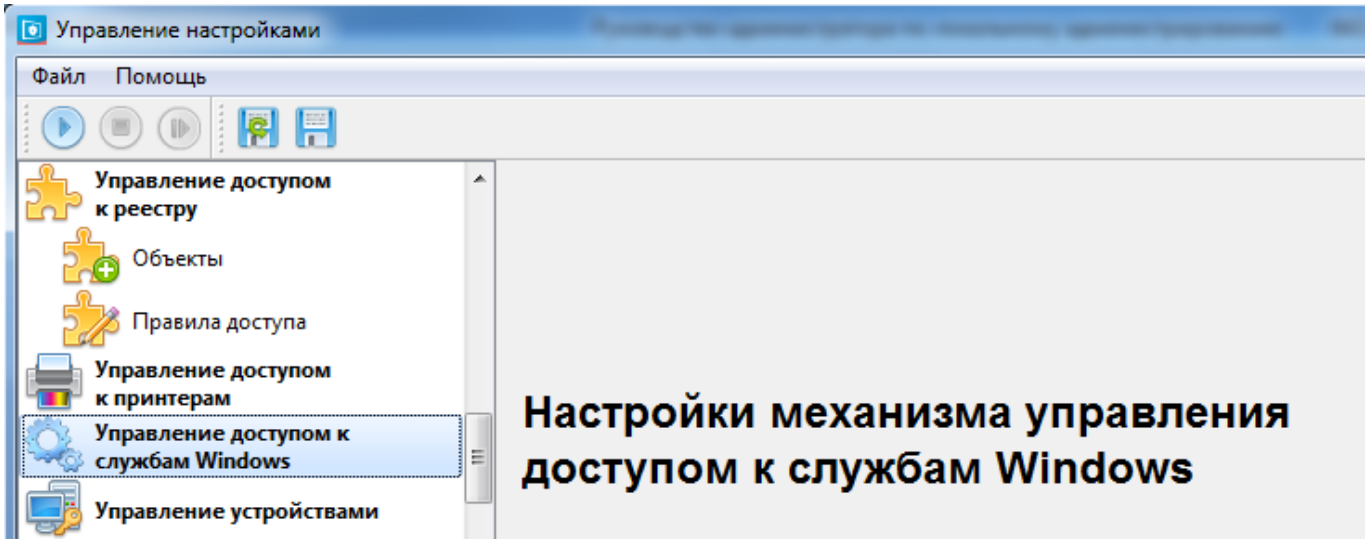


Рис.7.2.1. Интерфейс механизма «Управление доступом к реестру»

При настройке данного механизма следует учитывать следующее:

1. Объект необходимо задавать в соответствии с его типом (значение ключа реестра, ключ реестра, маска).

В СЗИ «ViPNet SafePoint» реализуется разграничение доступа профилей к объектам реестра. С учетом возможности использования масок, одновременно несколько объектов реестра, заведенных в СЗИ «ViPNet SafePoint», могут соответствовать реальному объекту реестра, к которому запрашивается доступ. Для выбора правила доступа введен следующий приоритет обработки объектов реестра, заданных в СЗИ «ViPNet SafePoint»: значение ключа реестра, ключ реестра, маска. Заданные в СЗИ «ViPNet SafePoint» объекты реестра сравниваются с реальными объектами в заданном порядке обработки (значение ключа реестра, ключ реестра, маска) и выбирается правило доступа для первого из подошедших объектов реестра.

2. При задании разграничений на ветвь реестра, разграничения накладываются непосредственно на саму ветвь и на все ее содержимое.
3. При указании «*» после ветви реестра разграничения действуют только на ее содержимое, на саму ветвь разграничения не действуют. Следовательно, при указании «*» после ветви реестра, во избежание отмены разграничений на содержимое, в связи с доступными изменениями ветви (переименование, удаление), необходимо задавать отдельное правило на саму ветвь.

Нельзя указывать после ветви реестра «\», т.к. разграничения на ветвь и ее содержимое не будут действовать.

7.2.1. Создание, редактирование и удаление объектов доступа

Для создания объекта реестра, для которого далее будут назначены правила доступа, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к реестру» → «Объекты».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Объекты» и в контекстном меню (рис.7.2.1.1) выбрать пункт «Добавить объект».

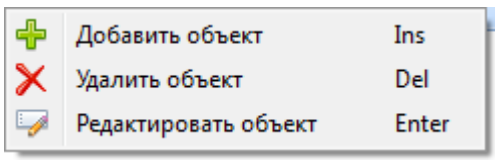


Рис.7.2.1.1. Контекстное меню окна «Объекты»

3. В появившемся окне «Создание нового объекта реестра» (рис.7.2.1.2) произвести следующие настройки:

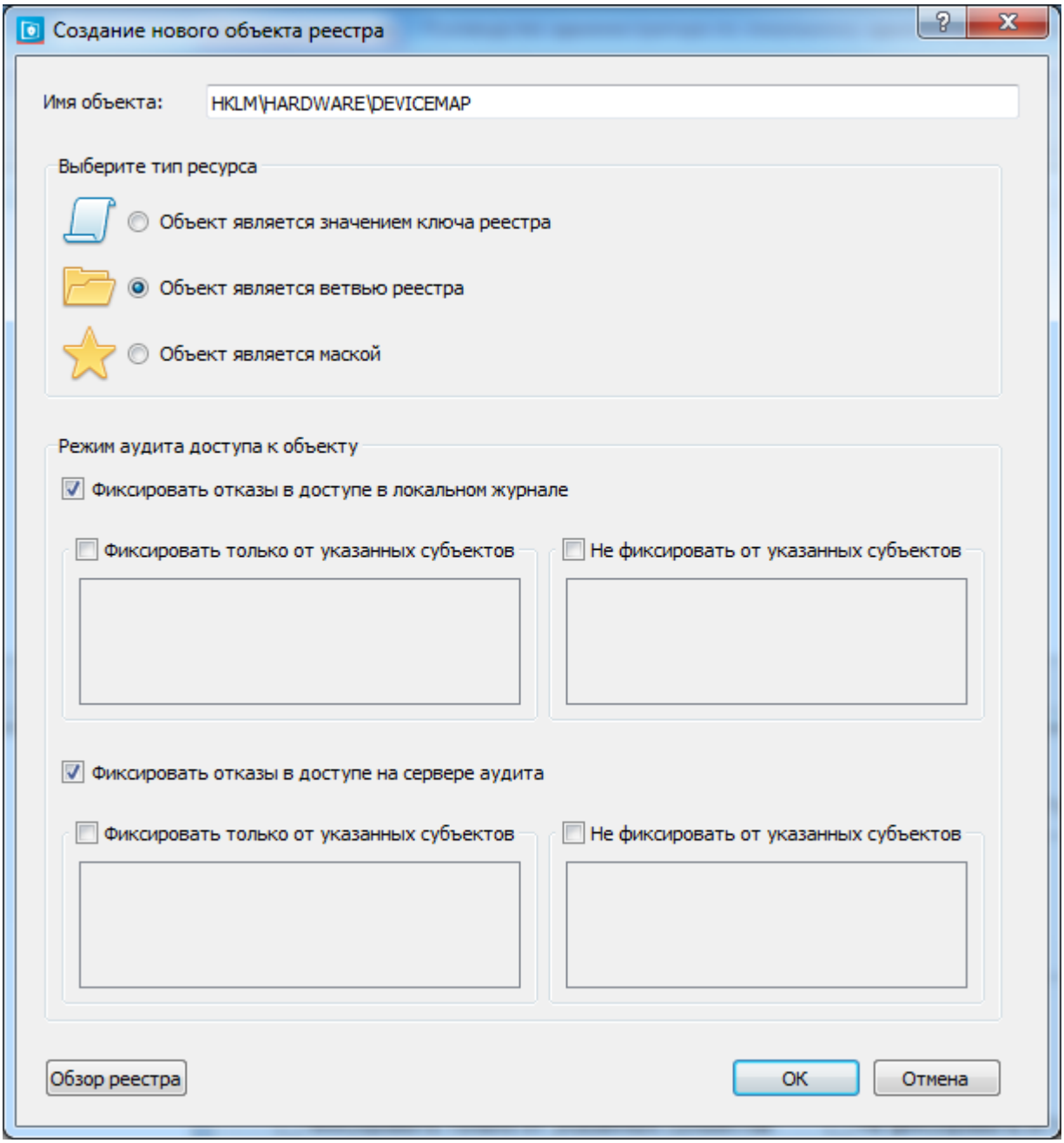


Рис.7.2.1.2. Окно создания нового объекта реестра

1) Задать имя объекта, используя «Обзор реестра» или вручную, путем указания маски или полнопутевого имени ветви реестра или имени ключа реестра.

Выбрав объект реестра, используя «Обзор реестра», в строке «Имя объекта» появится имя выбранного объекта реестра, это имя возможно дополнить, используя маски для задания необходимого пользователю объекта.

В СЗИ «ViPNet SafePoint» реализован собственный обзор реестра системы, для работы с ним обязательно должна быть запущена служба СЗИ «ViPNet SafePoint».

В обзоре отображаются только три корневые ветви реестра, в связи с тем, что некоторые ветви, отображаемые в «regedit.exe», не существуют на самом деле, а являются символическими ссылками на существующие. Ветвь HKEY_CLASSES_ROOT - это символическая ссылка на объединение ветвей HKEY_LOCAL_MACHINE\SOFTWARE\Classes (классы, зарегистрированные для всего компьютера) и HKEY_CURRENT_USER\Software\Classes (классы, зарегистрированные для текущего пользователя), HKEY_CURRENT_USER - это символическая ссылка на одну из ветвей корневой ветви HKEY_USERS (объекты реестра всех пользователей, которые успешно зашли в систему.

Для указания объекта, отображаемого в «regedit.exe» в одной из ветвей, являющихся символическими ссылками на корневые ветви, необходимо найти этот объект в корневых ветвях.

В обзоре СЗИ «ViPNet SafePoint» при наведении курсора мыши на SID пользователя появляется подсказка, отражающая имя пользователя, соответствующее данному идентификатору.

2) Выбрать тип объекта или оставить автоматически установленный тип.
3) Настроить режим аудита (раздел 15.2.2 Аудит доступа к объектам).

4. Нажать кнопку «ОК».

Для **просмотра** заведенных объектов реестра необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к реестру» → «Объекты». Объекты реестра отображаются в интерфейсе (рис.7.2.1.3), в котором указан тип объекта (пиктограмма), его имя, и режим аудита. Выделив объект левой кнопкой мыши, и, при наведении курсора на тип, имя или режим аудита объекта, появится всплывающее окно с пояснением.

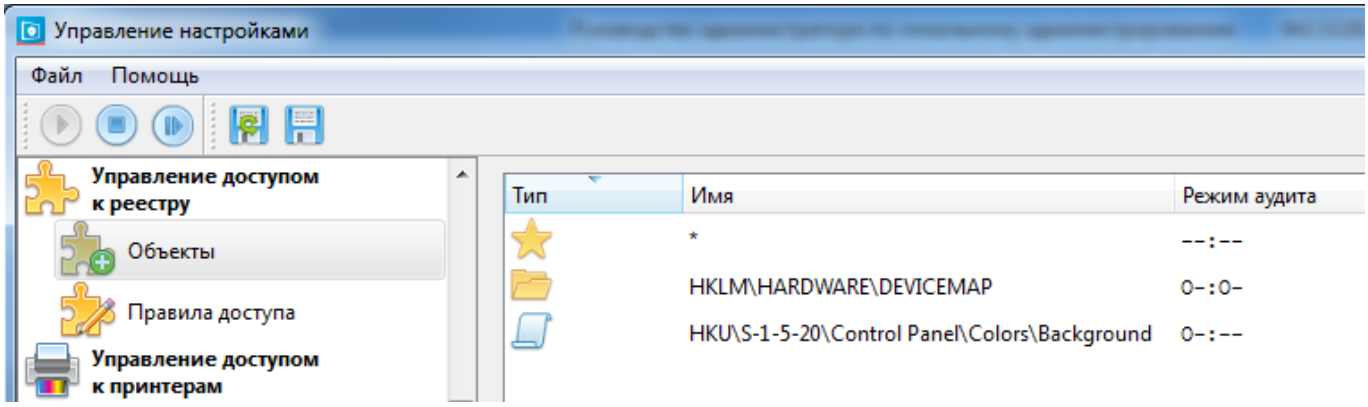


Рис.7.2.1.3. Интерфейс просмотра заведенных объектов реестра

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к реестру».

Существует возможность **редактировать** уже добавленный объект. Для этого следует выбрать объект и нажать правой кнопкой мыши и в контекстном меню выбрать «Редактировать объект», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка объект доступа следует нажать правой кнопкой мыши по объекту и в контекстном меню выбрать «Удалить объект».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.2.2. Назначение правил доступа

Для назначения правил доступа к объектам реестра, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к реестру» → «Правила доступа».
2. В выпадающем списке «Профиль» выбрать профиль, для которого будут назначены правила доступа.
3. Нажать правой кнопкой мыши по пустой области интерфейса «Правила доступа» в контекстном меню (рис.7.2.2.1) выбрать «Добавить правило».

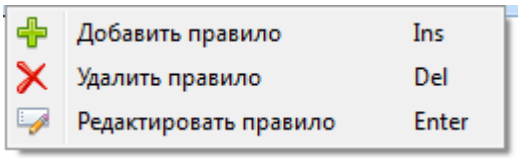


Рис.7.2.2.1. Контекстное меню окна «Правила доступа»

4. В появившемся окне «Добавить новое правило» (рис.7.2.2.2) произвести следующие настройки:

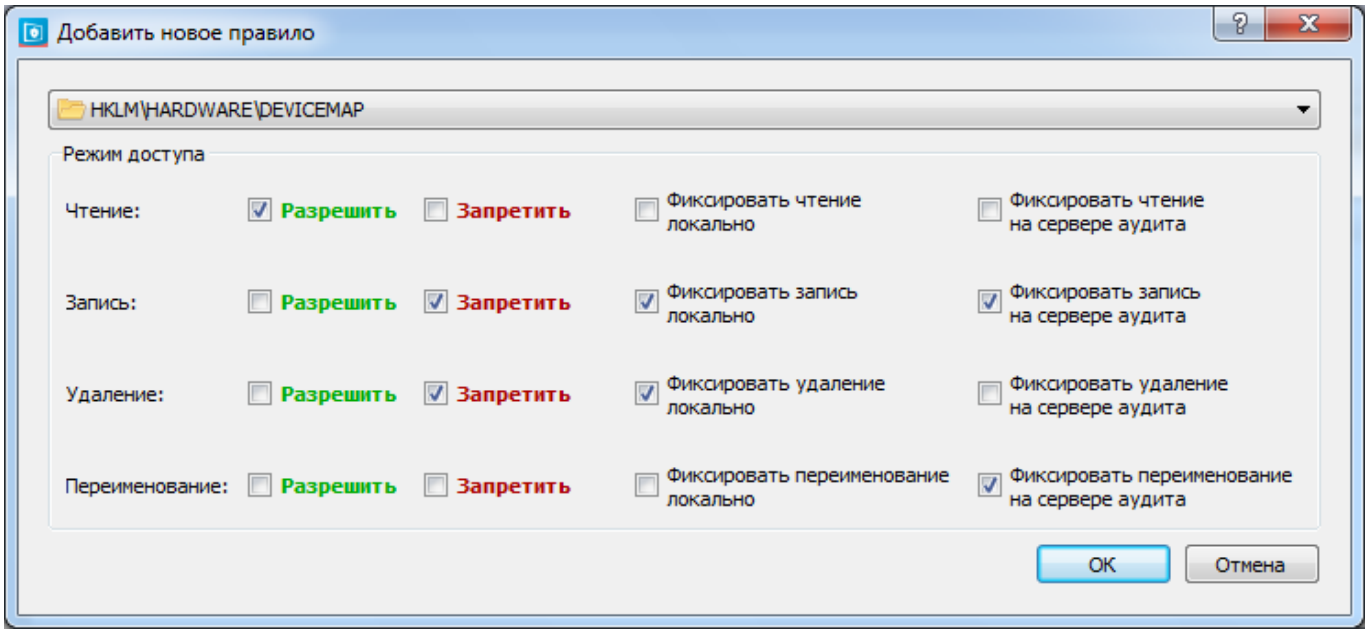


Рис.7.2.2.2. Окно добавления нового правила

1) Выбрать объект из выпадающего списка.
2) Установить необходимые флаги «Разрешить» или «Запретить» на чтение, запись, удаление, переименование.

Режим доступа «Чтение» подразумевается любой доступ к объекту реестра, не изменяющий сам объект. Режим доступа «Запись» – это любой доступ изменяющий объект реестра. Режимы доступа «Удаление» и «Переименование» являются частными случаями режима доступа «Запись» и вынесены отдельно для удобства процесса администрирования.

3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил доступа к объектам реестра необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к реестру» → «Правила доступа». Назначенные правила представлены в интерфейсе, в котором указаны: тип объекта (пиктограмма), объект реестра, режим доступа и режим аудита. Выделив правило левой кнопкой мыши, и, при наведении курсора на тип объекта, объект реестра, режим доступа или режим аудита, появится всплывающее окно с пояснением (рис.7.2.2.3).

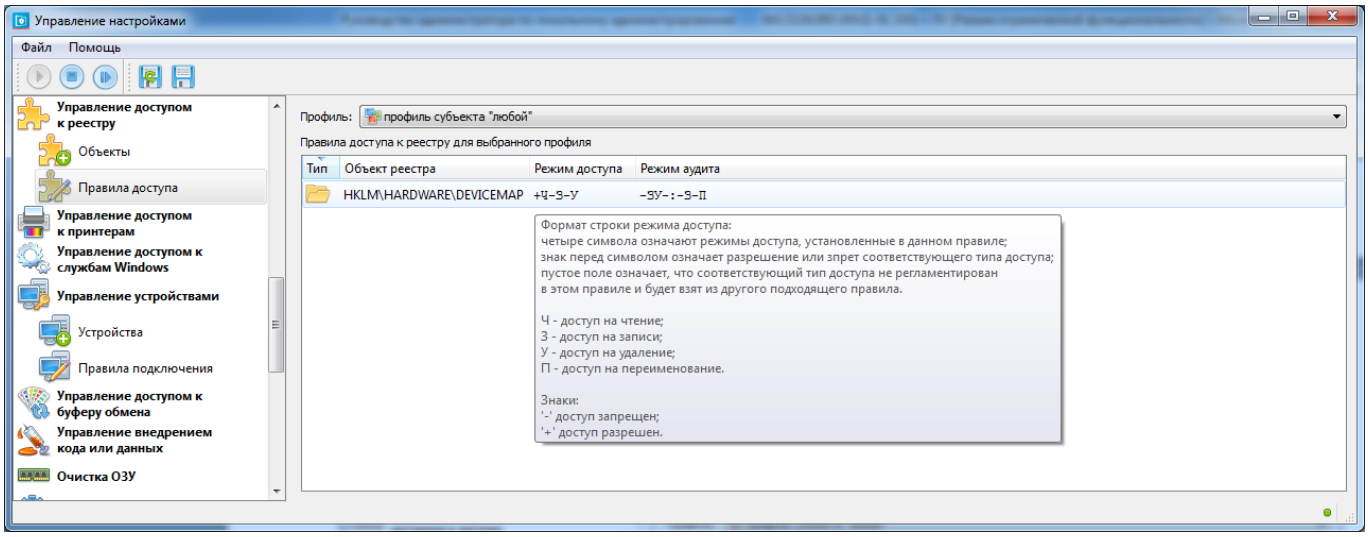


Рис.7.2.2.3. Интерфейс просмотра назначенных правил доступа к объектам реестра

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к реестру».

Существует возможность **редактировать** назначенные правила. Для этого следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка правило доступа следует нажать правой кнопкой мыши по правилу и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.3. МЕХАНИЗМ КОНТРОЛЯ ДОСТУПА К ПРИНТЕРАМ. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Данный механизм защиты, предназначенный для реализации разграничительной политики доступа в отношении объектов – принтеры, реализуется по полной аналогии с механизмом контроля доступа к статичным файловым объектам, с естественной поправкой, определяемой физическим смыслом данных объектов.

Особенностью реализации опять же является то, что правила доступа задаются для субъектов (а не назначаются в качестве атрибутов доступа объектам). Объектами доступа выступают принтеры, как локальные, так и сетевые, к которым можно получить доступ с компьютера, на котором настраивается соответствующая разграничительная политика доступа.

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то

запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к принтерам.

Разграничительная политика реализуется для профилей.

Основное назначение данного механизма контроля доступа – предоставление возможности печати конфиденциальных документов только на тех принтерах, которые располагаются в контролируемой зоне, и в отношении которых реализованы соответствующие организационные (физические) меры защиты.

Окно интерфейса механизма «Управление доступом к принтерам» представлено на рис.7.3.1. Данный механизм следует настраивать последовательно, сначала задать принтеры, далее назначить правила доступа.

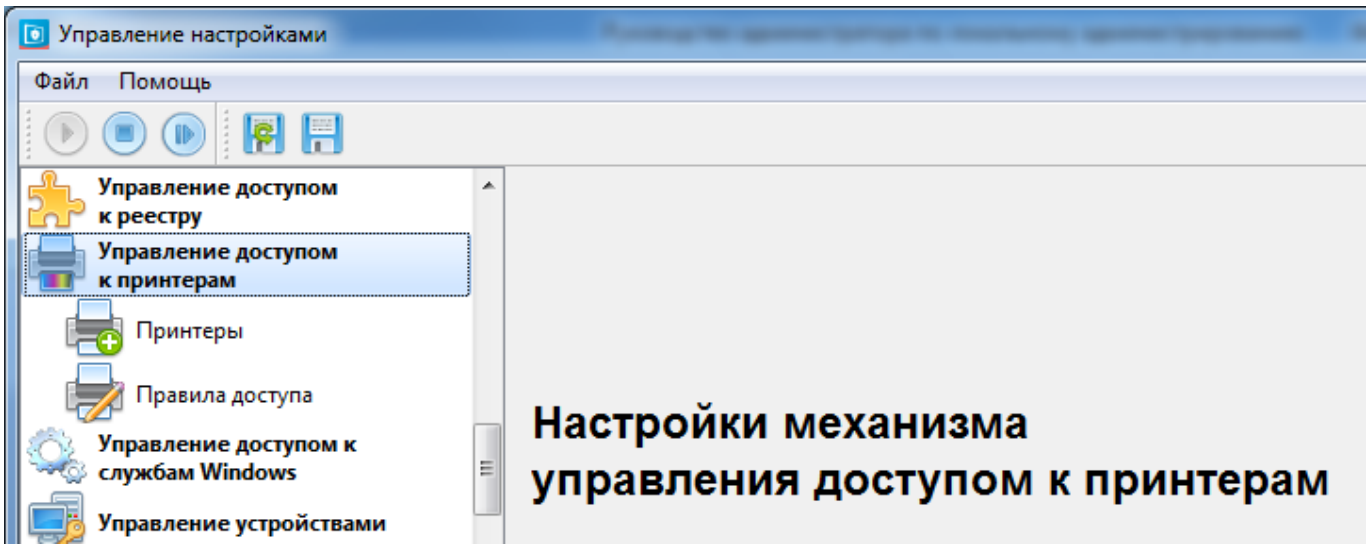


Рис.7.3.1. Интерфейс настройки механизма управления доступом к принтерам

7.3.1. Создание, редактирование и удаление принтера

Для добавления нового принтера, для которого далее будут назначены правила доступа, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к принтерам» → «Принтеры».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Принтеры» и в контекстном меню (рис.7.3.1.1) выбрать «Добавить принтер».

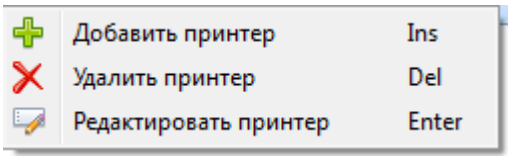


Рис.7.3.1.1. Контекстное меню окна «Принтеры»

3. В появившемся окне «Добавление нового принтера» (рис.7.3.1.2) произвести следующие настройки:

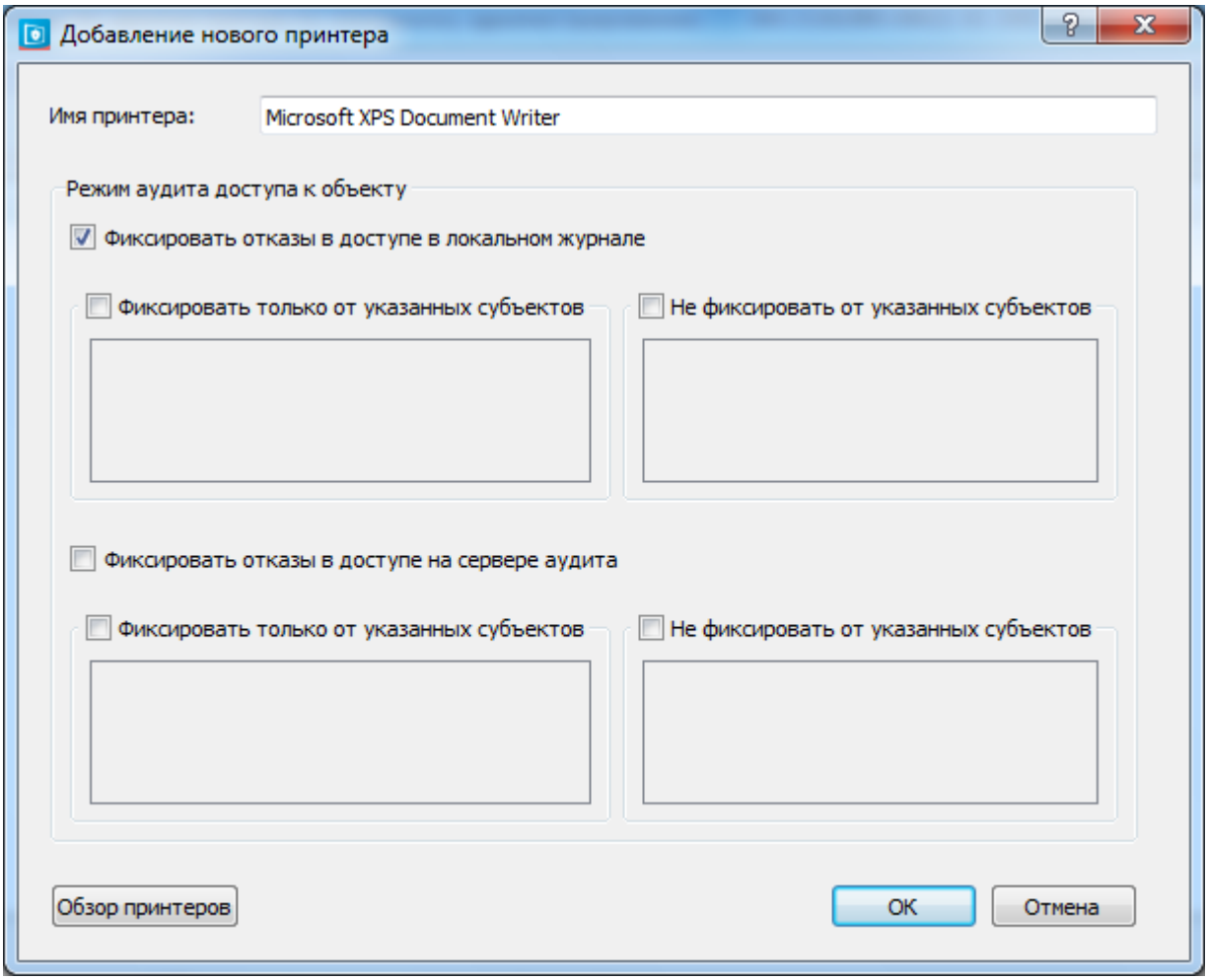


Рис.7.3.1.2. Окно добавления нового принтера

1) Задать имя принтера, используя «Обзор принтеров» или вручную, путем указания маски или полнопутевого имени.

В обзоре отображаются локальные принтеры и, заведенные в системе, сетевые принтеры.

2) Настроить режим аудита (раздел 15.2.2 Аудит доступа к объектам).

4. Нажать кнопку «ОК».

Для **просмотра** заведенных принтеров необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к принтерам» →

«Принтеры». Заведенные принтеры отображаются в интерфейсе (рис.7.3.2.3), в котором указаны: тип объекта (пиктограмма), его имя и режим аудита. Выделив принтер левой кнопкой мыши, и, при наведении курсора на тип, имя или режим аудита, появится всплывающее окно с пояснением.

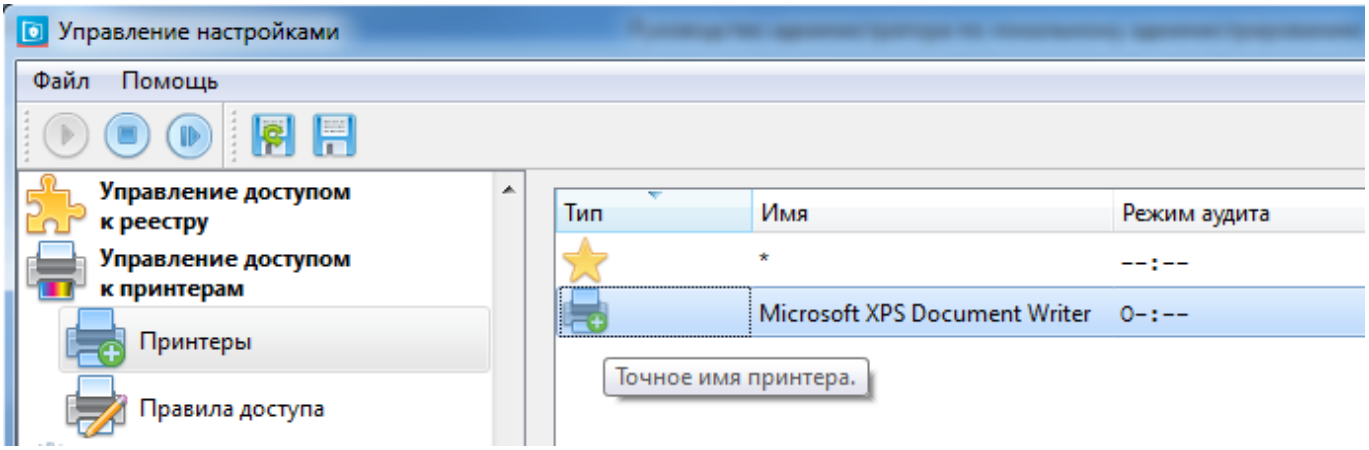


Рис.7.3.1.3. Интерфейс просмотра заведенных принтеров

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом принтерам».

Существует возможность **редактировать** уже добавленный принтер. Для этого следует нажать правой кнопкой мыши по выбранному принтеру в области интерфейса «Принтеры» и в контекстном меню выбрать «Редактировать принтер», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка принтер следует нажать правой кнопкой мыши по выбранному принтеру в области интерфейса «Принтеры» и в контекстном меню выбрать «Удалить принтер».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.3.2. Назначение правил доступа

Правила доступа задаются для профилей. Для назначения правил доступа к принтерам, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к принтерам» → «Правила доступа».
2. В выпадающем списке «Профиль» выбрать профиль, для которого будут назначены правила доступа.
3. Нажать правой кнопкой мыши по пустой области интерфейса «Правила доступа для выбранного профиля» и в контекстном меню (рис.7.3.2.1) выбрать «Добавить правило».

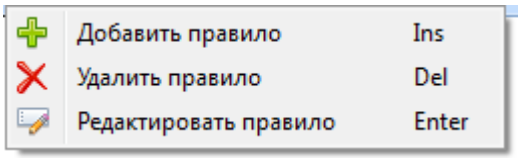


Рис.7.3.2.1. Контекстное меню окна «Правила доступа»

4. В появившемся окне «Добавление нового правила» (рис.7.3.2.2) следует:

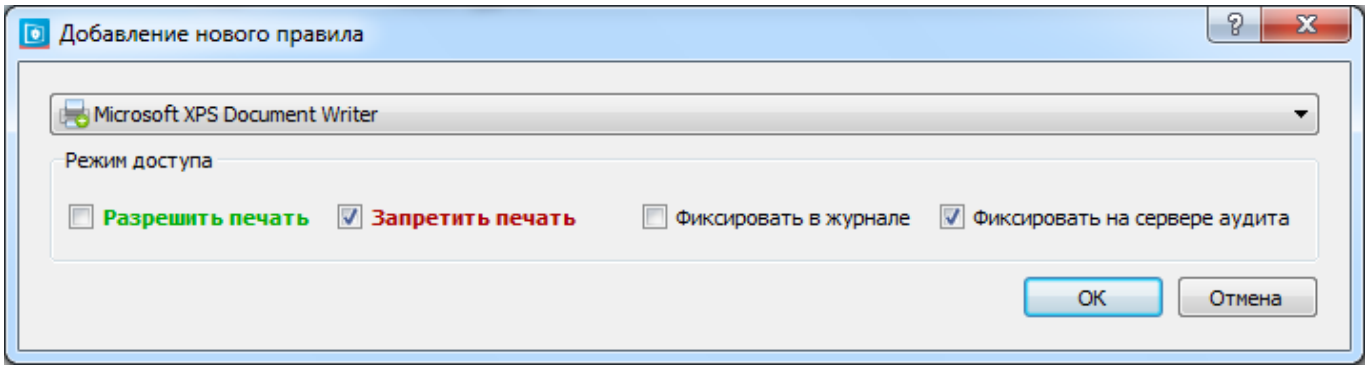


Рис.7.3.2.2. Окно добавления нового правила

1) Выбрать принтер из выпадающего списка.
2) Установить необходимые флаги «Разрешить печать» или «Запретить печать».
3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к принтерам» → «Правила доступа». Назначенные правила представлены в интерфейсе, в котором указаны тип объекта (пиктограмма), имя принтера, режим доступа и режим аудита.

После добавления правила разграничения доступа, правило отображается зеленым, если выбран режим доступа «Разрешить печать», и красным, если выбран режим доступа «Запретить печать».

Выделив правило левой кнопкой мыши, и, при наведении курсора на тип объекта, имя принтера или режим аудита, появится всплывающее окно с пояснением (рис.7.3.2.3).

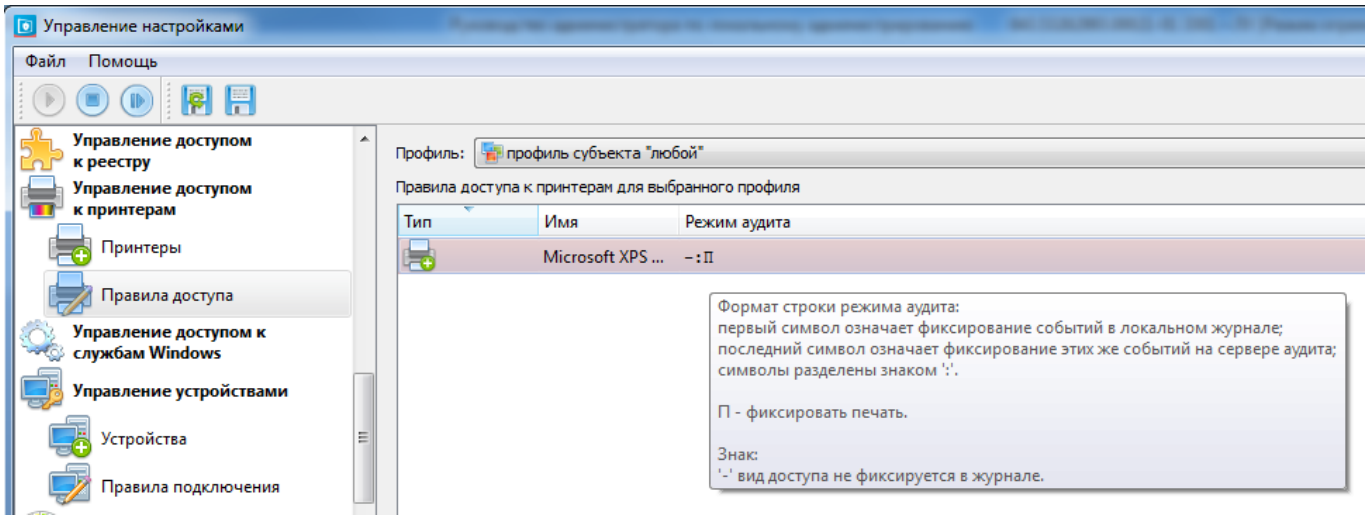


Рис.7.3.2.3. Интерфейс просмотра назначенных правил

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к принтерам».

Существует возможность **редактировать** назначенные правила. Для этого следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» и в контекстном меню выбрать «Редактировать правило», после чего внести необходимые изменения.

Для того чтобы **удалить** из списка правило доступа следует нажать правой кнопкой мыши по правилу и в контекстном меню выбрать «Удалить правило».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

7.4. МЕХАНИЗМ УПРАВЛЕНИЯ ДОСТУПОМ К БУФЕРУ ОБМЕНА. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Данный механизм защиты, предназначенный для реализации разграничительной политики доступа к буферу обмена ОС, реализуется по полной аналогии с механизмом контроля доступа к создаваемым файлам (файловым объектам), с естественной поправкой, определяемой физическим смыслом данного объекта. Механизмом защиты реализуется контроль доступа субъектов к буферу обмена при записи в него данных и разграничение доступа в соответствии с заданными правилами иных субъектов к данным, записанным определенным субъектом в буфер обмена.

По умолчанию разрешен доступ субъекту к данным, записанным им же в буфер обмена.

Учетная информация субъекта при контроле доступа к буферу обмена задается тремя сущностями: первичный идентификатор пользователя; эффективный идентификатор

пользователя; процесс. Эта информация запоминается диспетчером доступа СЗИ «ViPNet SafePoint», при записи данных в буфер обмена.

В данном механизме защиты в разграничительной политике доступа используются не профили, а именно субъекты доступа, определяемые соответствующими тремя сущностями, т.к. именно в этом случае достигается принципиальное упрощение задачи администрирования.

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к буферу обмена.

Основное назначение данного механизма контроля доступа – разграничение прав доступа между субъектами доступа к обрабатываемой на компьютере информации в дополнение к механизмам контроля доступа к файловым объектам. Может эффективно использоваться для реализации разграничительной политики доступа процессов к обрабатываемой на компьютере информации, в том числе, для реализации изолированных режимов обработки информации процессами (приложениями). Это может быть реализовано, как для защиты от несанкционированного доступа к информации процессов, наделяемых вредоносными свойствами, так и для защиты от хищения информации санкционированными пользователями (инсайдерами). Например, механизмом контроля доступа к создаваемым файлам почтовому клиенту может быть запрещен доступ к файлам, создаваемым на компьютере иными приложениями, а механизмом контроля доступа к буферу обмена – предотвращена возможность несанкционированного доступа почтовым клиентом к соответствующей информации через буфер обмена. При предотвращении доступа к сетевым ресурсам иными приложениями, решается задача защиты от хищения конфиденциальной информации санкционированным пользователем.

По умолчанию установлен флаг «Очищать буфер обмена, при изменении его содержимого непосредственно операционной системой», т.е. в случае, если установить субъект, создавший содержимое буфера обмена не удается, буфер обмена очищается. Примером являются снимки экрана, сделанные при помощи нажатия клавиши «Print Screen».

Для отключения автоматического очищения буфера обмена в описанных случаях необходимо убрать флаг «Очищать буфер обмена, при изменении его содержимого непосредственно операционной системой».

Интерфейс механизма представлен на рисунке 7.4.1.

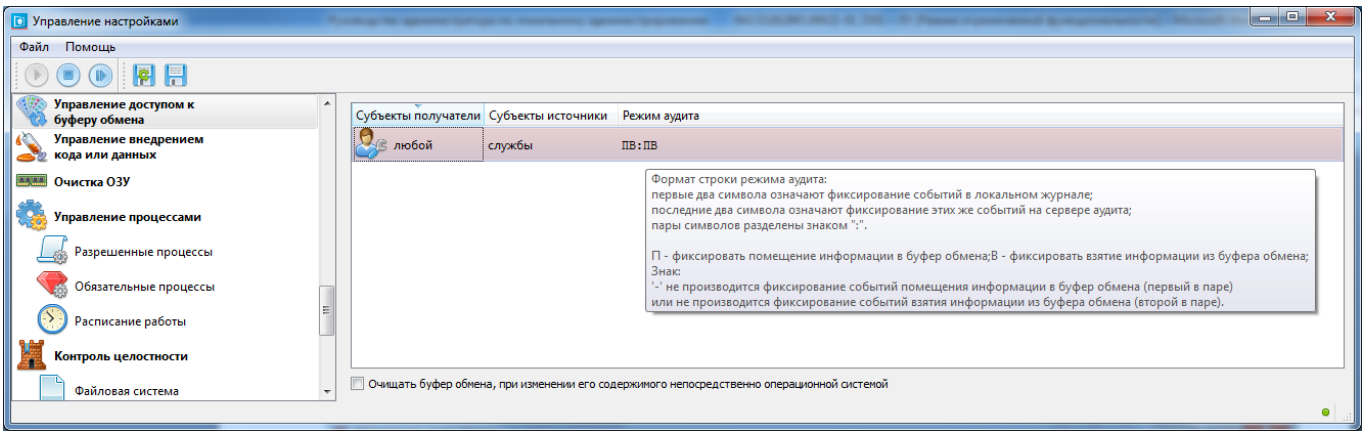


Рис.7.4.1. Интерфейс механизма управления доступом к буферу обмена

7.4.1. Назначение правил управления доступом к буферу обмена

Сначала необходимо завести субъектов доступа (см. раздел 6.2. Создание, изменение и удаление субъекта доступа), для которых в дальнейшем будут назначены правила управления доступом к буферу обмена.

Для назначения правил управления доступом к буферу обмена необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к буферу обмена».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Управление доступом к буферу обмена» и в контекстном меню (рис.7.4.1.1) выбрать «Добавить правило».

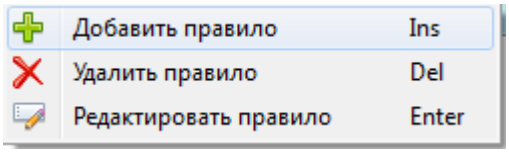


Рис.7.4.1.1. Контекстное меню окна «Управление доступом к буферу обмена»

3. В появившемся окне «Добавление нового правила» (рис.7.4.1.2) произвести следующие настройки:

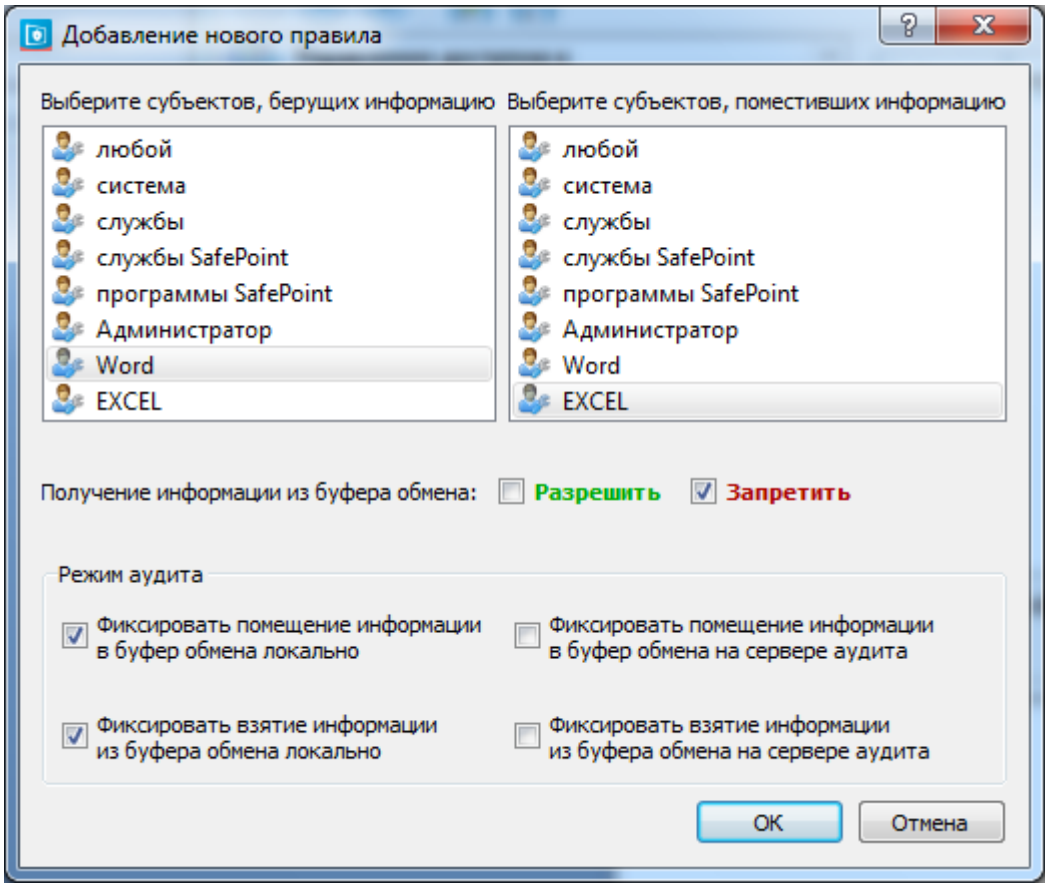


Рис.7.4.1.2. окно добавления нового правила

1) Выбрать субъектов, поместивших информацию в буфер обмена.
2) Выбрать субъектов, берущих информацию из буфера обмена.
3) Установить флаг «Запретить» или «Разрешить» для получения информации из буфера обмена.
4) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».
5. Установить или убрать флаг «Очищать буфер обмена, при изменении его содержимого непосредственно операционной системой» по необходимости.

Для **просмотра** назначенных правил управления доступом к буферу обмена необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к буферу обмена» (рис.7.4.1.3). В интерфейсе отражаются субъекты источники и субъекты получатели информации из буфера обмена и режим аудита.

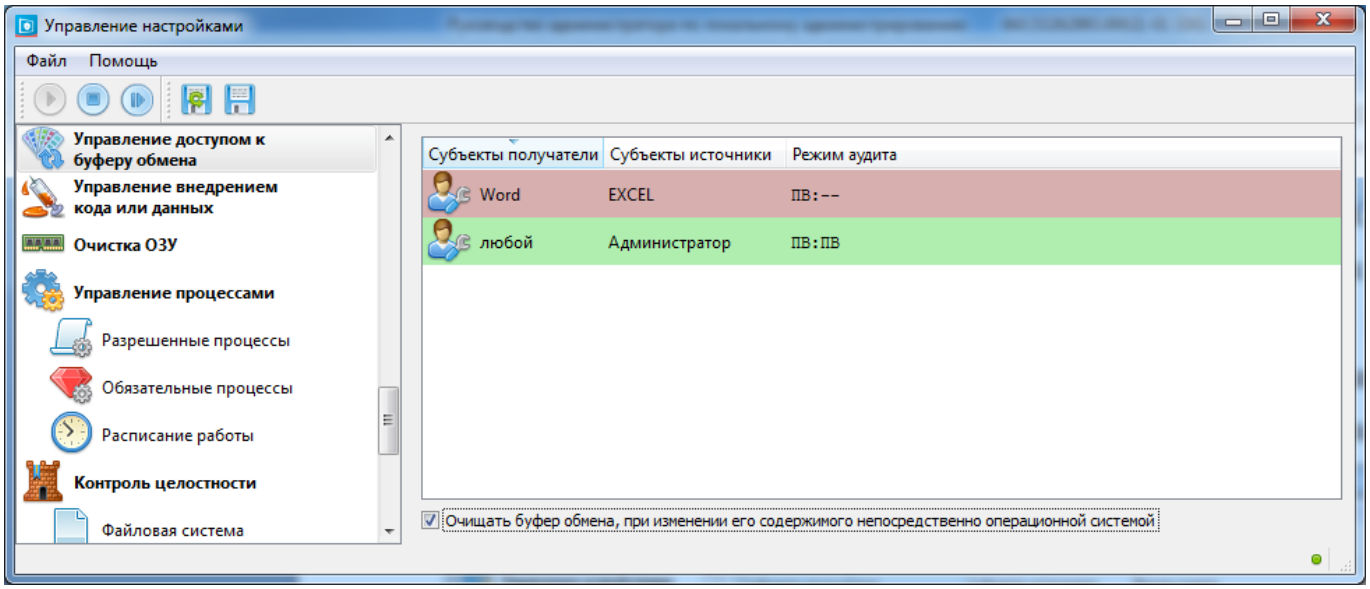


Рис.7.4.1.3. Просмотр назначенных правил управления доступом к буферу обмена

В интерфейсе разрешающие правила подсвечиваются зеленым, а запрещающие – красным.

Аналогично механизму управления доступом к создаваемым файлам (дискреционное управление доступом), правила могут быть заданы как для отдельных субъектов, так и для нескольких субъектов одновременно.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к буферу обмена».

Для **редактирования** назначенных правил следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление доступом к буферу обмена» (рис.9.2) и в контекстном меню выбрать «Изменить», внести нужные изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление доступом к буферу обмена» (рис.9.2) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

8. МЕХАНИЗМ ЗАЩИТЫ ОТ СКРЫТЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

8.1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Основу модели защиты СЗИ «ViPNet SafePoint» составляет реализация разграничительной политики доступа субъектов к ресурсам (либо между субъектами, при реализации контроля доступа к создаваемым файлам). При этом разграничительная политика доступа потенциально может быть обойдена злоумышленником при использовании ряда штатных возможностей, предоставляемых ОС.

В части защиты от скрытых действий пользователя, направленных на обход разграничительной политики доступа, в СЗИ «ViPNet SafePoint» реализованы контроль (разграничение прав) доступа к сервисам олицетворения (штатным сервисам ОС, позволяющим процессу возможность запросить у ОС и получить от нее право работы под другой учетной записью) и прямого доступа к дискам. Прямой доступ к дискам, опять же, штатная возможность ОС, позволяет получить доступ к хранимой на дисках (на жестком диске и внешних файловых накопителях) напрямую, а не как к файловым объектам, т.е. в обход заданной администратором разграничительной политики доступа к файловым объектам.

8.2. КОНТРОЛЬ ОЛИЦЕТВОРЕНИЯ. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Для идентификации контекста защиты процесса или потока в ОС используется объект, называемый маркером доступа (access token). В процессе регистрации в системе создается начальный маркер, представляющий пользователя, который входит в систему, и сопоставляет его с процессом оболочки, применяемой для регистрации пользователя.

Маркер может быть основным (идентифицирует контекст защиты процесса) или олицетворяющим (применяется для временного заимствования потоком другого контекста защиты — обычно другого пользователя). Олицетворение (impersonation) — средство, используемое в модели защиты Windows, предоставляющее возможность отдельному потоку выполняться в контексте защиты отличном от контекста защиты процесса, т.е. действовать от лица другого пользователя. Олицетворение, например, применяется в модели программирования «клиент-сервер».

Таким образом, ОС предоставляет санкционированную возможность запроса и получения процессом прав другого пользователя (смены учетной записи, от лица которой будет осуществлен доступ к ресурсу), что несет в себе реальную угрозу обхода разграничительной политики доступа. При использовании данной возможности пользователь (процесс) может запросить у системы права

другого пользователя, в результате чего, повысить своим привилегии, получив права системы, либо администратора.

В результате подобных действий злоумышленник может не только получить права другого пользователя, с которыми осуществить доступ к защищаемым ресурсам в обход разграничительной политики, но и, что еще хуже, получив права привилегированного пользователя воздействовать на СЗИ «ViPNet SafePoint», либо ОС (в рамках, предоставляемых этому пользователю прав СЗИ «ViPNet SafePoint» и/или ОС, например, с правами администратора).

Назначение данного механизма защиты – реализация контроля (разграничительной политики) доступа к сервисам олицетворения, реализующая защиту от повышения привилегий пользователя, за счет использования штатной возможности ОС.

В качестве субъекта доступа в разграничительной политике, реализуемой данным механизмом защиты, выступает процесс (могут использоваться, как полнопутевые имена, так и маски), для субъекта доступа (правила доступа назначаются субъектам) задается из какого в какое имя (учетные записи) субъекту разрешено/запрещено олицетворение (может быть реализована, как разрешительная, так и запретительные политики олицетворений для процессов).

Заданием соответствующего правила олицетворения, им одновременно предотвращается возможность запуска процесса (приложения) под другой учетной записью блокируется штатная возможность ОС по запуску процесса (приложения) с правами другого пользователя после прохождения соответствующей процедуры аутентификации. Например, используя утилиту runas.

Правила контроля олицетворения могут задаваться, как в отношении прикладных, так и в отношении системных процессов. В последнем случае могут быть реализованы дополнительные возможности защиты. *Например, запретом олицетворения системы с каким-либо пользователем для процесса winlogon, предотвращается возможность входа этого пользователя в систему.*

При реализации контроля доступа на основе меток безопасности для защиты обработки категорированной по уровням конфиденциальности информации, к повышению привилегий пользователя может быть в равной степени отнесено, как получение пользователем права обрабатывать информацию более высокого, чем заданный для него, уровня конфиденциальности (при этом пользователь получает запрещенный для него доступ к категорированной по соответствующему уровню конфиденциальности информации (по чтению), так и получение пользователем права обрабатывать информацию (по записи) более низкого, чем заданный для него, уровня конфиденциальности (при этом пользователь получает запрещенный для обработки информации данного уровня конфиденциальности режим обработки – доступ к ресурсам). При использовании контроля доступа на основе меток безопасности в данном случае должна предотвращаться возможность олицетворения с пользователем, имеющим любую отличающуюся метку безопасности, тем более с пользователем, для которого метка безопасности не установлена.

Окно интерфейса механизма управления олицетворением представлено на рис.8.2.1. В окне отображаются информация о правиле олицетворения: имя процесса, имя пользователя, из которого происходит олицетворение, имя пользователя, в которого происходит олицетворение, режим аудита.

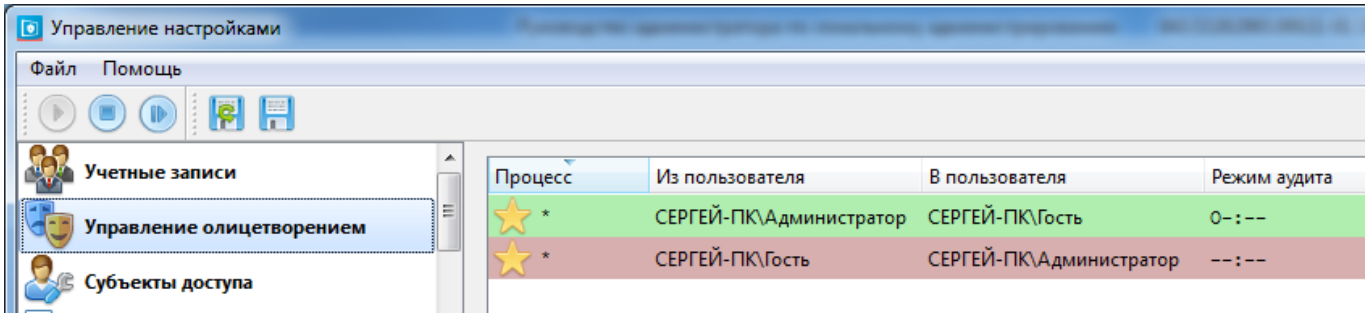


Рис.8.2.1. Интерфейс механизма управления олицетворением

Для назначения нового правила олицетворения следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление олицетворением».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Управление олицетворением» и в контекстном меню (рис.8.2.2) выбрать «Добавить правило».

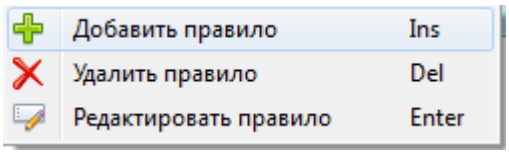


Рис.8.2.2. Контекстное меню окна «Управление олицетворением»

3. В появившемся окне «Добавление нового правила» (рис.8.2.3) произвести следующие настройки:

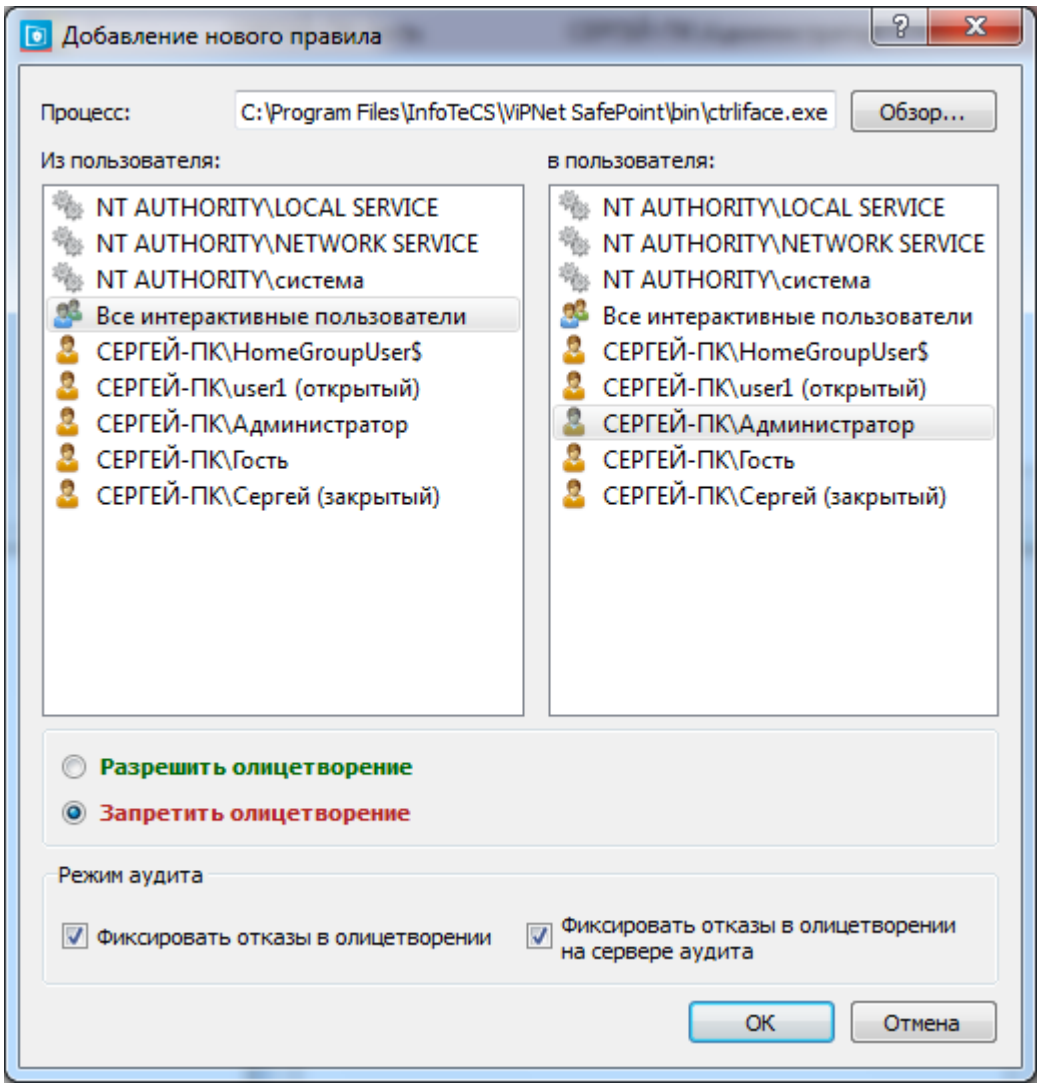


Рис.8.2.3. Окно добавления нового правила

1) Задать процесс, используя «Обзор» или задать вручную. Возможно использование масок.

2) Выбрать из списка пользователя, из которого осуществляется олицетворение. Есть возможность выбрать нескольких пользователей путем одновременного нажатия клавиш «Ctrl» и левой кнопки мыши.

Для удобства администрирования, если пользователю назначен уровень доступа, он отображается в скобках после имени пользователя. Аналогичным образом уровни доступа отражаются во всех механизмах, в которых разграничения доступа назначаются для пользователей.

3) Выбрать из списка пользователя, в которого осуществляется олицетворение. Есть возможность выбрать нескольких пользователей путем одновременного нажатия клавиш «Ctrl» и левой кнопки мыши.

Невозможно разрешить или запретить олицетворение пользователя в самого себя.

В списках пользователей «Из пользователя» и «В пользователя» присутствует сущность «**Все интерактивные пользователи**», она включает в себя пользователей системы, за исключением системных пользователей. Данная сущность введена для назначения правил контроля олицетворения для всех пользователей, кроме системных, одновременно.

4) Выбрать флаг «Разрешить олицетворение» или «Запретить олицетворение».

5) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».

Зеленым цветом в интерфейсе отображается правило, разрешающее олицетворение. Красным отображается запрет олицетворения.

Для **просмотра** назначенных правил олицетворения необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление олицетворением» (рис.8.2.4). В интерфейсе отражается процесс, имена пользователей, для которых запрещено или разрешено олицетворение, и режим аудита.

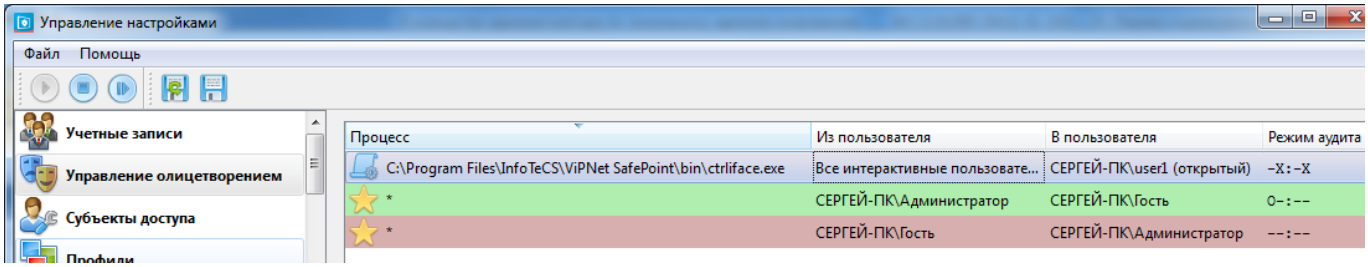


Рис.8.2.4. Просмотр назначенных правил олицетворения

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления олицетворением».

Для **редактирования** назначенных правил следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление олицетворением» (рис.8.2.2) и в контекстном меню выбрать «Изменить», внести нужные изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление олицетворением» (рис.8.2.2) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

8.3. КОНТРОЛЬ ПРЯМОГО ДОСТУПА К ДИСКАМ. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Данный механизм защиты, предназначенный для реализации разграничительной политики прямого доступа к дискам, в отношении, как жесткого диска, так и внешних накопителей, реализуется по полной аналогии с механизмами контроля доступа к файловым накопителям, при этом объект доступа - устройство (включая жесткий диск) задается в разграничительной политике доступа идентификатором модели устройства, либо конкретного устройства (с учетом его серийного номера).

Реализация контроля (разграничения прав) прямого доступа к дискам предполагает реализацию дискреционного контроля доступа (на основе матрицы доступа) с принудительным управлением потоками информации. Правила доступа задаются для субъектов (а не назначаются в качестве атрибутов доступа объектам - дискам).

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к дискам.

Разграничительная политика реализуется для профилей.

Назначение данного механизма защиты – реализация контроля (разграничительной политики) прямого доступа к дискам (как к жесткому диску (дискам), так внешним файловым накопителям), который может быть использован злоумышленником для обхода разграничительной политики доступа к файловым объектам.

Окно интерфейса механизма «Управление прямым доступом к дискам» представлено на рис.8.3.1. Данные механизм следует настраивать последовательно, сначала задать устройства, далее правила доступа.

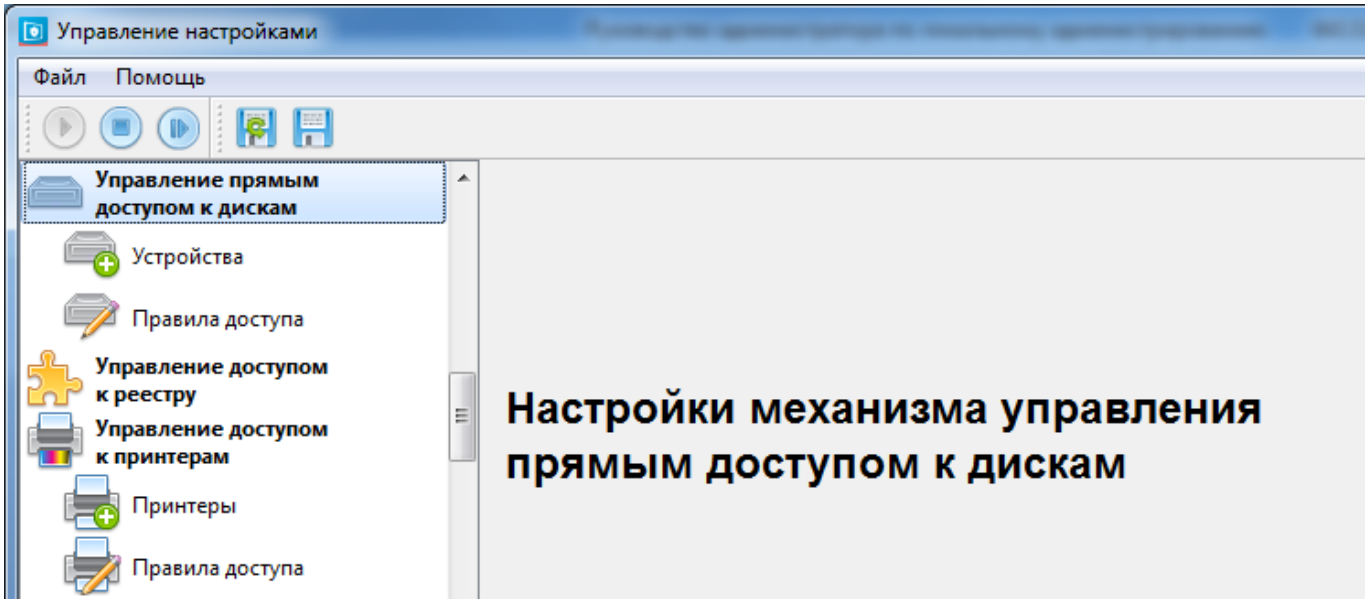


Рис.8.3.1. Интерфейс настройки механизма «Управление прямым доступом к дискам»

С учетом возможности использования масок, одновременно несколько устройств, заведенных в СЗИ «ViPNet SafePoint», могут соответствовать реальному устройству, к которому запрашивается доступ. Для выбора правила доступа введен следующий приоритет обработки устройств, заданных в СЗИ «ViPNet SafePoint»: конкретное уникальное устройство, модель устройств (группы устройств), маска. Заданные в СЗИ «ViPNet SafePoint» устройства сравниваются с реальными объектами в заданном порядке обработки (конкретное уникальное устройство, модель устройств (группы устройств), маска) и выбирается правило доступа для первого из подошедших устройств.

В СЗИ «ViPNet SafePoint» тип устройства (конкретное уникальное устройство, модель устройств (группы устройств), маска) задается автоматически, но при реализации конкретной разграничительной политики, пользователь может установить тип устройства вручную, для изменения порядка его обработки (сравнения объекта, заведенного в СЗИ «ViPNet SafePoint», с реальным объектом, к которому запрашивается доступ).

Для настройки механизма управления прямым доступом к дискам, сначала необходимо задать устройство:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление прямым доступом к дискам» → «Устройства».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Устройства» в контекстном меню (рис.8.3.2) выбрать «Добавить объект».

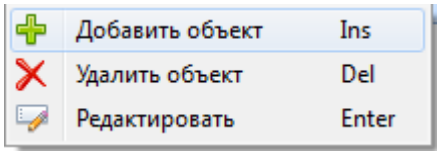


Рис.8.3.2. Контекстное меню окна «Устройства»

3. В появившемся окне «Создание нового объекта» (рис.8.3.3) произведите следующие настройки:

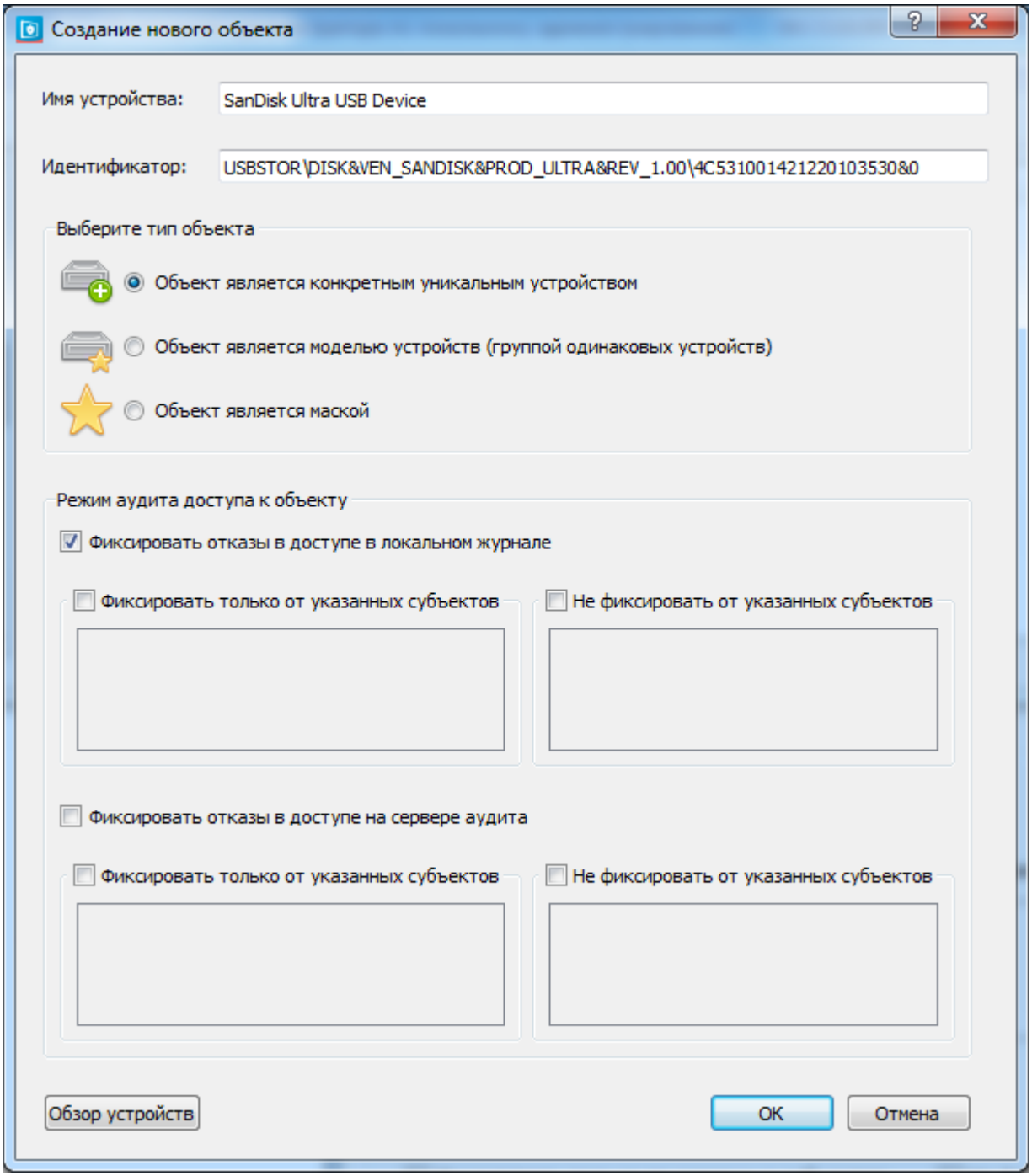


Рис.8.3.3. Окно создания нового объекта

1) Задать с помощью «Обзора устройств» или вручную «Имя устройства» и «Идентификатор».
2) Выбрать тип объекта или оставить автоматически установленный тип.
3) Настроить режим аудита (см. раздел 15.2.2 Аудит доступа к объектам).
4. Нажать кнопку «ОК».

Для **просмотра** заведенных в СЗИ «ViPNet SafePoint» устройств необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление прямым

доступом к дискам» → «Устройства» (рис.8.3.4). В интерфейсе указывается тип (пиктограмма) устройства, его имя и режим аудита.

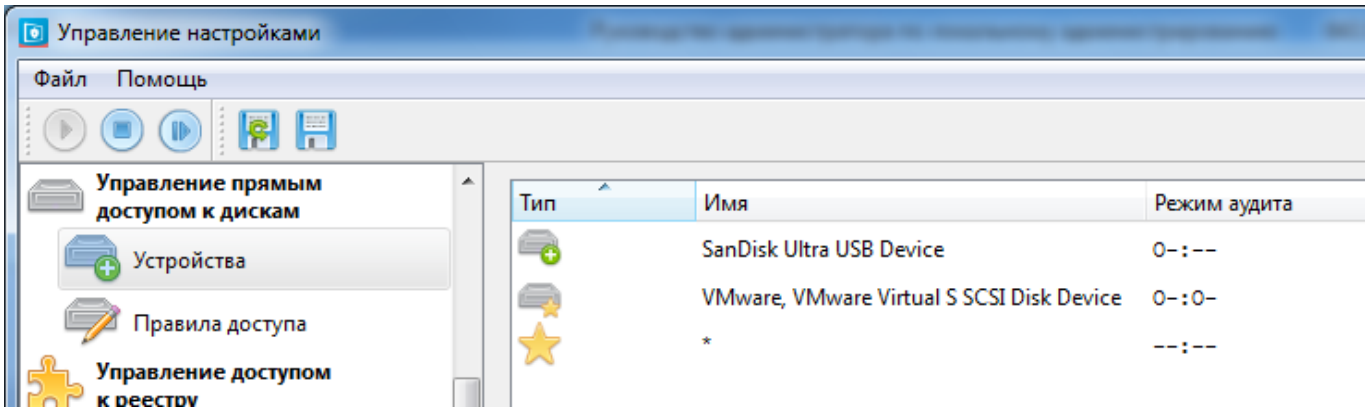


Рис.8.3.4. Интерфейс просмотра заведенных устройств

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления прямым доступом к дискам».

Для **редактирования** уже созданных устройств следует нажать правой кнопкой мыши по правилу в интерфейсе «Устройства» (рис.8.3.2) и в контекстном меню выбрать «Изменить», внести нужные изменения и внести нужные изменения.

Для **удаления** объектов доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Устройства» (рис.8.3.2) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

Правила прямого доступа назначаются для профилей. Для назначения правил прямого доступа необходимо:

1. В «Меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление прямым доступом к дискам» → «Правила доступа».
2. Выбрать профиль, для которого будут назначены правила.
3. Нажать по пустой области интерфейса «Правила доступа» и в контекстном меню (рис.8.3.5) выбрать «Добавить правило».

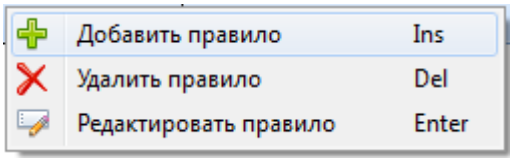


Рис.8.3.5. Контекстное меню окна «Правила доступа»

4. В появившемся окне «Добавление нового правила» (рис.8.3.6) произвести следующие настройки:

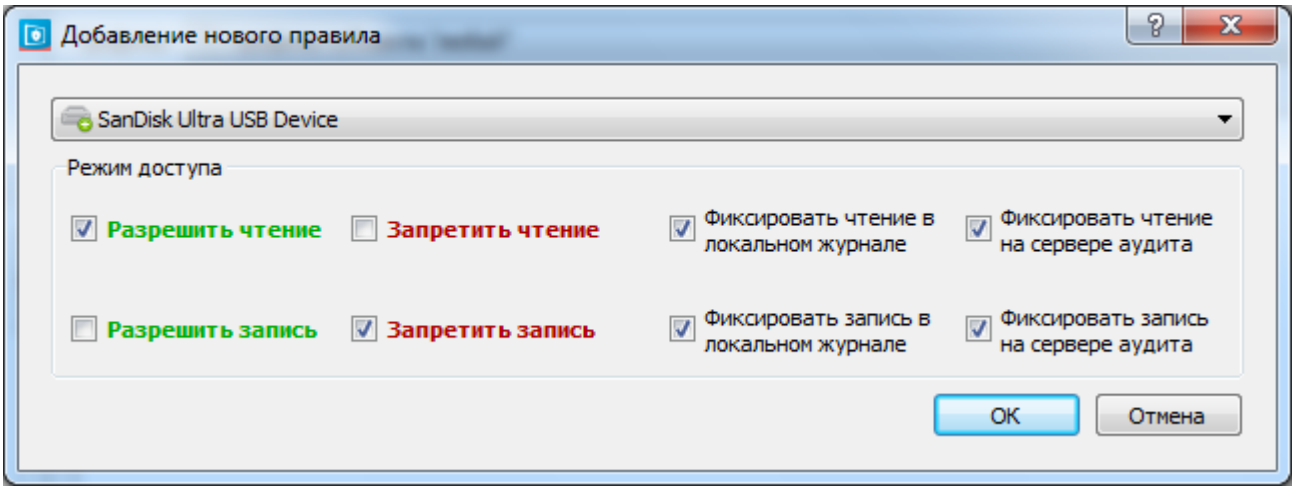


Рис.8.3.6. Окно добавления нового правила

1) Выбрать из выпадающего списка объект.
2) Установить необходимые флаги «Разрешить» или «Запретить» на чтение, и запись.
3) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил прямого доступа к дискам необходимо в «Меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление прямым доступом к дискам» → «Правила доступа» (рис.8.3.7). В интерфейсе указывается тип (пиктограмма), имя объекта (дискового устройства), режим доступа и режим аудита.

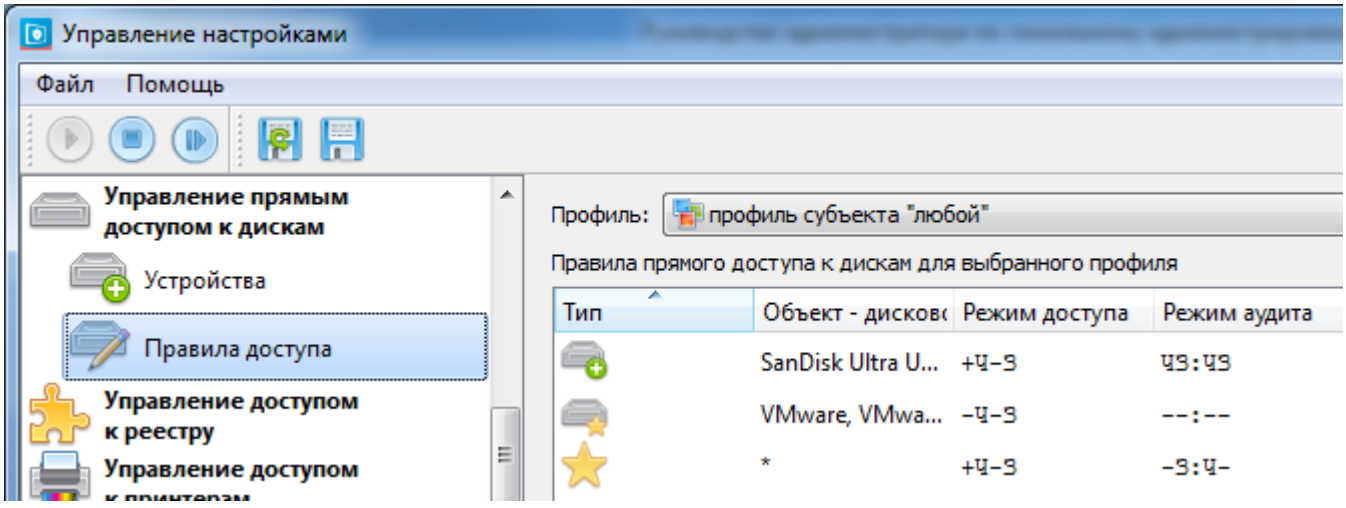


Рис.8.3.7. Интерфейс просмотра назначенных правил

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления прямым доступом к дискам».

Для **редактирования** назначенных правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» (рис.8.3.7) и в контекстном меню выбрать «Изменить», внести нужные изменения и внести нужные изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Правила доступа» (рис.8.3.7) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

9. МЕХАНИЗМ УПРАВЛЕНИЯ МОНТИРОВАНИЕМ УСТРОЙСТВ. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ. ИНТЕРФЕЙС

Механизм управления монтированием устройств в модели защиты СЗИ «ViPNet SafePoint» имеет крайне важное значение. Основу СЗИ «ViPNet SafePoint» составляет реализация разграничительной политики доступа к ресурсам, механизм же управления монтированием устройств позволяет локализовать необходимые, как для использования в информационной системе в целом, так и для использования отдельными пользователями, либо в отдельных сессиях – режимах обработки информации, устройства.

Кроме того, данный механизм защиты служит для исключения возможности монтирования устройств, использование которых, по каким-либо причинам, несет в себе угрозу несанкционированного доступа к информации (например, смартфоны, не являющиеся файловыми накопителями ОС Microsoft Windows).

Данный механизм защиты в обязательном порядке должен быть настроен при построении эффективной защиты информационной системы.

Особенностью реализации данного механизма управления монтированием устройств в СЗИ «ViPNet SafePoint» является следующее:

- механизм позволяет не только разрешать монтировать к системе (подключать) устройства в соответствии с заданными правилами в процессе функционирования информационной системы, но может и отмонтировать от системы (отключать) устройства, при определенных условиях, заданных соответствующими правилами;
- несмотря на то, что монтирование устройств осуществляется к системе, возможность монтирования (необходимость отмонтирования) устройств определяется работающими в системе пользователями (учетными записями). Как следствие, в качестве субъектов доступа, в отношении которых разрешается/запрещается использование устройств, может выступать не только система, но и отдельные пользователи (учетные записи);
- устройства могут задаваться с учетом их серийных номеров (конкретные устройства).

Существует несколько идентификаторов устройств:

- идентификатор тома, присваиваемый при форматировании, хранящийся в секторе на устройстве;
- идентификатор, присваиваемый ОС для сопоставления с буквой диска, хранится в реестре ОС;
- идентификатор, прошиваемый в устройство производителем (не изменяется).

Механизм управления монтированием устройств в СЗИ «ViPNet SafePoint» использует идентификатор, прошиваемый в устройство производителем.

При управлении монтированием устройств может быть реализована, как разрешительная «Все, что явно не разрешено – явно не указано, то запрещено», так и запретительная «Все, что явно не запрещено – явно не указано, то разрешено».

При этом в отношении каждого устройства, для которого задаются правила монтирования/отмонтирования, могут задаваться пользователи (учетные записи), при активности которых в информационной системе (осуществили локальный или удаленный вход на компьютер), устройство разрешается подключать, либо должно быть принудительно (средствами СЗИ «ViPNet SafePoint») отключено от системы. При нарушении задаваемого правила монтирования устройств в отношении какого-либо устройства, механизмом защиты предотвращается возможность его монтирования к системе, либо, соответственно, устройство принудительно отмонтируется от системы (например, если в систему вошел пользователь, для которого использование соответствующего устройства запрещено).

Не все устройства могут автоматически монтироваться к системе и отмонтироваться от системы в процессе ее функционирования по соответствующей команде СЗИ «ViPNet SafePoint» (без перезагрузки компьютера). Прежде чем реализовать ту или иную разграничительную политику, проверьте возможность монтирования/отмонтирования интересующих вас устройств в процессе работы системы.

Если устройство невозможно отмонтировать для интерактивного пользователя по соответствующей команде СЗИ «ViPNet SafePoint», то оно будет отображаться с пометкой . Данные устройства могут быть отключены только для системы и после перезагрузки операционной системы.

Если устройство невозможно отмонтировать для интерактивного пользователя по соответствующей команде СЗИ «ViPNet SafePoint» (отображаться с пометкой), но существует необходимость настройки возможности монтирования такого устройства, необходимо проверить, возможно, данное устройство монтируется также как устройство иного класса, для которого возможно монирование/отмонтирование по соответствующей команде, в таком случае правила монтирования могут быть назначены для этого же устройства, отображаемого в другом классе.

Выбор окна интерфейса механизма «Управление устройствами» представлен на рис.9.

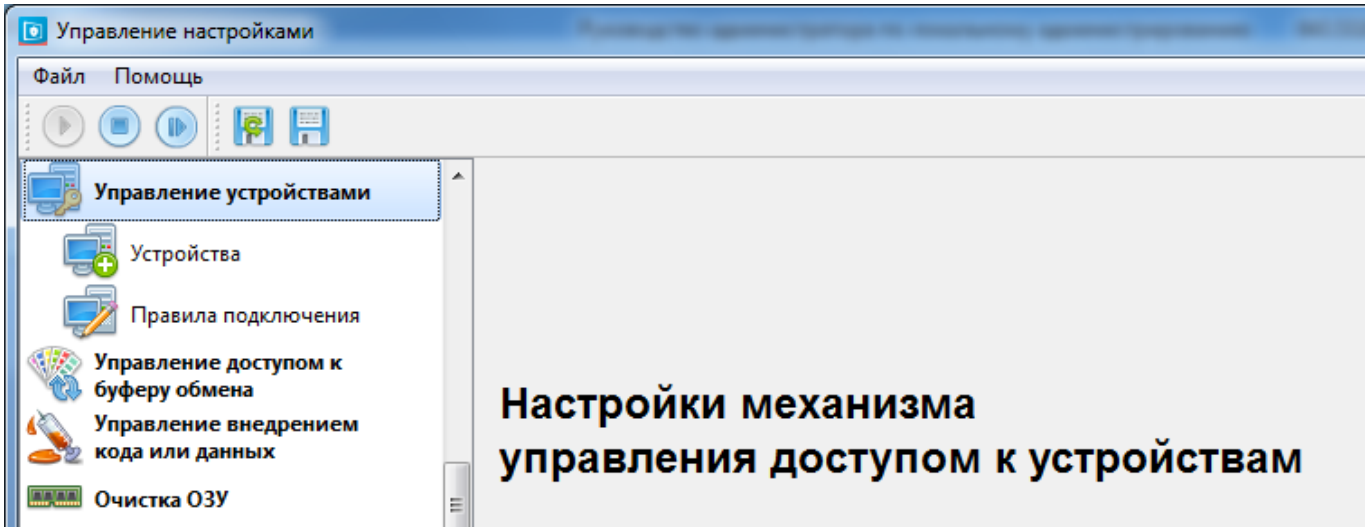


Рис.9. Интерфейс механизма управления доступом к устройствам

Данный механизм следует настраивать последовательно, сначала задать устройства, далее правила их подключения.

9.1. УСТРОЙСТВА

При настройке механизма монтирования устройств необходимо задать устройства, к которым далее будут применены правила подключения. Для внесения устройства в отображаемый список устройств необходимо подключить устройство к системе. Далее убедиться (средствами ОС), что в данный момент устройство подключено. Определить класс устройства, для которого далее будут назначены правила подключения. Список устройств запрашивается драйвером у операционной системы и выдается в виде, в котором его предоставляет ОС.

Для отображения списка устройств и классов устройств, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление устройствами» → «Устройства».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Устройства» или по имени машины и в контекстном меню (рис.9.1.1) выбрать «Обновить список классов».

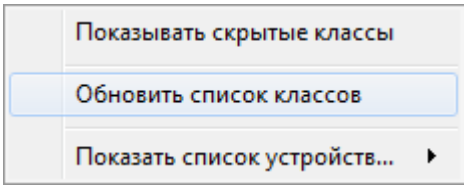


Рис.9.1.1. Контекстное меню окна «Устройства»

По умолчанию отображаются только основные классы устройств и скрыты некоторые дополнительные классы. Для просмотра всех классов устройств в контекстном меню необходимо выбрать пункт «Показывать скрытые классы».

3. Установить флаг напротив класса устройств или устройства, для которых будут назначены правила подключения.
4. В меню верхней панели интерфейса СЗИ «ViPNet SafePoint» выбрать «Файл» → «Сохранить настройки», либо воспользоваться меню сохранения и загрузки предыдущих настроек.
5. Перезагрузить систему, оставив устройства подключенными.
6. В контекстном меню (рис.9.1.2) выбрать показать список устройств из файла конфигурации.

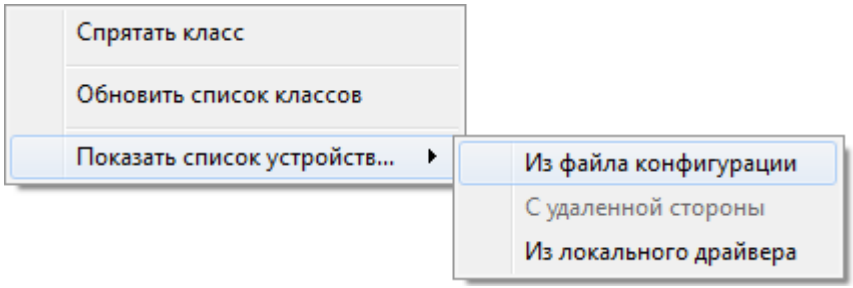


Рис.9.1.2. Контекстное меню окна «Устройства»

Файл конфигурации отражает все устройства, выбранных классов, которые были подключены перед перезагрузкой системы. Устройства автоматически добавляются в файл конфигурации.

Устройства, которые были только подключены, считаются новыми и отображаются в файле конфигурации с пометкой NEW. После перезагрузки операционной системы данная пометка исчезнет.

Список устройств из локального драйвера отображает все устройства, подключенные к локальной машине.

Есть возможность не отображать определенные классы устройств. Для этого следует нажать правой кнопкой мыши по названию класса и в контекстном меню выбрать «Спрятать класс». Далее нажать правой кнопкой мыши по имени компьютера и выбрать показать или не показывать скрытые классы.

Для просмотра списка устройств и классов устройств необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление устройствами» → «Устройства» (рис.9.1.3). При наведении курсора на устройство, появится всплывающее окно с данными об этом устройстве.

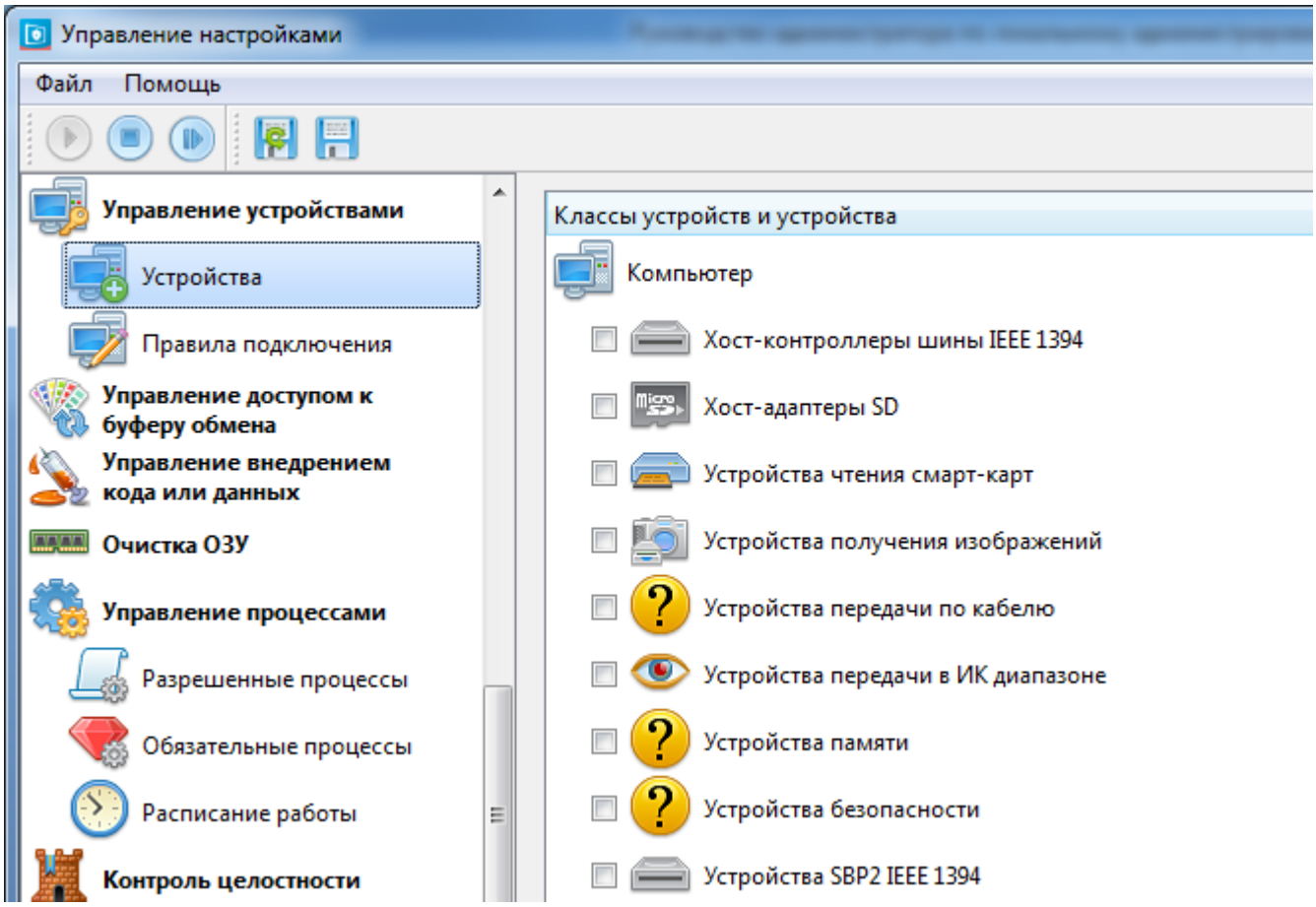


Рис.9.1.3. Интерфейс просмотра списка устройств и классов устройств

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

9.2. ПРАВИЛА ПОДКЛЮЧЕНИЯ

Правила подключения назначаются для пользователей относительно устройств или классов устройств.

Для назначения правил подключения устройств или классов устройств необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление устройствами» → «Правила подключения».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Правила подключения» и в контекстном меню (рис.9.2.1) выбрать «Добавить правило».

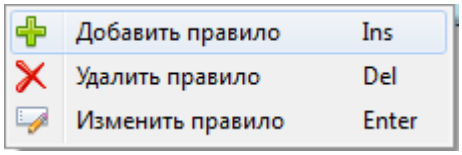


Рис.9.2.1. Контекстное меню окна «Правила подключения»

3. В появившемся окне «Добавить правило» (рис.9.2.2) произвести следующие настройки:

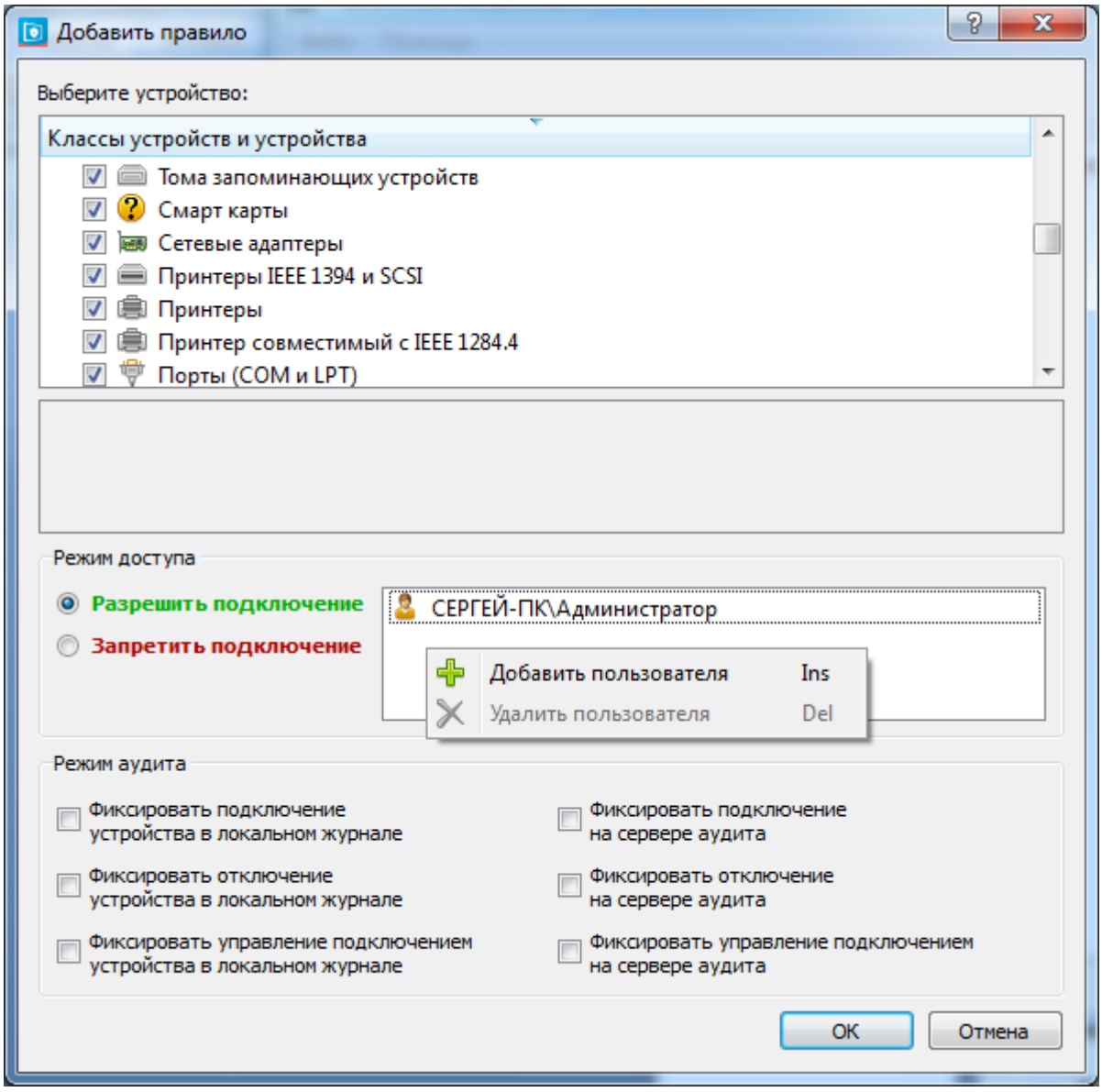


Рис.9.2.2. Окно добавления правила разграничения

1) Выбрать устройство или класс устройств.
2) Выбрать «Разрешающий» или «Запрещающий» режим доступа подключения.

Если устанавливается разрешающий/запрещающий режим монтирования устройств без указания пользователей, то разграничения действуют для всех пользователей и вступают в силу после сохранения настроек. При указании конкретных пользователей, правила вступают в силу после входа одного из указанных пользователей в систему.

3) Для назначения правила подключения для определенных пользователей, необходимо:

- нажать правой кнопкой мыши по пустой области окна «Режим доступа»;
- во всплывающем окне выбрать строку «Добавить пользователя»;
- выбрать пользователей для добавления в список (рис.9.2.3), для удобства администрирования, заданные уровни доступа отображаются в скобках после имен пользователей;

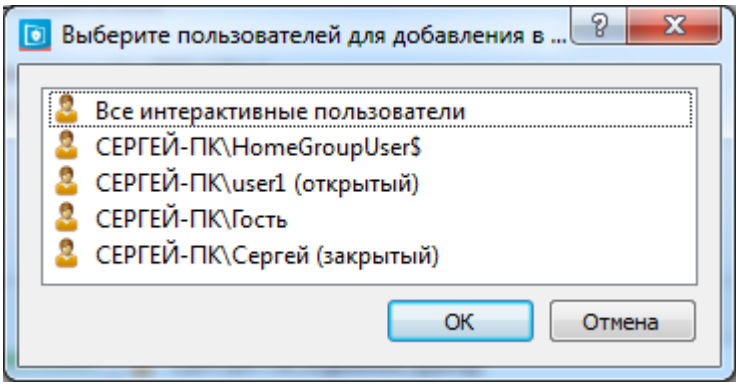


Рис.9.2.3. Выбор пользователей для добавления в список

В списке пользователей присутствует сущность «**Все интерактивные пользователи**», она включает в себя пользователей системы, за исключением системных пользователей. Данная сущность введена для назначения правил монтирования устройств для всех пользователей, кроме системных, одновременно.

- нажать кнопку «ОК».

4) Настроить режим аудита (см. раздел 15.2.3 Аудит действий субъектов доступа).

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил подключения устройств или классов устройств необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление устройствами» → «Правила подключения» (рис.9.2.4). Назначенные правила представлены в интерфейсе, в котором указаны: объект (пиктограмма), режим доступа и режим аудита. Выделив правило левой кнопкой мыши, и, при наведении курсора на режим аудита, появится всплывающее окно с пояснением.

В интерфейсе зеленым цветом подсвечиваются правила, разрешающие монтирование устройств, а красным – запрещающие монтирование устройств.

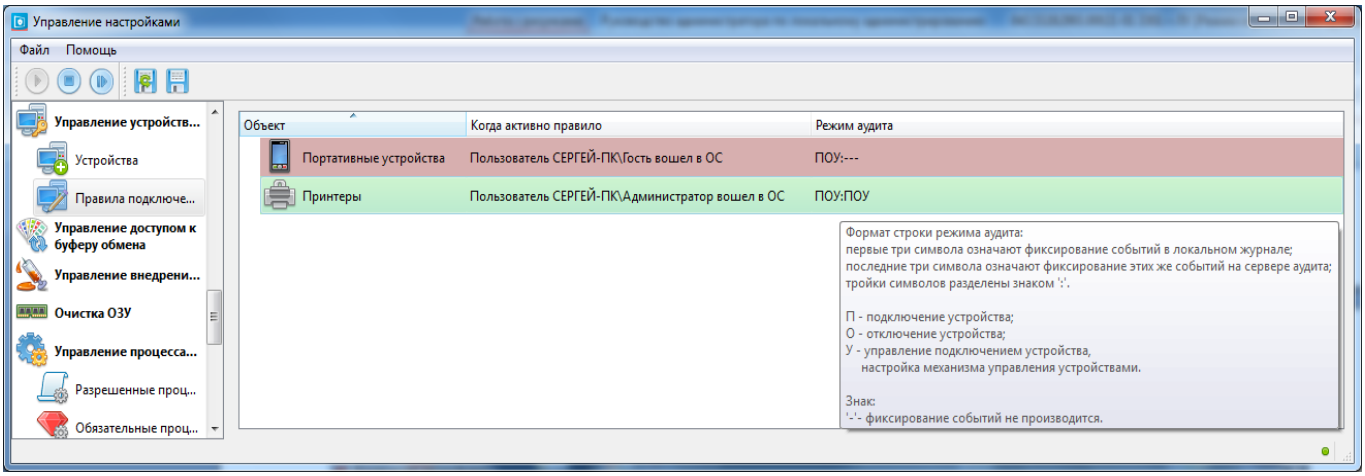


Рис.9.2.4. Интерфейс просмотра правил подключения устройств или классов устройств

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления подключением устройств».

Для **редактирования** или **удаления** правила подключения необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление устройствами» → «Правила подключения», далее воспользоваться контекстным меню окна (рис.9.2.1), для удаления или внесения необходимых изменений в правило.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

При назначении правил для класса устройств и для конкретных устройств данного класса необходимо либо назначить правила для каждого пользователя (рис.9.2.5), либо использовать для смены пользователей функцию «Выйти из системы» («Пуск» → «Завершение работы» → «Выйти из системы») и дальнейший вход другим пользователем.

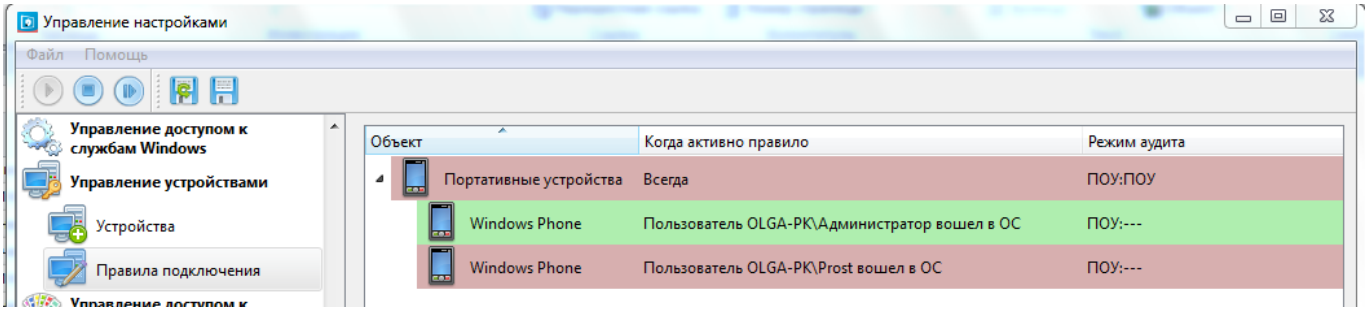


Рис.9.2.5. Интерфейс просмотра правил подключения классов и устройств

9.3. КОНТРОЛЬ УСТРОЙСТВ

В СЗИ "ViPNet SafePoint" при помощи механизма «Управление устройствами» возможно реализовать контроль аппаратной конфигурации как в части системных устройств, так и в части подключаемых устройств. При этом, в качестве реакции на события подключения/отключения

устройств, может быть настроен аудит реального времени (т.е. отправка сообщений на сервер аудита) и локальный аудит, отображающие как санкционированное подключение устройств, так и попытки подключения неразрешенных устройств.

Для реализации данной возможности необходимо задать разрешающие правила по монтированию санкционированных устройств и, если другие устройства данного класса не разрешены для применения, задать запрещающее правило монтирования для всего класса устройств.

На рисунке 9.3.1 приведен пример такой настройки механизма управления монтированием устройств для дисковых устройств.

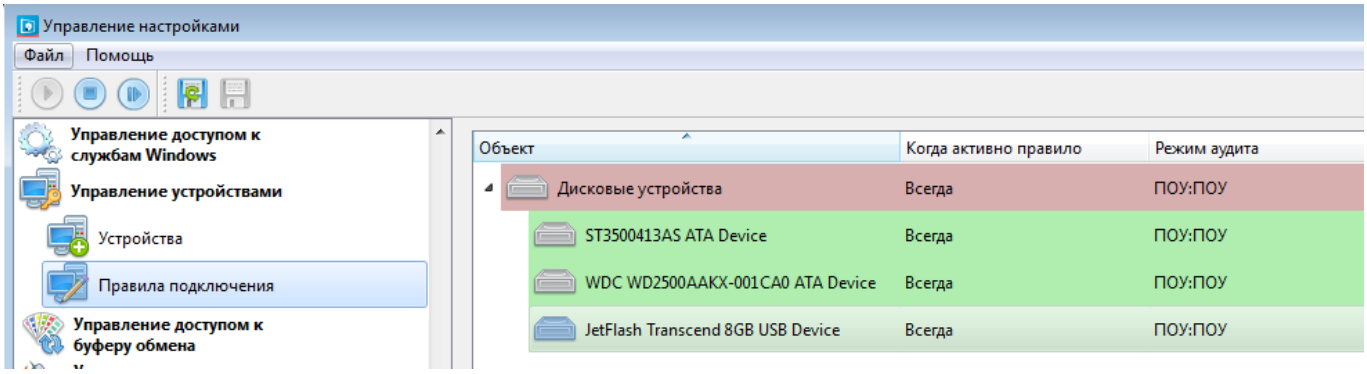


Рис.9.3.1. Пример реализации контроля аппаратной конфигурации в отношении дисковых устройств

10. МЕХАНИЗМЫ КОНТРОЛЯ

10.1. НАЗНАЧЕНИЕ, СОСТАВ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Модель защиты СЗИ «ViPNet SafePoint» основана на реализации разграничительной политики доступа субъектов к защищаемым ресурсам. Реализация данного контроля (разграничительной политики) направлена на предотвращение несанкционированного доступа к информации, с целью нарушения ее конфиденциальности, обеспечения целостности и доступности. В части обеспечения доступности информации в СЗИ «ViPNet SafePoint» решается задача защиты от несанкционированного удаления/модификации системных объектов (файловых объектов и объектов реестра ОС).

При этом на практике всегда остается потенциальная возможность скрытых действий злоумышленника, направленных на обход реализованной разграничительной политики доступа к ресурсам. Для защиты от подобных действий злоумышленника в СЗИ «ViPNet SafePoint» реализован ряд дополнительных механизмов защиты, опять же основанных на контроле доступа (например, контроль доступа к сервисам олицетворения, прямого доступа к дискам).

Вместе с тем, все эти меры не могут на 100% гарантировать невозможность обхода реализованной разграничительной политики доступа к ресурсам, ввиду многообразия и невозможности полного предсказания всех скрытых действий злоумышленника. Критичным в данном случае является и то, что, поскольку доступ к ресурсу будет реализован в рамках реализованной разграничительной политики (в противном случае, он будет признан механизмами контроля доступа к ресурсам несанкционированным и будет предотвращен), факт подобного несанкционированного доступа не будет даже зарегистрирован в журнале аудита событий.

В качестве дополнительной защиты от скрытых действий злоумышленника, направленных на обход разграничительной политики доступа к ресурсам, в модели защиты СЗИ «ViPNet SafePoint» предусмотрена реализация двух групп механизмов контроля – контроля процессов и контроля целостности.

Принципиальной особенностью реализации данных групп механизмов контроля является то, что они реализуют синхронный (по расписанию) контроль фактов уже свершившихся событий (не анализируют запросы, приводящие к свершению событий, а анализируются свершившиеся события в системе). Защита реализована на ином уровне и иными средствами, нежели механизмы контроля доступа к ресурсам, что позволяет выявлять скрытые действия злоумышленника, позволившие ему реализовать обход разграничительной политики доступа к ресурсам.

Важным для механизмов контроля является оперативная (естественно, зависящая от периода проведения процедуры контроля) реакция на выявленное несанкционированное событие. В СЗИ «ViPNet SafePoint», кроме регистрации выявленного несанкционированного события,

предусмотрена возможность задания администратором соответствующей реакции, предотвращающей в системе подобное событие.

В рамках контроля процессов в СЗИ «ViPNet SafePoint» реализованы следующие механизмы защиты:

- контроль запуска разрешенных процессов (задаваемых, либо списком полнопутевых имен процессов – их исполняемых файлов, разрешенных к запуску в системе, либо списком папок, из которых могут выполняться разрешенные к запуску процессы, также могут использоваться маски). В качестве реакции на обнаружение запуска в системе несанкционированного процесса, администратор может задать его принудительное завершение средствами СЗИ «ViPNet SafePoint»;
- контроль запуска обязательных процессов (задаваемых их полнопутевыми именами – исполняемыми файлами). Администратор имеет возможность задать процессы, которые в обязательном порядке должны быть активными в системе, в частности, это процессы, реализующие функции защиты информации, в том числе, сторонних производителей. В качестве реакции на обнаружение несанкционированного удаления в системе обязательного процесса, администратор может задать его принудительные запуск, причем от лица требуемой учетной записи, в том числе, от лица системы;
- контроль запуска приложений (задаваемых их полнопутевыми именами – исполняемыми файлами, каталогами (папками), масками) по расписанию. Это важнейший механизм контроля, направленный на временную регламентацию работы пользователей в информационной системе. Для любого приложения администратор может указать дни недели и/или интервалы времени, в которые данное приложение может быть активным в системе. При указании, с какого времени – приложение не сможет быть запущено до этого времени, при указании до какого времени – приложение при наступлении данного момента времени будет принудительно завершено СЗИ «ViPNet SafePoint». Администратор может регламентировать работу пользователей не только с любыми приложениями, но и с системными процессами, что позволяет реализовать некоторые дополнительные функции защиты. Например, при задании соответствующего временного интервала для системного процесса winlogon, обеспечивается возможность доступа к системе по расписанию – пользователи смогут войти в систему только с указанного момента времени, соответственно, система будет активной только до указанного момента времени, после чего работа системы будет принудительно завершена. Таким образом, в качестве реакции на обнаружение несанкционированного использования приложения, по отношению к

заданным временным интервалам, в СЗИ «ViPNet SafePoint» установлено принудительное завершение подобного процесса.

В рамках обеспечения контроля целостности в СЗИ «ViPNet SafePoint» реализованы следующие механизмы защиты:

- контроль целостности файловых объектов (задаваемых их полнопутевыми именами – именами файлов или каталогов, в отношении файлов которых будет производиться контроль). В первую очередь данный механизм защиты предназначен для обеспечения целостности системных файловых объектов, в том числе, может быть использован для синхронного контроля файловых объектов СЗИ «ViPNet SafePoint». Однако подобный контроль администратор может реализовать и в отношении любого файлового объекта, не предназначенного для модификации в системе. Для постановки файлового объекта на контроль администратор средствами СЗИ «ViPNet SafePoint» формирует контрольные суммы контролируемых файлов. При назначении контрольных сумм для каталогов, СЗИ «ViPNet SafePoint» создаются контрольные суммы всех файлов, содержащихся в контролируемом каталоге, а также запоминаются имена всех файлов в контролируемом каталоге. В качестве реакции на обнаружение несанкционированное изменение контролируемого файлового объекта, администратором может быть задано его автоматическое восстановление СЗИ «ViPNet SafePoint» из резервной копии. С этой целью администратором предварительно средствами СЗИ «ViPNet SafePoint» должны быть созданы резервные копии контролируемых файлов. В случае, если в качестве контролируемого файлового объекта администратором указывается каталог, то создаются резервные копии всех файлов из данного каталога. Файл при этом в контролируемом каталоге автоматически восстанавливается не только в случае его несанкционированной модификации, но и в случае его несанкционированного удаления или переименования;
- контроль целостности объектов реестра ОС (задаваемых их полнопутевыми именами – именами ключей или ветвей, в отношении ключей которых будет производиться контроль). В том числе, данный механизм защиты может быть использован для синхронного контроля объектов реестра, используемых СЗИ «ViPNet SafePoint». Для постановки объектов реестра ОС на контроль администратор средствами СЗИ «ViPNet SafePoint» формирует контрольные суммы контролируемых ключей реестра. При назначении контроль сумм для ветвей реестра, СЗИ «ViPNet SafePoint» создаются контрольные суммы всех ключей, а также запоминаются имена всех ключей в контролируемой ветви. В качестве реакции на обнаружение несанкционированное изменение контролируемого ключа реестра, администратором может быть задано его автоматическое восстановление СЗИ «ViPNet

SafePoint» из резервной копии. С этой целью администратором предварительно средствами СЗИ «ViPNet SafePoint» должны быть созданы резервные копии контролируемых ключей реестра ОС. В случае если в качестве контролируемого объекта реестра ОС администратором указывается ветвь, то создаются резервные копии всех ключей из данной ветви. Ключ при этом в контролируемой ветви автоматически восстанавливается не только в случае его несанкционированной модификации, но и в случае его несанкционированного удаления или переименования;

- контроль целостности объектов СЗИ «ViPNet SafePoint». Контроль целостности объектов СЗИ «ViPNet SafePoint» – файловых объектов с системными файлами и файлами настроек СЗИ, а также важнейших объектов реестра ОС, используемых СЗИ «ViPNet SafePoint», реализован в СЗИ «ViPNet SafePoint» автоматически (не требует каких-либо настроек). Контроль осуществляется при каждом старте службы СЗИ «ViPNet SafePoint», в том числе, осуществляемом при загрузке системы, и синхронно – с периодом 10 минут (при необходимости увеличить частоту контроля, можно воспользоваться механизмами контроля, рассмотренными выше). Реакцией на несанкционированные действия в отношении контролируемых событий, установленной в СЗИ «ViPNet SafePoint» по умолчанию, является автоматическое восстановление несакнционированно измененных контролируемых объектов СЗИ «ViPNet SafePoint» из резервной копии. Резервные копии исполняемых объектов СЗИ «ViPNet SafePoint» создаются автоматически, резервные копии настроек СЗИ «ViPNet SafePoint» – при их сохранении, при задании или модификации из интерфейса СЗИ «ViPNet SafePoint» (модифицировать настройки не из интерфейса СЗИ «ViPNet SafePoint» не допустимо – при старте службы будут восстановлены исходные настройки, произведенные ранее из интерфейса). Все несанкционированные события, связанные с нарушением целостности СЗИ «ViPNet SafePoint» и ее восстановлением, фиксируются в соответствующем журнале аудита.

Механизмы контроля целостности объектов файловой системы и объектов реестра ОС могут быть весьма ресурсозатратными, при частом (небольшом установленном периоде) контроле большого объема объектов – могут оказывать большую дополнительную нагрузку на вычислительные ресурсы. Перед использованием данных механизмов контроля целесообразно оценить влияние задаваемой администратором политики контроля на загрузку вычислительного ресурса информационной системы.

10.2. КОНТРОЛЬ САНКЦИОНИРОВАННОСТИ ЗАПУСКА ПРОЦЕССОВ. ИНТЕРФЕЙС

Выбор окна интерфейса механизма «Управления процессами» представлен на рис.10.2.1. В основном окне можно включить или отключить механизмы контроля разрешенных процессов, контроля обязательных процессов, механизм расписания работы процессов.

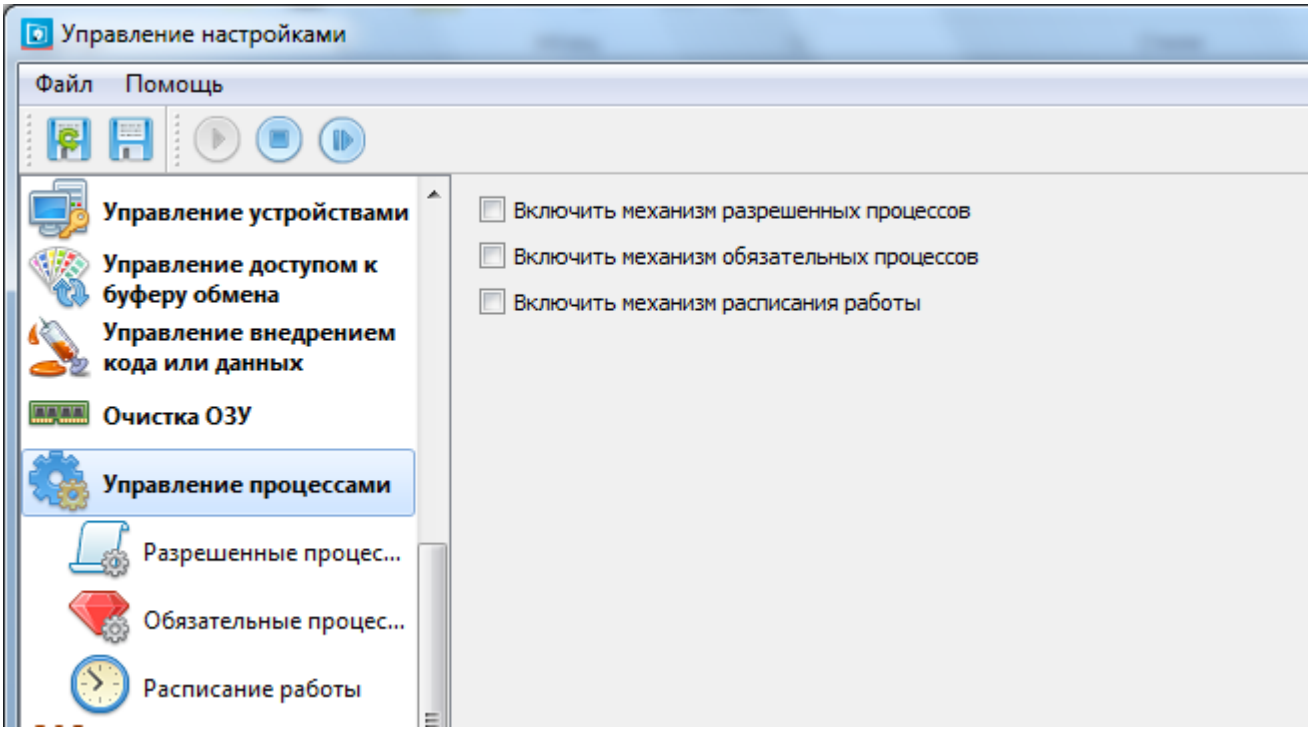


Рис.10.2.1. Интерфейс механизма «Управление процессами»

Для включения настроенных механизмов требуется в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» и установить флаги напротив необходимых для включения механизмов.

10.2.1. Разрешённые процессы (программы)

В СЗИ «ViPNet SafePoint» по умолчанию заведен список разрешенных системных процессов, заданных с использованием переменных среды окружения. Это процессы из системных каталогов запущенной операционной системы.

По умолчанию в СЗИ «ViPNet SafePoint» заведены разрешенные системные процессы. При включении данного механизма, эти процессы в обязательном порядке должны быть в списке разрешенных процессов. В противном случае система не сможет корректно функционировать.

Для создания нового разрешенного процесса следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» → «Разрешенные процессы».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Разрешенные процессы» и в контекстном меню выбрать «Добавить процесс» (рис.10.2.1.1).

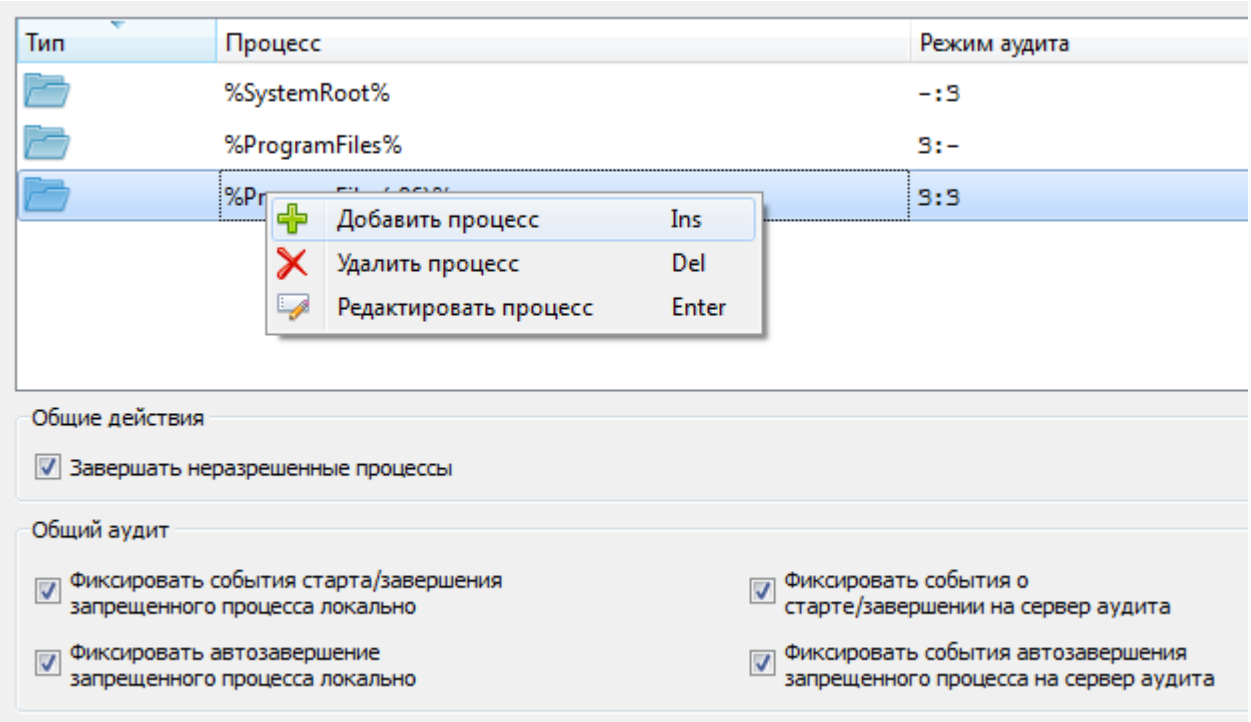


Рис.10.2.1.1. Интерфейс окна разрешенных процессов и его контекстное меню

3. В появившемся окне «Добавление нового разрешенного процесса» (рис.10.2.1.2) произвести следующие настройки:

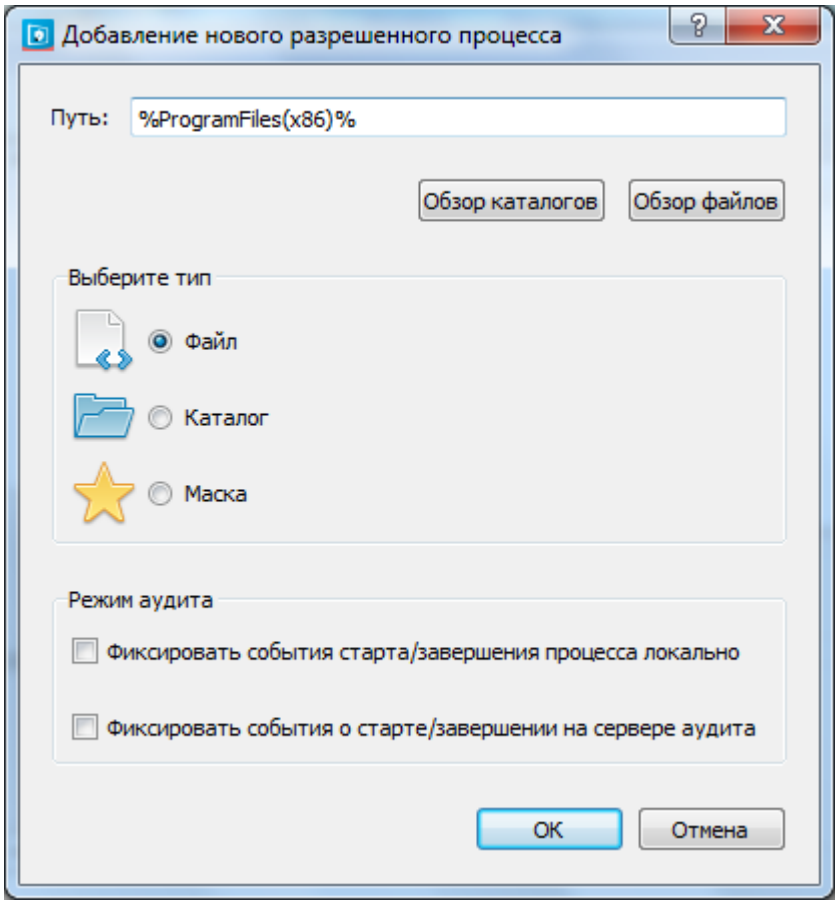


Рис.10.2.1.2. Окно добавления нового разрешенного процесса

1) Задать путь нового разрешенного процесса, используя «Обзор каталогов» либо «Обзор файлов» в зависимости от выбранного типа или задать путь вручную. Возможно использование масок файлов и переменных среды окружения.
2) Выбрать необходимый тип или оставить автоматически назначенный СЗИ «ViPNet SafePoint».
3) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».

Далее настроить общие действия и режимы общего аудита. Для этого необходимо:

1. В интерфейсе (рис.10.2.1.1) установить, при необходимости, флаг «Завершать неразрешенные процессы».
2. В интерфейсе (рис.10.2.1.1.) настроить режимы общего аудита (см. раздел 15.2.4. Аудит событий).

Просмотр разрешенных процессов осуществляется в окне интерфейса механизма «Управления процессами» (рис.10.2.1.3). В интерфейсе отражены: тип (пиктограмма), имя процесса, режим аудита. Так же в окне интерфейса можно просмотреть выставленные флаги общих действий и общего аудита.

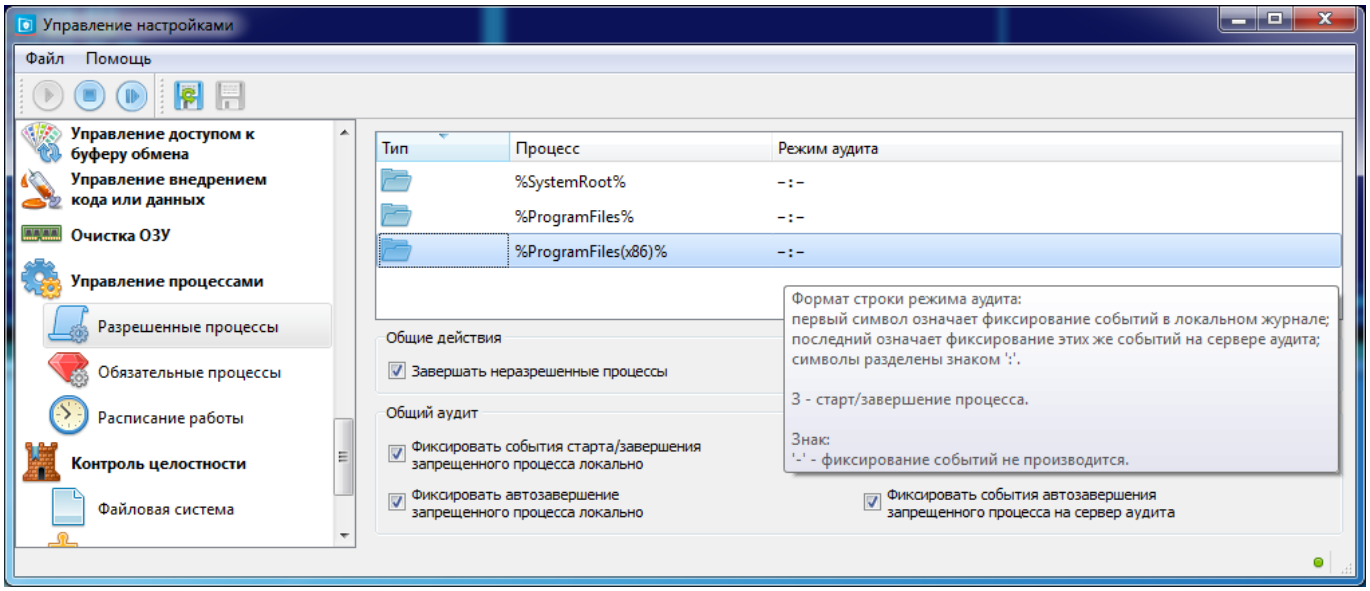


Рис.10.2.1.3. Просмотр разрешенных процессов

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления процессами».

Для **редактирования** уже созданных разрешенных процессов следует нажать правой кнопкой мыши по процессу в интерфейсе «Разрешенные процессы» (рис.10.2.1.3) и в контекстном меню выбрать «Изменить», затем внести нужные изменения.

Для **удаления** разрешенных процессов и списка следует нажать правой кнопкой мыши по процессу в интерфейсе «Разрешенные процессы» (рис.10.2.1.3) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

10.2.2. Обязательные процессы (программы)

Обязательные для выполнения процессы должны указываться их полнопутевыми именами.

В список обязательных процессов системные процессы включать не обязательно.

Для создания нового обязательного процесса, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» → «Обязательные процессы».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Обязательные процессы».
3. В контекстном меню (рис.10.2.2.1) выбрать «Добавить правило».

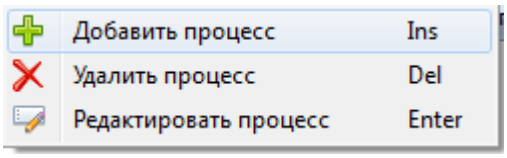


Рис.10.2.2.1. Контекстное меню окна «Обязательные процессы»

4. В появившемся окне «Добавление нового обязательного процесса» (рис.10.2.2.2) произвести следующие настройки:

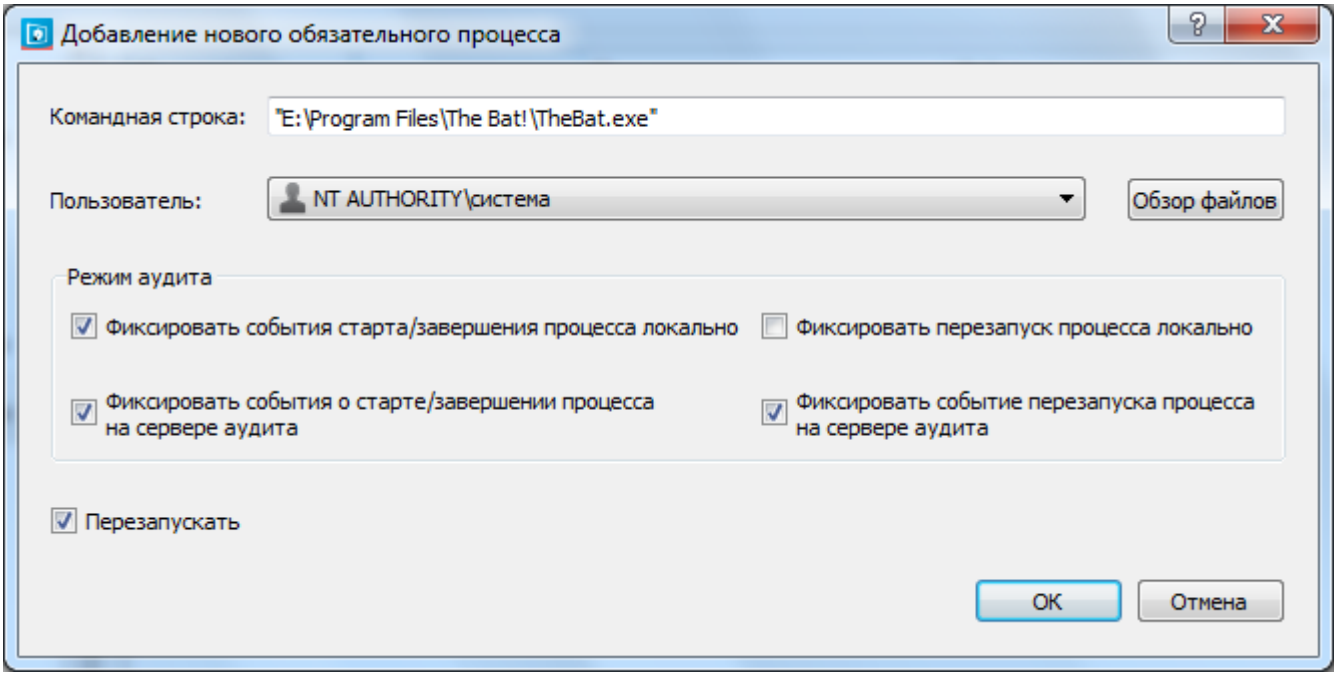


Рис.10.2.2.2. Окно добавления нового обязательного процесса

1) Задать путь исполняемого файла процесса в «Командную строку», используя «Обзор файлов» или задать путь вручную.
2) Выбрать пользователя из выпадающего списка**.**
3) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

5. Нажать кнопку «ОК».

Список пользователей будет пустым, если в меню «Учетные записи» не заведен ни один пользователь.

Для **просмотра** заведенных обязательных процессов необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» → «Обязательные процессы» (рис.10.2.2.3). В интерфейсе отражается: имя процесса, пользователь, для которого запуск процесса обязателен, и действие (перезапуск) и режим аудита.

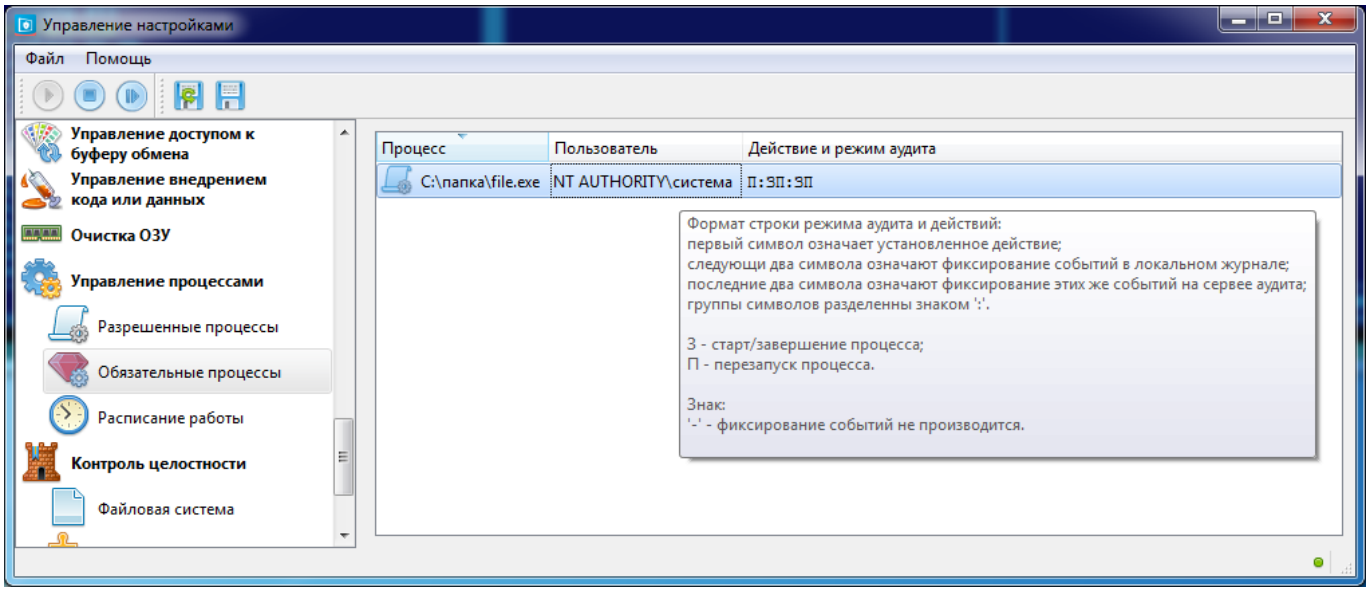


Рис.10.2.2.3. Интерфейс просмотра обязательных процессов

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления процессами».

Для **редактирования** уже созданных обязательных процессов следует нажать правой кнопкой мыши по процессу в интерфейсе «Обязательные процессы» (рис.10.2.2.3) и в контекстном меню выбрать «Изменить», затем внести нужные изменения.

Для **удаления** обязательных процессов следует нажать правой кнопкой мыши по процессу в интерфейсе «Обязательные процессы» (рис.10.2.2.3) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

10.2.3. Расписание работы процессов (программ)

Для создания расписания работы процесса, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» → «Расписание работы».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Расписание работы».
3. В контекстном меню (рис.10.2.3.1) выбрать «Добавить процесс».

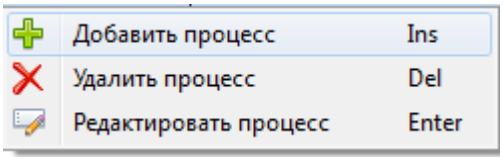


Рис.10.2.3.1. Контекстное меню окна «Расписание работы»

4. В появившемся окне «Создание расписания работы процесса» (рис.10.2.3.2) произвести следующие настройки:

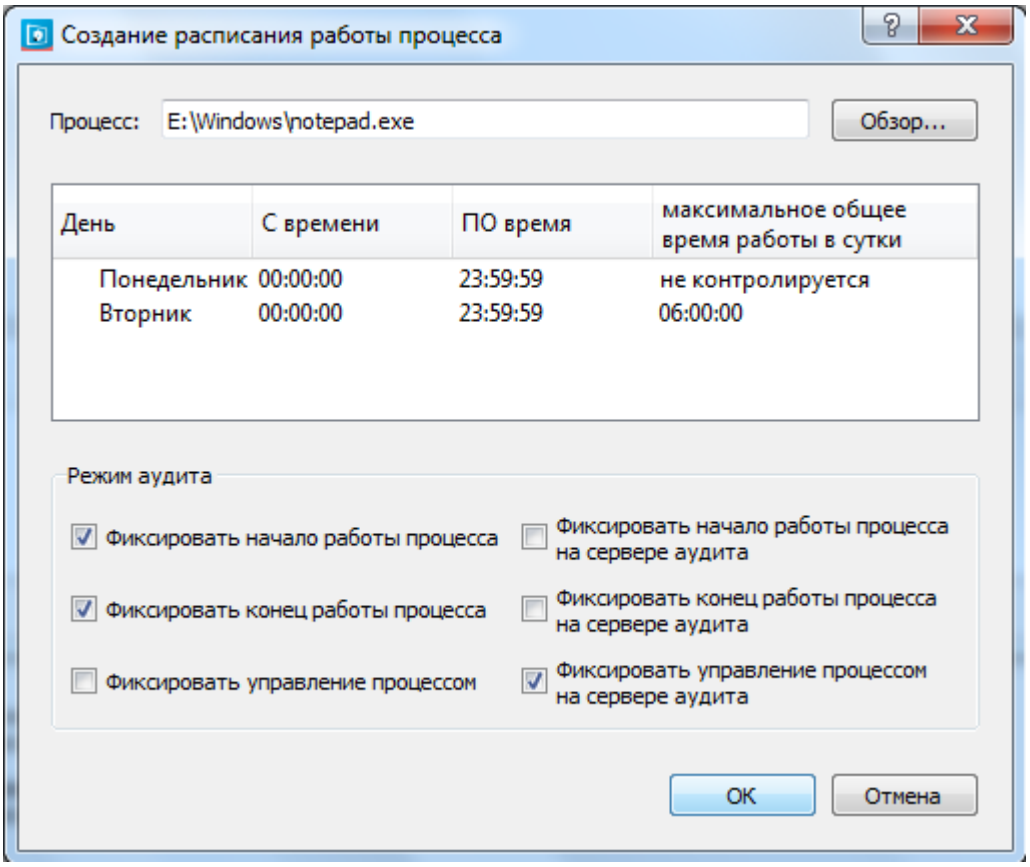


Рис.10.2.3.2. Окно создания расписания работы процесса и его контекстное меню

1) Задать имя исполняемого файла процесса, используя «Обзор» или задать путь вручную. Возможно использование масок.
2) Нажать правой кнопкой мыши по пустой области интерфейса «Создание расписания работы процесса».
3) В контекстном меню выбрать «Добавить/Изменить».
4) В появившемся окне «Редактирование элемента расписания» (рис.10.2.3.3) произвести следующие настройки:

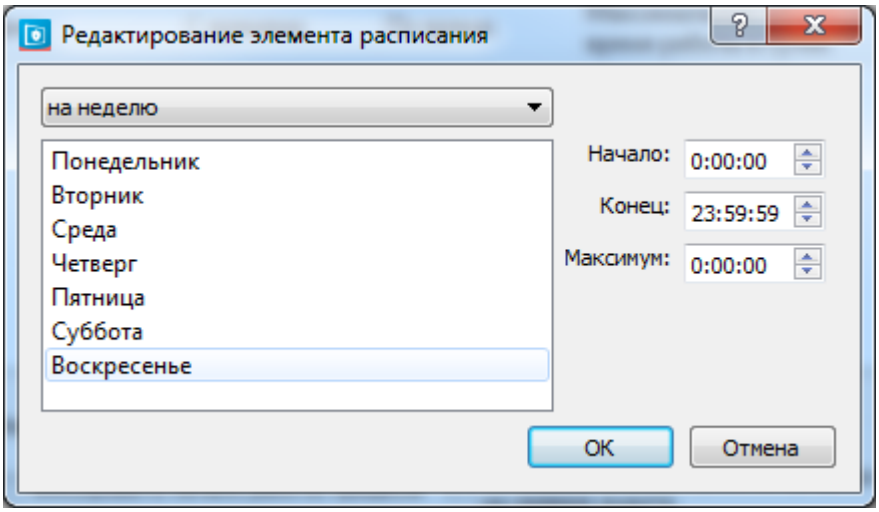


Рис.10.2.3.3. Окно редактирования элемента расписания

- выбрать в выпадающем списке период времени расписания работы процесса «на неделю» или «на месяц»;
- выбрать день (дни) недели;
- установить «Начало» работы процесса;
- установить «Конец» работы процесса;
- установить «Максимум», максимальное общее время работы процесса в сутки;
- нажать кнопку «ОК».

5) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

5. Нажать кнопку «ОК».

Для **просмотра** расписания работы процессов необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление процессами» → «Расписание работы» (рис.10.2.3.4).

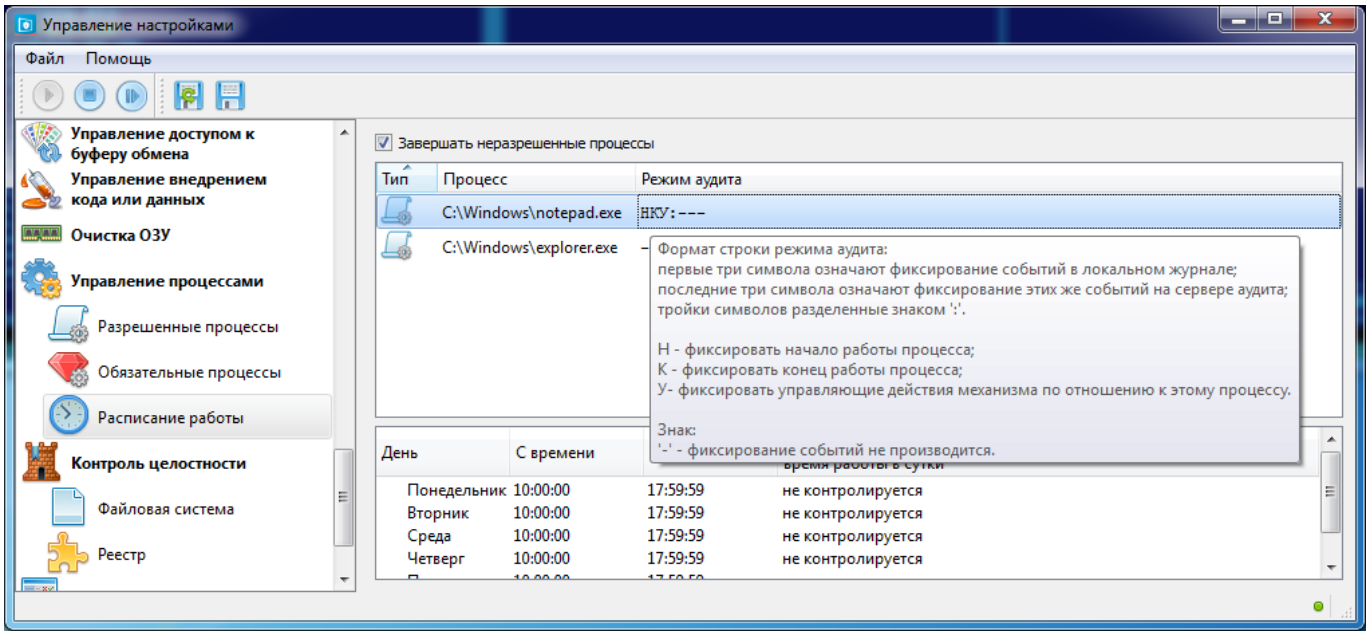


Рис.10.2.3.4. Интерфейс просмотра расписания работы процессов

В СЗИ «ViPNet SafePoint» есть возможность завершать неразрешенные процессы, для включения этого механизма необходимо установить соответствующий флаг в интерфейсе (рис.10.2.3.4). В интерфейсе отражаются тип (пиктограмма), имя процесса, режим аудита. Выделив процесс, в нижней части окна отразится назначенное для него расписание работы (день недели, интервал времени работы, максимальное общее время работы в сутки).

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления процессами».

Для **редактирования** уже созданного расписания работы следует нажать правой кнопкой мыши по процессу в интерфейсе «Расписание работы» (рис.10.2.3.4) и в контекстном меню выбрать «Изменить», затем внести нужные изменения.

Для **удаления** расписания работы следует нажать правой кнопкой мыши по процессу в интерфейсе «Расписание работы» (рис.10.2.3.4) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

10.3. КОНТРОЛЬ ЦЕЛОСТНОСТИ

Основное окно интерфейса механизма контроля целостности объектов файловой системы (ФС) и реестра представлено на рис.10.3. В основном окне задаются общие параметры работы механизма контроля целостности.

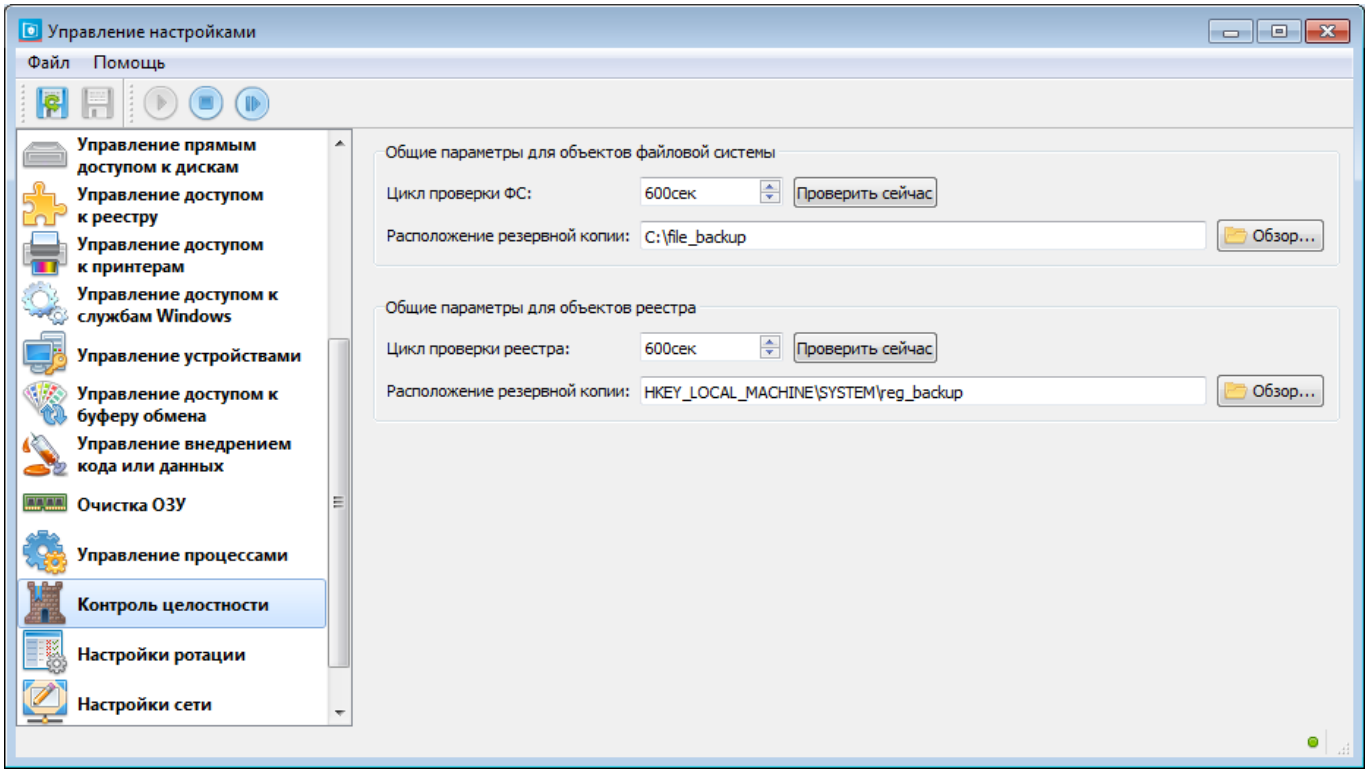


Рис.10.3. Интерфейс настройки механизма контроля целостности

Для задания общих настроек механизма контроля целостности объектов ФС и реестра необходимо:

1. Задать цикл проверки файловой системы (периодичность проверки в секундах).
2. Указать расположение резервной копии, используя «Обзор» или задать путь вручную.
3. Задать цикл проверки реестра (периодичность проверки в секундах).
4. Указать расположение резервной копии, используя «Обзор» или задать путь вручную.

Дополнительно можно запустить внеочередную проверку целостности. Также из меню (“Файл” можно запустить внеочередную проверку собственной целостности SafePoint.

10.3.1. Контроль целостности объектов файловой системы

Выбор интерфейса механизма контроля целостности объектов файловой системы представлен на рис.10.3.1.1.

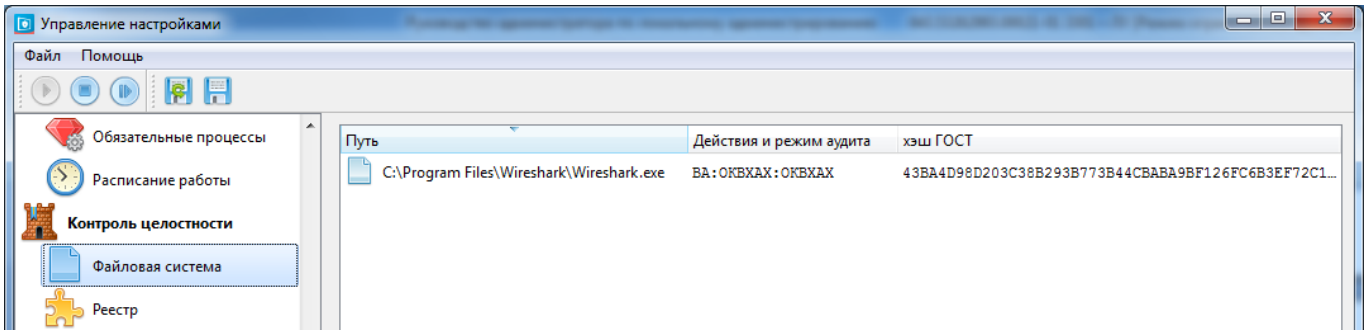


Рис.10.3.1.1. Интерфейс механизма контроля целостности объектов ФС

Объект ФС необходимо задавать путем конкретного указания либо файлов, либо каталогов. Использование масок невозможно.

Контроль целостности разделенных в сети файловых объектов производится на той машине, на которой физически хранятся файловые объекты.

Для создания нового контролируемого объекта файловой системы следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Контроль целостности» → «Файловая система».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Файловая система» и в контекстном меню (рис.10.3.1.2) выбрать «Добавить объект ФС».

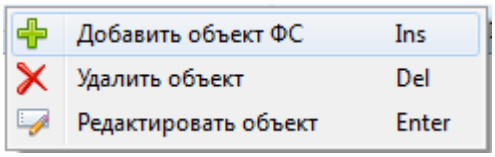


Рис.10.3.1.2. Контекстное меню «Добавления объекта ФС»

3. В появившемся окне «Добавление нового файлового объекта» (рис.10.3.1.3) произвести следующие настройки:

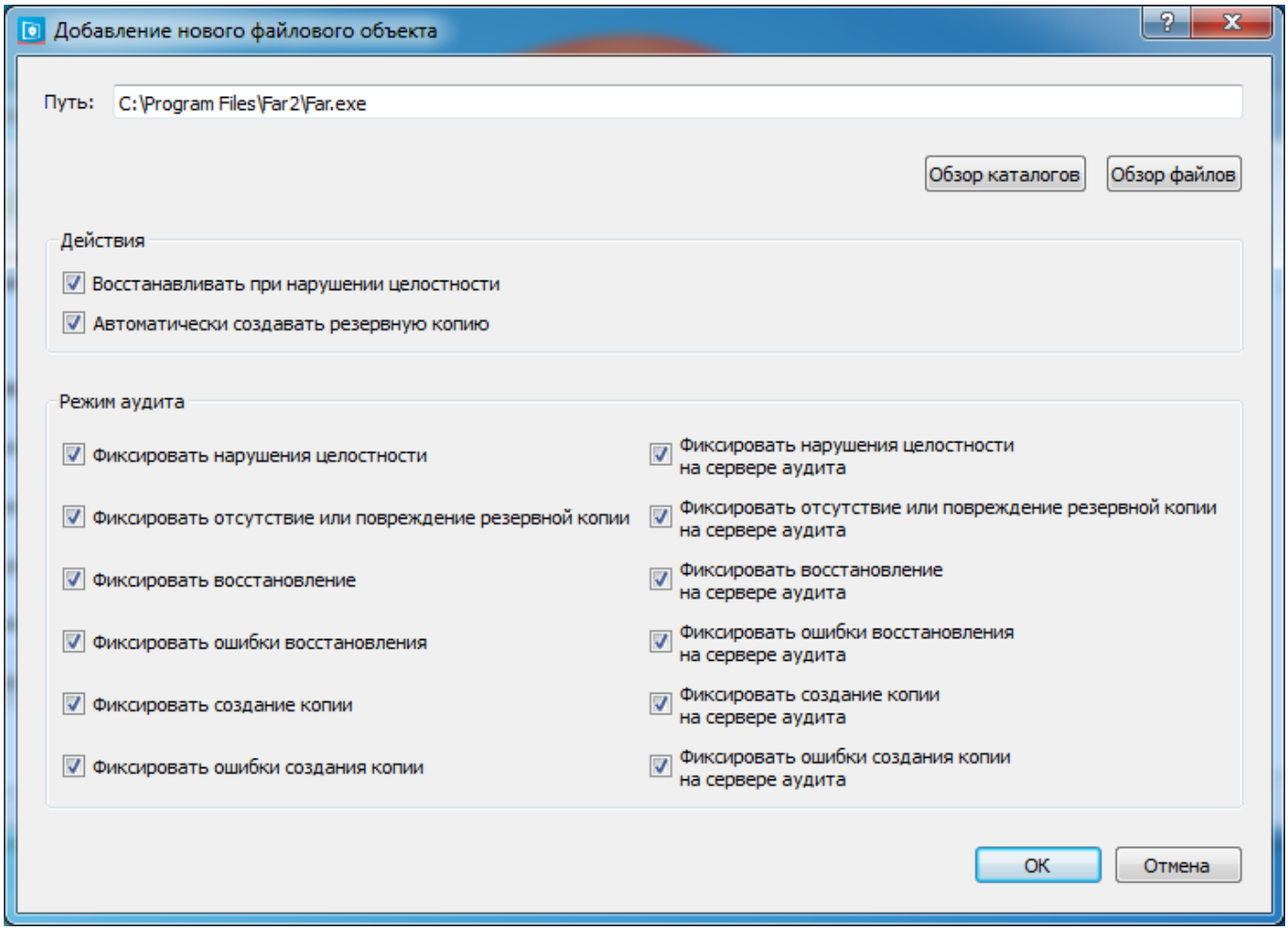


Рис.10.3.1.3. Окно добавления нового файлового объекта

1) Задать путь к объекту, используя «Обзор каталогов», «Обзор файлов» в зависимости от типа объекта или задать вручную.
2) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».

Для **просмотра** контролируемых объектов необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Контроль целостности» → «Файловая система». В интерфейсе указывается путь к объекту и его имя, действия и режим аудита, значение хеш-функции, вычисленной по ГОСТ 34.11-94 (рис.10.3.1.4).

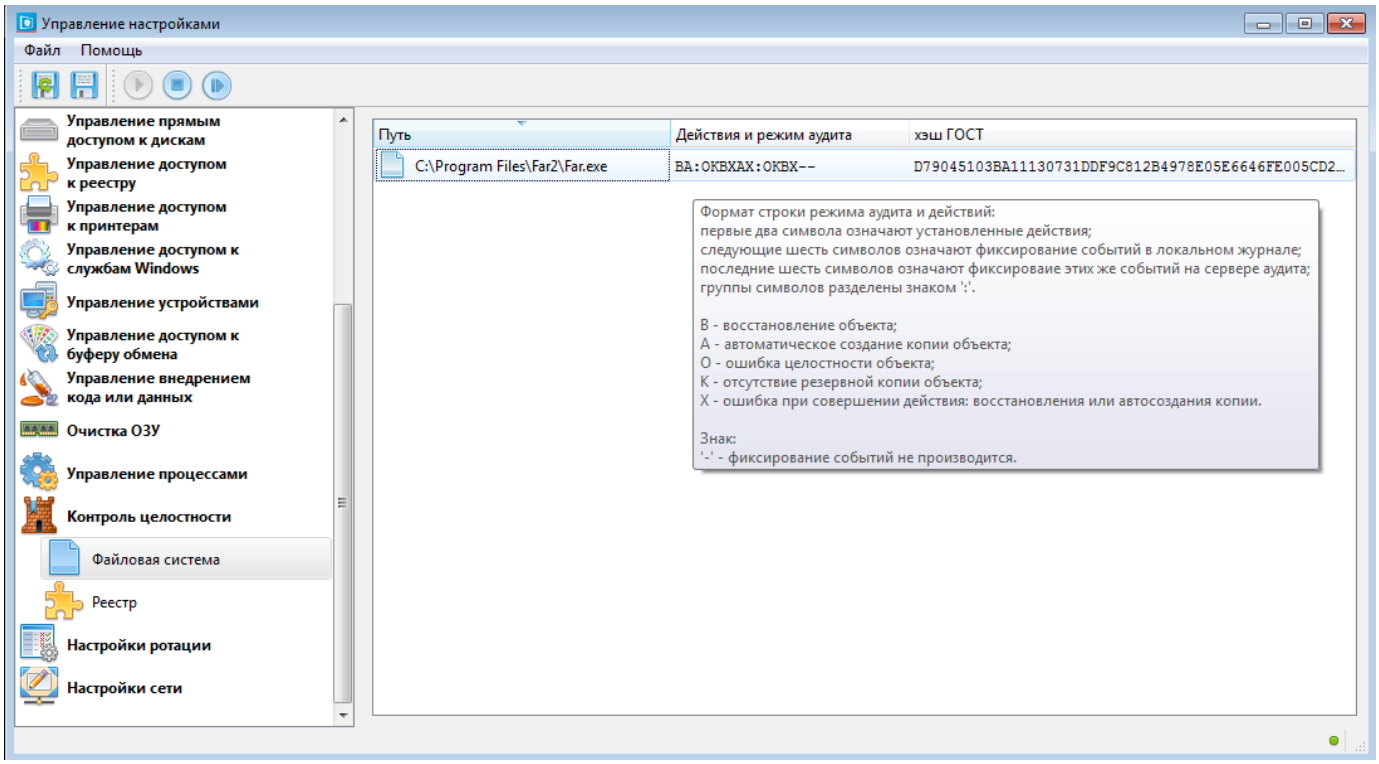


Рис.10.3.1.4. Просмотр контролируемых объектов ФС

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал контроля целостности».

Для **редактирования** уже созданного объекта ФС следует нажать правой кнопкой мыши по объекту в интерфейсе «Файловая система» (рис.10.3.1.4) и в контекстном меню выбрать «Изменить», внести нужные изменения.

Для **удаления** объекта ФС следует нажать правой кнопкой мыши по объекту в интерфейсе «Файловая система» (рис.10.3.1.4) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

10.3.2. Контроль целостности объектов реестра ОС

Выбор интерфейса механизма контроля целостности объектов реестра представлен на рис.10.3.2.1.

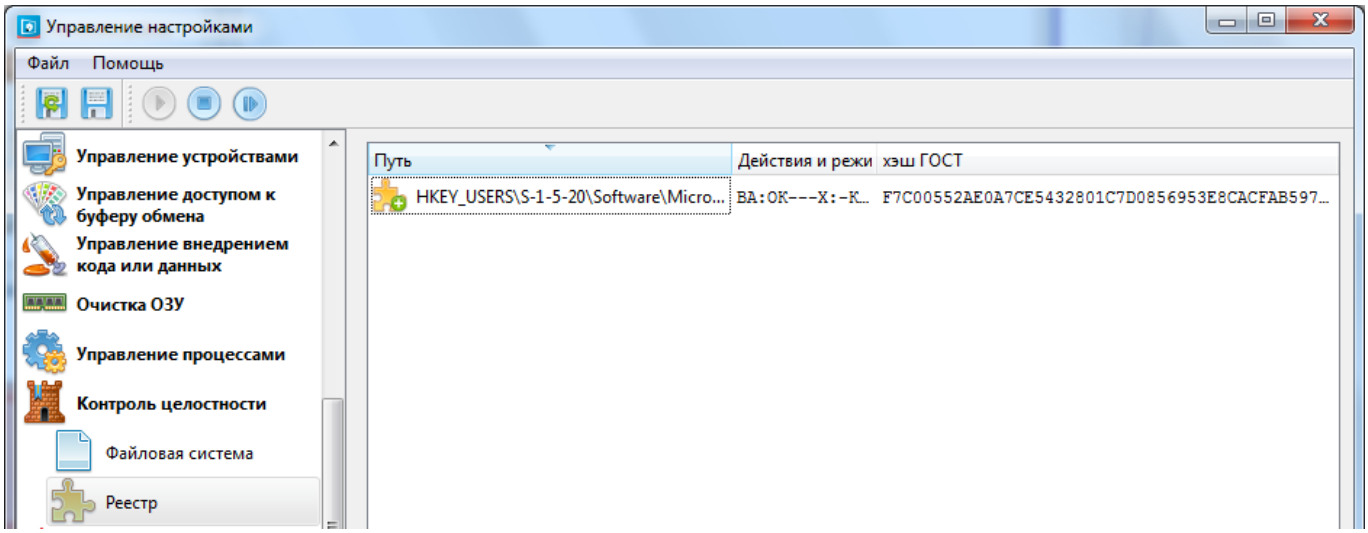


Рис.10.3.2.1. Интерфейс механизма контроля целостности объектов реестра

Объекты реестра необходимо задавать путем конкретного указания либо ключей, либо ветвей реестра. Использование масок невозможно.

Для создания нового контролируемого объекта реестра следует:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Контроль целостности» → «Реестр».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Реестр» и во всплывающем контекстном меню (рис.10.3.2.2) выберите пункт «Добавить объект».

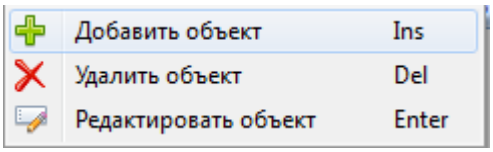


Рис.10.3.2.2. Контекстное меню окна «Реестр»

3. В появившемся окне «Добавление нового объекта реестра» (рис.10.3.2.3) произвести следующие настройки:

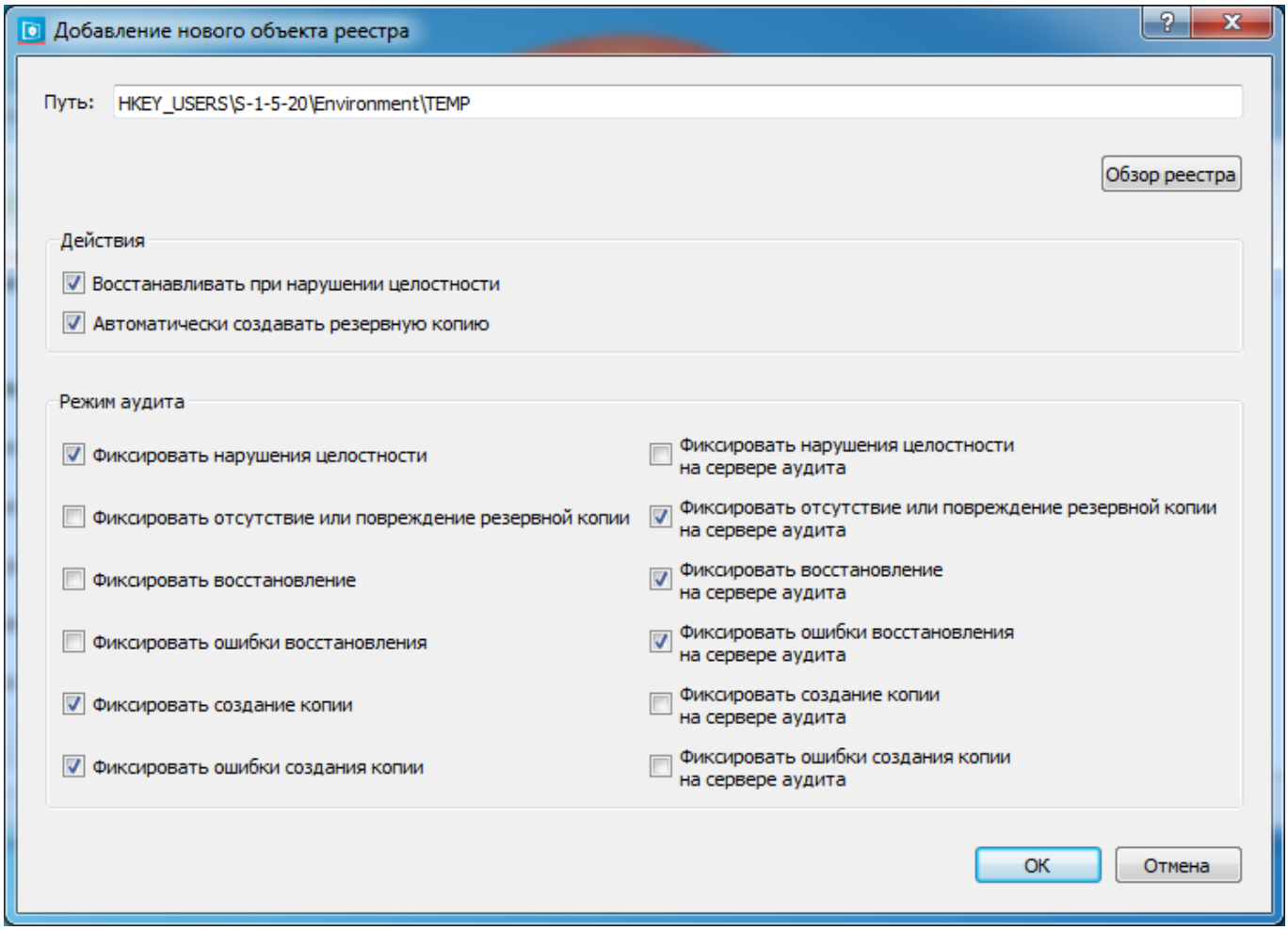


Рис.10.3.2.3. Окно добавления нового объекта реестра

1) Задать путь к объекту, используя «Обзор реестра» или задать путь вручную.

В обзоре отображаются только три корневые ветви реестра в связи с тем, что некоторые ветви, отображаемые в «regedit.exe» не существуют на самом деле, а являются символическими ссылками на существующие. Ветвь HKEY_CLASSES_ROOT - это символическая ссылка на объединение ветвей HKEY_LOCAL_MACHINE\SOFTWARE\Classes (классы, зарегистрированные для всего компьютера) и HKEY_CURRENT_USER\Software\Classes (классы зарегистрированные для текущего пользователя), HKEY_CURRENT_USER - это символическая ссылка на одну из ветвей корневой ветви HKEY_USERS (объекты реестра всех пользователей, которые успешно зашли в систему). Для указания объекта, отображаемого в «regedit.exe» в одной из ветвей, являющихся символическими ссылками на корневые ветви, необходимо найти этот объект в корневых ветвях.

2) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».

Для **просмотра** контролируемых объектов реестра необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Контроль целостности» → «Реестр». В интерфейсе указывается: полнопутевое имя объекта, действия и режим аудита, значение хеш-функции, вычисленной по ГОСТ 34.11-94 (рис.10.3.2.4).

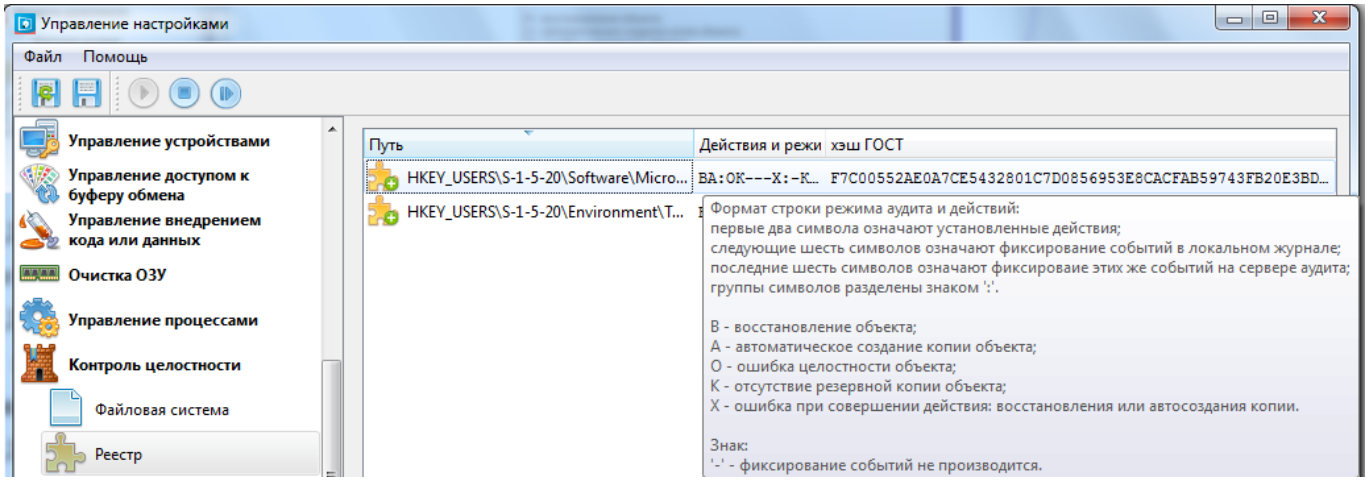


Рис.10.3.2.4. Просмотр контролируемых объектов реестра

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал контроля целостности».

Для **редактирования** уже созданного объекта реестра следует нажать правой кнопкой мыши по объекту в интерфейсе «Реестр» (рис.10.3.2.4) и в контекстном меню выбрать «Изменить», и внести нужные изменения.

Для **удаления** объекта реестра следует нажать правой кнопкой мыши по объекту в интерфейсе «Реестр» (рис.10.3.2.4) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

10.3.3. Контроль целостности объектов СЗИ «ViPNet SafePoint»

Контроль целостности объектов СЗИ «ViPNet SafePoint» состоит в контроле **файловых объектов с системными файлами** и **файлами настроек СЗИ «ViPNet SafePoint»**, а также **объектов реестра ОС**, используемых СЗИ «ViPNet SafePoint». Контролируемые объекты реестра:

- HKEY_LOCAL_MACHINE\Software\INFOTECS\VIPNET SAFEPOINT\Common\Package Config;
- HKEY_LOCAL_MACHINE\Software\INFOTECS\VIPNET SAFEPOINT Service\uuid;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\Parameters\DriversDir;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\Group;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\ImagePath;

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\Start;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\ErrorControl;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\Tag;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\armdrv3\Type;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\Group;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\ImagePath;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\Start;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\ErrorControl;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\Tag;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\devCtrl3\Type;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\Group;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\ImagePath;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\Start;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\ErrorControl;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\Tag;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\fileCtrl3\Type;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\Group;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\ImagePath;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\Start;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\ErrorControl;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\Tag;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regCtrl3\Type;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Armour service\ImagePath;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Armour service\ObjectName;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Armour service\Start;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Armour service\ErrorControl;
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Armour service\Type.

Контроль целостности объектов СЗИ «ViPNet SafePoint» реализован автоматически. Контроль осуществляется при каждом старте службы СЗИ «ViPNet SafePoint», осуществляемом при загрузке системы, либо вручную пользователем, и синхронно – с периодом в 10 минут. Реакцией на несанкционированные действия в отношении контролируемых событий является автоматическое восстановление измененных контролируемых объектов из резервной копии. Резервные копии объектов СЗИ «ViPNet SafePoint» создаются автоматически, резервные копии

настроек создаются, так же автоматически, при их сохранении, при задании или модификации настроек из интерфейса СЗИ «ViPNet SafePoint». Все несанкционированные события, связанные с нарушением целостности СЗИ «ViPNet SafePoint» и его восстановлением, фиксируются в Просмотрщике журналов аудита в «Журнале контроля целостности» (см. раздел 15.2.4. Аудит событий).

Механизм контроля целостности является ресурсозатратным механизмом, поэтому предусмотрена возможность отключения контроля целостности объектов СЗИ «ViPNet SafePoint». Для реализации данной возможности необходимо создать в реестре ключ «HKLM\Software\INFOTECS\VIPNET SAFEPOINT Service\Integrity Flags» типа DWORD и присвоить ему значение «0». Также присутствуют возможности по управлению данным механизмом, описание этих возможностей приведено в Приложении 1 к данному документу.

11. МЕХАНИЗМЫ ГАРАНТИРОВАННОГО УДАЛЕНИЯ И ОЧИСТКИ ПАМЯТИ

11.1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

Данная группа механизмов в модели защиты СЗИ «ViPNet SafePoint» предназначена для предотвращения доступа к обрабатываемой информации в обход разграничительной политики доступа к защищаемой информации, связанной с появлением в системе остаточной информации.

Остаточная информация образуется на файловых накопителях (жесткий диск и внешние файловые устройства) и в оперативной памяти. Причем, если остаточная информация в оперативной памяти существует до выключения питания компьютера, то на устройствах она может сохраняться продолжительное время. Это связано с тем, что при удалении файла, собственно информацию система не удаляет – системой изменяется соответствующая таблица MFT. При этом удаляемая системой информация уже не образует файловый объект – к ней невозможно получить доступ, как к объекту файловой системы, однако она остается записанной на накопителе, т.е. к ней можно получить доступ в обход разграничительной политики, в частности, с использованием утилит прямого доступа к диску.

Естественно, что особенно это критично в отношении внешних файловых накопителей.

В модели защиты СЗИ «ViPNet SafePoint» гарантированное удаление информации на жестких дисках и на внешних файловых накопителях предполагает реализацию двух механизмов. Это обусловлено реализацией двух механизмов контроля доступа к файловым объектам – к статичным файловым объектам и к создаваемым файлам, который, в свою очередь, предполагает реализацию дискреционного принципа контроля доступа и контроля.

При контроле доступа к статичным файловым объектам реализуется разграничительная политика субъектов к объектам. При этом администратором разрешается запись определенной информации в определенные объекты, т.е. критичность (необходимость гарантированного удаления) информации определяется объектом (именем объекта). Как следствие, правила гарантированного удаления статичных файловых объектов должны устанавливаться применительно к объектам файловой системы (как правило, к папкам).

При контроле же доступа к создаваемым файлам, объект доступа исключен из разграничительной политики. Любой субъект доступа в общем случае (если это не ограничивается механизмом контроля доступа к статичным файловым объектам и к файловым накопителям) может создавать файл в любой папке. Правила же доступа устанавливаются для субъектов в отношении файлов, создаваемых другими субъектами. При реализации принципа контроля доступа на основе меток безопасности, в качестве субъектов доступа выступают метки безопасности (соответствующие уровни). Как следствие, правила гарантированного удаления в

данном случае – к создаваемым файлам, должны устанавливаться не применительно к конкретным файловым объектам, а применительно к субъектам, создавшим файлы – должно задаваться файлы, созданные какими субъектами (или пользователями с какими метками безопасности), должны гарантированно удаляться, и с какими параметрами.

В качестве параметров гарантированного удаления в модели защиты СЗИ «ViPNet SafePoint» можно задавать (для любого объекта при контроле к статичным файловым объектам, для любого субъекта (или/и метки безопасности) при контроле к создаваемым файлам) шаблон (набор символов, который будет записан поверх информации при ее удалении) и число циклов перезаписи.

Работают механизмы гарантированного удаления информации СЗИ «ViPNet SafePoint» следующим образом. В случае удаления файлового объекта, для которого тем или иным образом (для объекта, либо для создающего его субъекта) заданы правила гарантированного удаления (шаблон и число циклов перезаписи), соответствующий запрос на удаление перехватывается СЗИ «ViPNet SafePoint». СЗИ «ViPNet SafePoint» осуществляет по заданным правилам запись информации (шаблона) в соответствующий объект, после чего возвращает системе запрос на удаление. В результате этого, системой штатными средствами удаляется уже модифицированный файл, в который СЗИ «ViPNet SafePoint» заданное число раз (по числу заданных циклов перезаписи) записан заданный шаблон символов. После выполнения гарантированного удаления остаточную информацию образуют символы записанного на место удаляемой информации шаблона.

Кроме того, в части гарантированного удаления в модели защиты СЗИ «ViPNet SafePoint» предусмотрен механизм ручного гарантированного удаления администратором разделов жесткого диска и внешних файловых накопителей. На жестком диске администратором создаются разделы. Любой из них (разделы, доступные для ОС, для удобства отображаются «буквой диска») может быть гарантированно удален (включая удаление всех файловых объектов и остаточной информации, присутствующих на разделе). Аналогично можно гарантированно удалить всю информацию на внешнем файловом накопителе. Для гарантированного удаления вручную администратором также может задаваться шаблон и количество циклов перезаписи.

Остаточная информация в оперативной памяти возникает в результате ее перераспределения (хранится до отключения питания компьютера). В качестве критичных событий в модели СЗИ «ViPNet SafePoint», в отношении необходимости удаления остаточной информации в оперативной памяти, приняты начало/завершения сеанса пользователя, запуск/завершение процесса (поскольку угрозу несанкционированного доступа к информации, в данном случае, к остаточной, в оперативной памяти, может нести в себе, как пользователь, так и

процесс (приложение)). В отношении данного события (а также любой их совокупности) может быть задана и реализована СЗИ «ViPNet SafePoint» очистка (очистка остаточной информации) оперативной памяти. При наступлении соответствующего (соответствующих) заданного события, диспетчером СЗИ «ViPNet SafePoint» будет удаляться остаточная информация в оперативной памяти.

При настройке правил гарантированного удаления необходимо помнить, что в ОС Windows предусмотрена функция удаления файлов в Корзину. Это действие не является фактическим удалением и, если такое действие разрешено администратором, то необходимо назначить правила гарантированного удаления для объекта «Корзина», которые будут срабатывать при ее очищении. Либо запретить «удаление файлов в корзину».

11.2. ГАРАНТИРОВАННОЕ УДАЛЕНИЕ

11.2.1. Создание шаблона с автоматическим заполнением значений

Под шаблоном гарантированного удаления понимается набор значений, которыми будут перезаписаны объекты, перед их удалением средствами ОС.

Прежде всего, следует создать шаблон, согласно которому будет производиться гарантированное удаление. Для создания шаблона с автоматическим заполнением значений необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление» в зависимости от механизма, для которого будет создан шаблон.
2. Нажать правой кнопкой мыши по пустой области окна «Шаблоны» и в контекстном меню (рис.11.2.1.1) выбрать «Добавить шаблон».

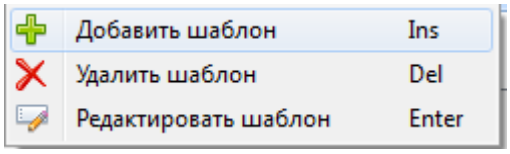


Рис.11.2.1.1. Контекстное меню окна «Шаблоны»

3. В окне «Создание нового шаблона» (рис.11.2.1.2) задать:

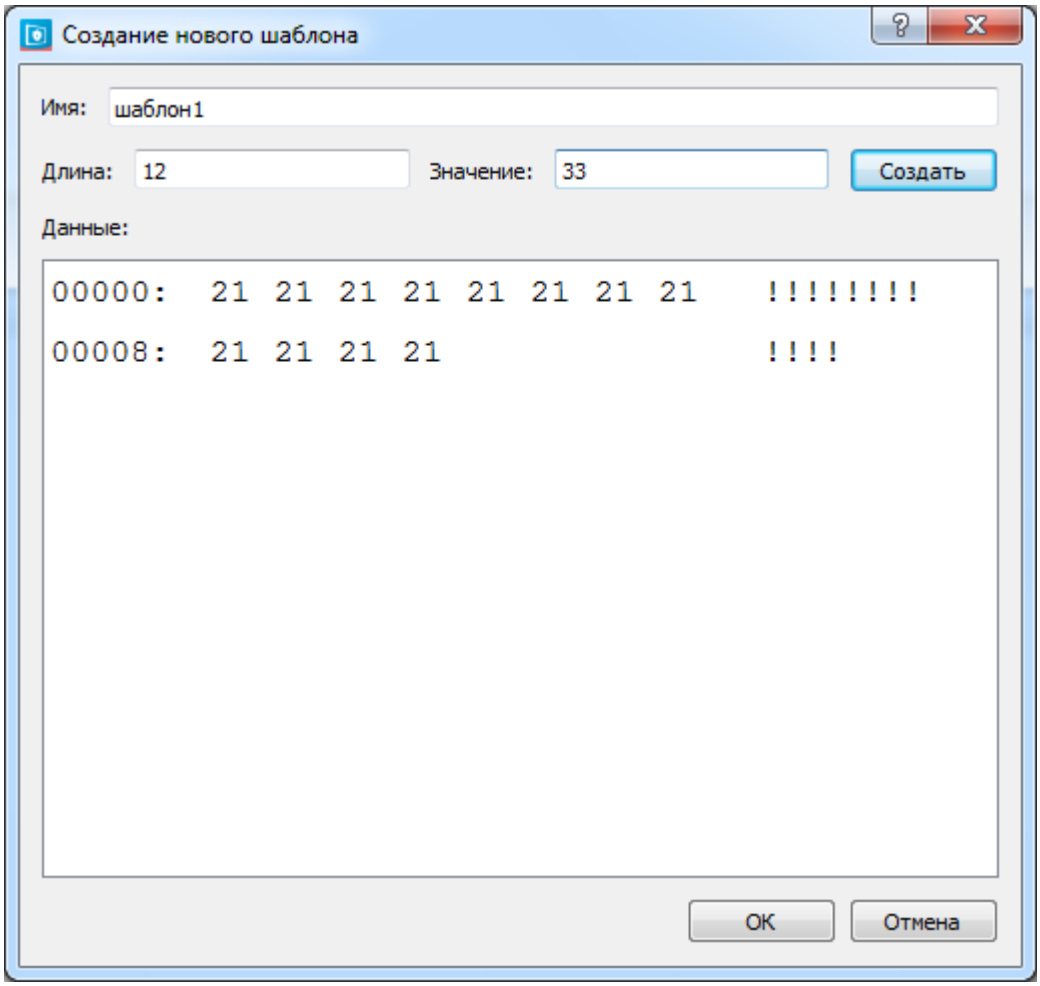


Рис.11.2.1.2. Окно создание нового шаблона

1) Имя шаблона.
2) Длину шаблона (максимальная длинна 65536).
3) Значение шаблона (максимальное значение 255).

4. Нажать кнопку «Создать» и затем кнопку «ОК».

Для **просмотра** созданных шаблонов гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление» (рис.11.2.1.3). В интерфейсе для каждого шаблона указаны имя, длина и данные.

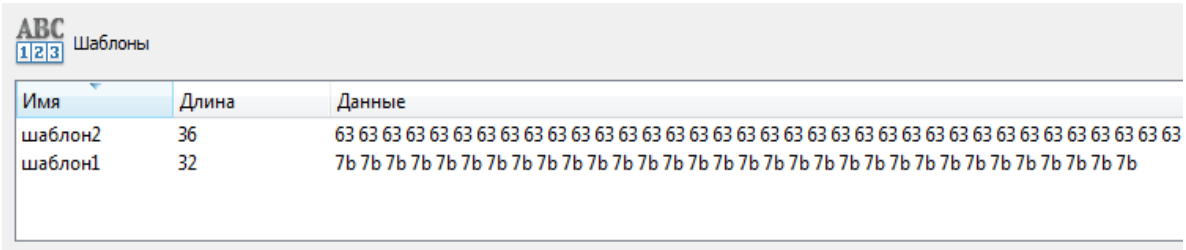


Рис.11.2.1.2. Интерфейс просмотра шаблонов гарантированного удаления

Для **редактирования** или **удаления** шаблонов гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление», выбрать шаблон и воспользоваться контекстным меню окна (рис.11.2.1.1, рис. 11.2.2.1), для удаления или внесения изменений в шаблон.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

11.2.2. Создание шаблона с ручным заполнением значений

Для создания шаблона гарантированного удаления с ручным заполнением значений необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление» в зависимости от механизма, для которого будет создан шаблон.
2. Нажать правой кнопкой мыши по пустой области окна «Шаблоны» и в контекстном меню (рис.11.2.2.1) выбрать «Добавить шаблон».

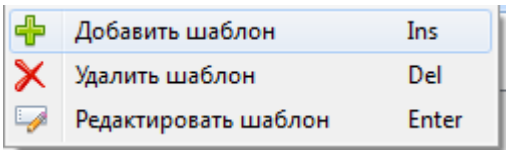


Рис.11.2.2.1. Контекстное меню окна «Шаблоны»

3. В окне «Создание нового шаблона» (рис.11.2.2.2) задать:

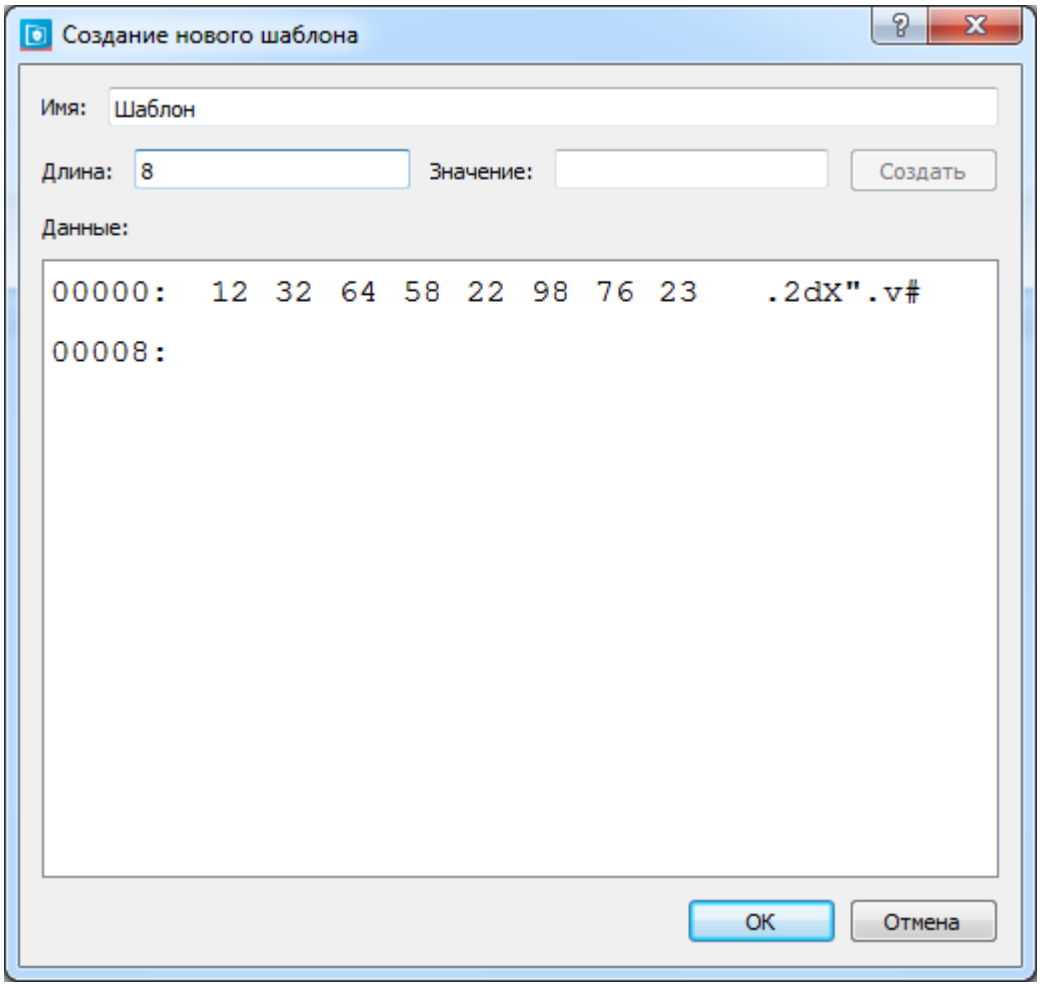


Рис.11.2.2.2. Окно «Создание нового шаблона»

1) Имя шаблона.
2) Длина шаблона заполняется автоматически в зависимости от значений.
3) Оставить поле «Значение» пустым.
4) Последовательно задать значения шаблона.

4. Нажать кнопку «ОК».

Для **просмотра** созданных шаблонов гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление» (рис.11.2.2.3).В интерфейсе для каждого шаблона указаны имя, длина и данные.

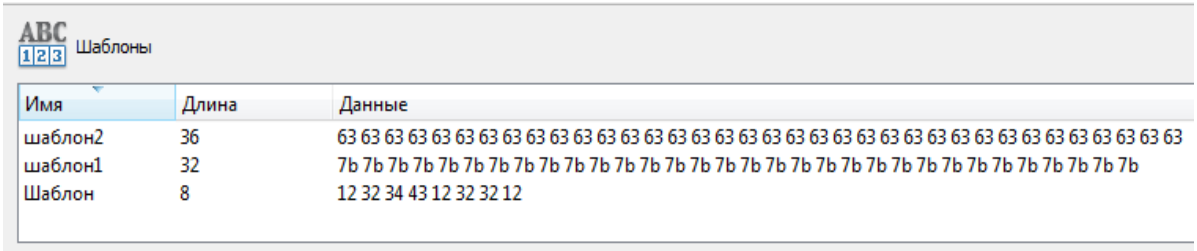


Рис.11.2.2.2. Интерфейс просмотра шаблонов гарантированного удаления

Для **редактирования** или **удаления** шаблонов гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» или выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление», выбрать шаблон и воспользоваться контекстным меню окна (рис.11.2.1.1, рис.11.2.2.1), для удаления или внесения изменений в шаблон.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

11.2.3. Назначение правила гарантированного удаления статичных файловых объектов

Правила гарантированного удаления статичных файловых объектов задаются для объектов, заведенных в СЗИ «ViPNet SafePoint». Для назначения правила гарантированного удаления статичных файловых объектов необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление».
2. Нажать правой кнопкой мыши по пустой области окна «Правила гарантированного удаления» и в контекстном меню (рис.11.2.3.1) выбрать «Добавить правило».

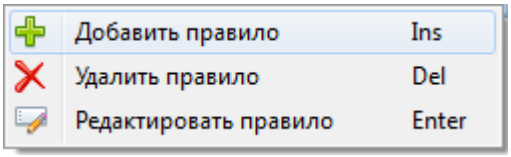


Рис.11.2.3.1. Контекстное меню окна «Правила гарантированного удаления»

3. В окне «Редактирование правила гарантированного удаления» (рис.11.2.3.2) следует:

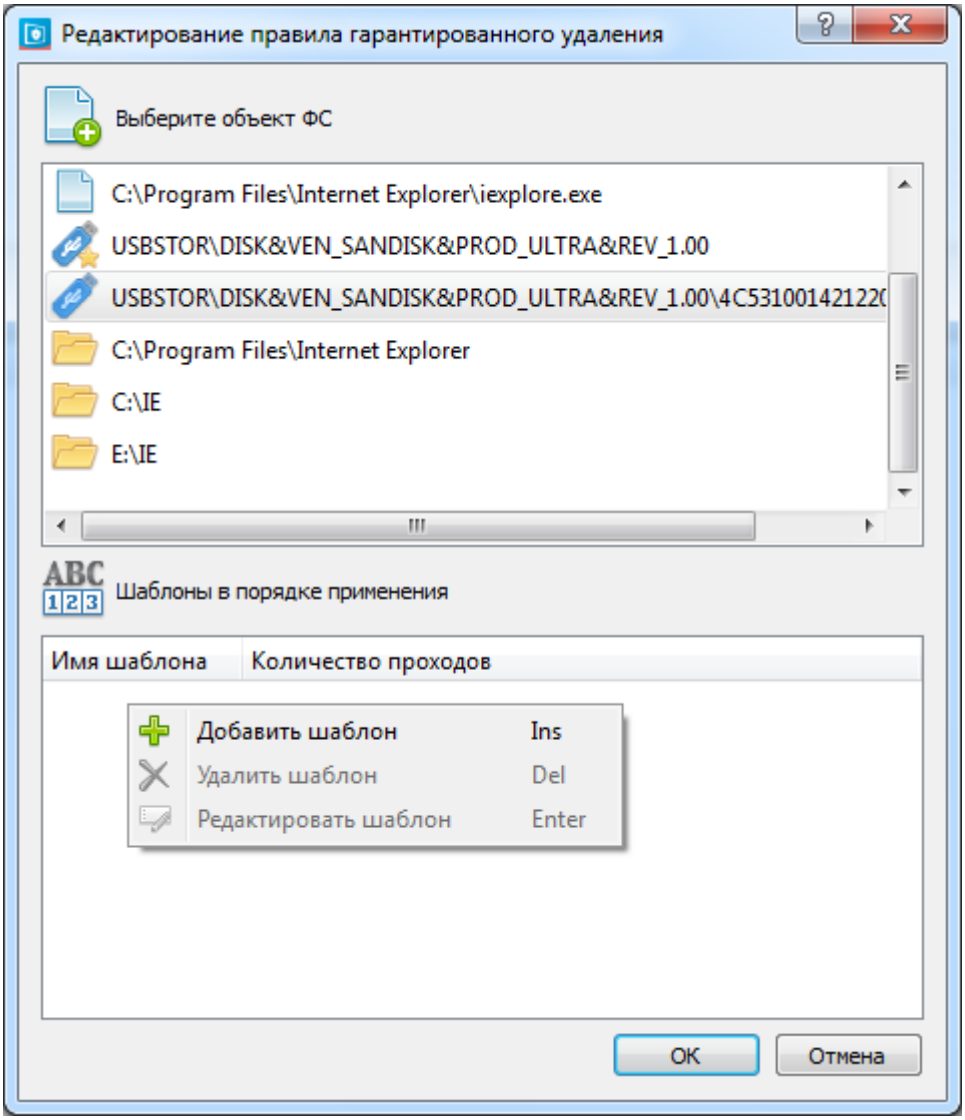


Рис.11.2.3.2. Окно редактирования правил гарантированного удаления

1) Выбрать объект ФС из списка.
2) Нажать правой кнопкой мыши по пустой области окна «Шаблоны в порядке применения».
3) В контекстном меню выбрать «Добавить шаблон».
4) В появившемся окне «Редактирование правила применения шаблонов»:
   - выбрать шаблон;
   - задать количество проходов (максимальное значение 63) - число циклов перезаписи;

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» (рис.11.2.3.3). В интерфейсе

отражается объект ФС, для которого назначено правило гарантированного удаления, и шаблон, с указанием количества проходов в скобках.

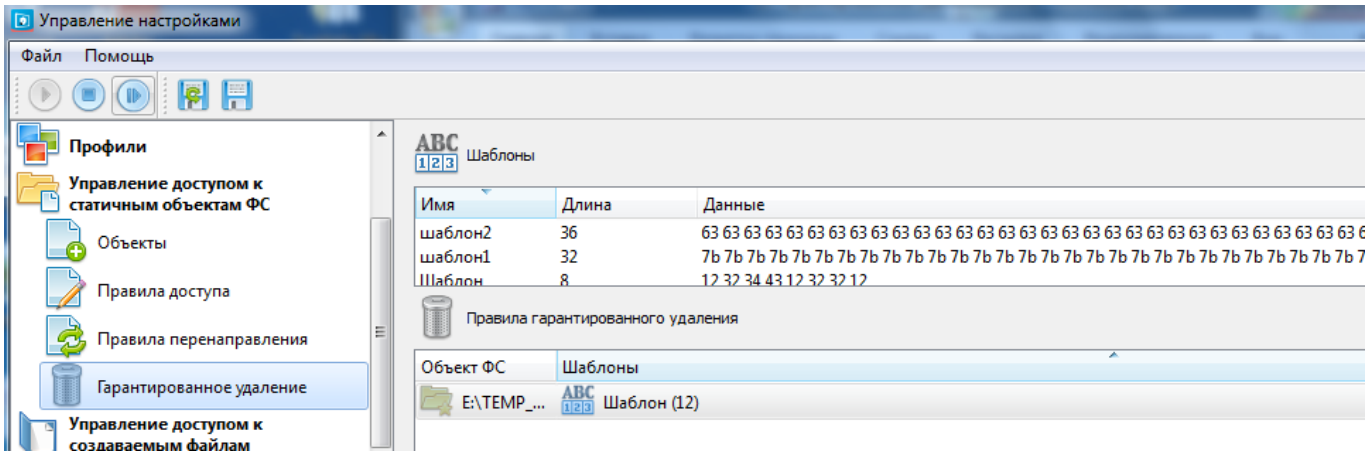


Рис.11.2.3.3. Интерфейс просмотра назначенных правил гарантированного удаления

Для **редактирования** или **удаления** правил гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление», выбрать правило и воспользоваться контекстным меню окна (рис.11.2.3.1), для внесения изменений или удаления правила.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

11.2.4. Назначение правил гарантированного удаления создаваемых файлов

Правила гарантированного удаления создаваемых файлов задаются по уровням доступа или для конкретных субъектов доступа. Для назначения правила гарантированного удаления создаваемых файлов необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление».
2. Нажать правой кнопкой мыши по пустой области окна «Правила гарантированного удаления» и в контекстном меню (рис.11.2.4.1) выбрать «Добавить правило».

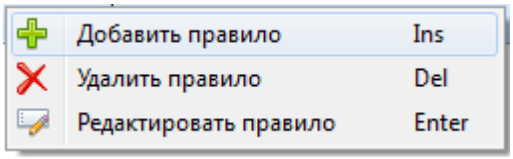


Рис.11.2.4.1. Контекстное меню окна «Правила гарантированного удаления»

3. В окне «Добавление нового правила гарантированного удаления» (рис.11.2.4.2) следует:

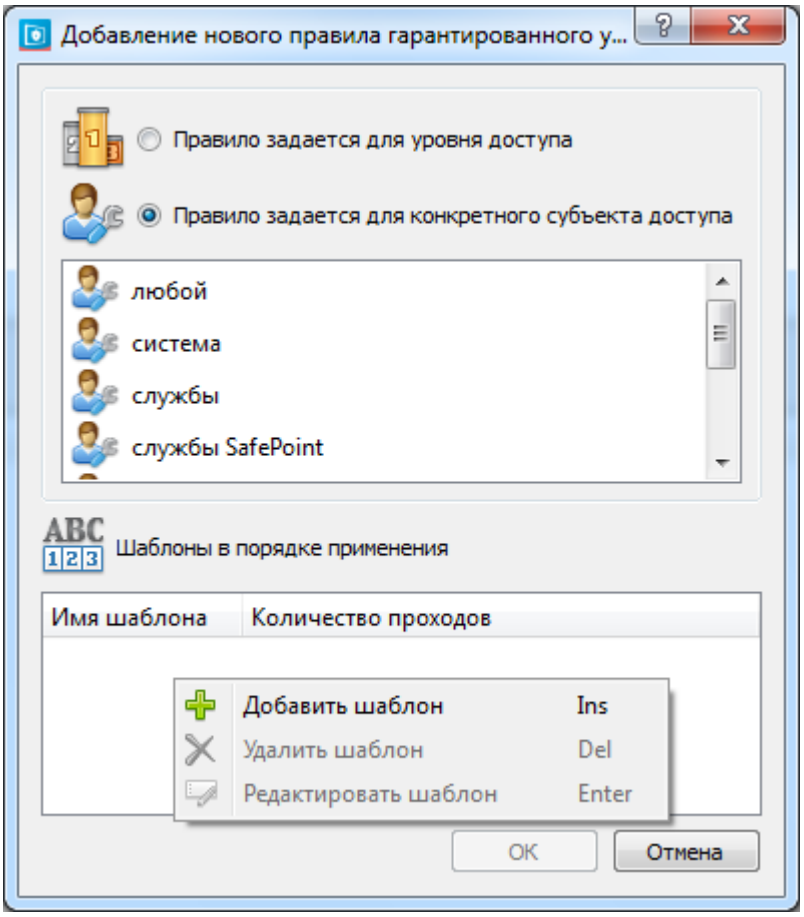


Рис.11.2.4.2. Окно добавления нового правила гарантированного удаления

1) В целях задания правила для механизма контроля доступа на основе меток безопасности выбрать «Правило задается для уровня доступа» и указать необходимый уровень доступа. В целях задания правила для механизма дискреционного управления доступом выбрать «Правило задается для конкретного субъекта доступа» и указать необходимый субъект доступа.
2) Нажать правой кнопкой мыши по пустой области окна «Шаблоны в порядке применения».
3) В контекстном меню выбрать «Добавить шаблон».
4) В появившемся окне «Редактирование правила применения шаблонов»:
   - выбрать шаблон;
   - задать количество проходов (максимальное значение 63) - число циклов перезаписи.

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление (рис.11.2.4.3). В интерфейсе

отражается уровень доступа или субъект, для которого назначено правило гарантированного удаления, и шаблон, с указанием количества проходов.

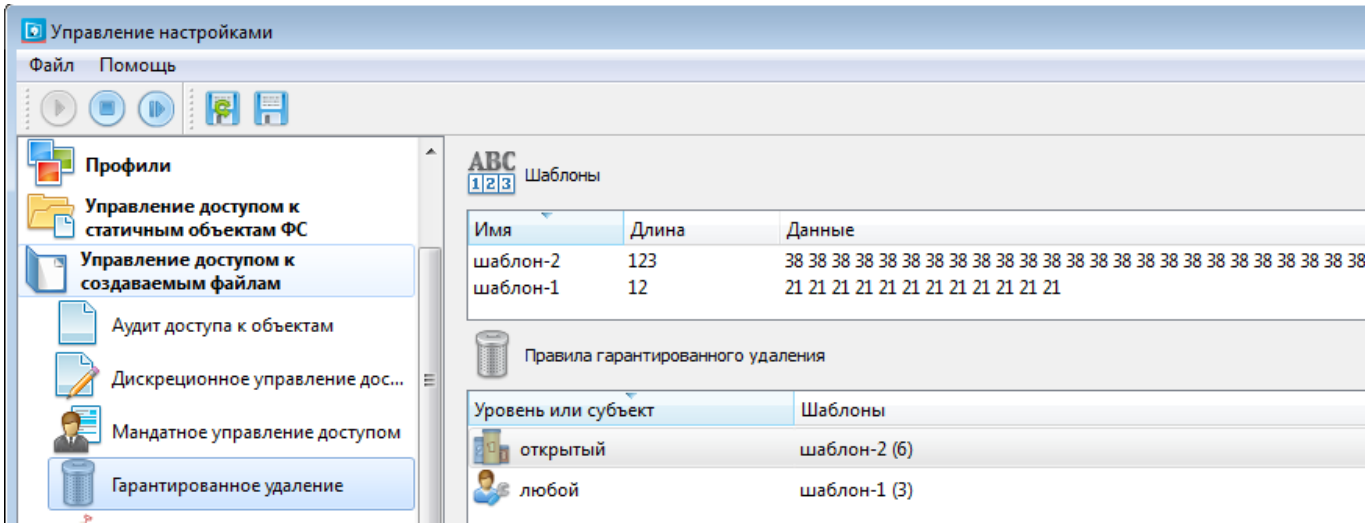


Рис.11.2.4.3. Интерфейс просмотра назначенных правил гарантированного удаления

Для **редактирования** или **удаления** правил гарантированного удаления необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к создаваемым файлам» → «Гарантированное удаление» выбрать правило и воспользоваться контекстным меню окна (рис.11.2.4.1), для внесения изменений или удаления правила.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

11.2.5. Механизм полной очистки дисковых устройств. Интерфейс

В очищаемой области будут записаны данные из шаблонов записи, перед ее очисткой средствами ОС.

Для открытия интерфейса механизма полной очистки дисковых устройств необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к статичным объектам ФС» → «Гарантированное удаление» и запустить программу полной очистки дисковых устройств (рис.11.2.5.1).

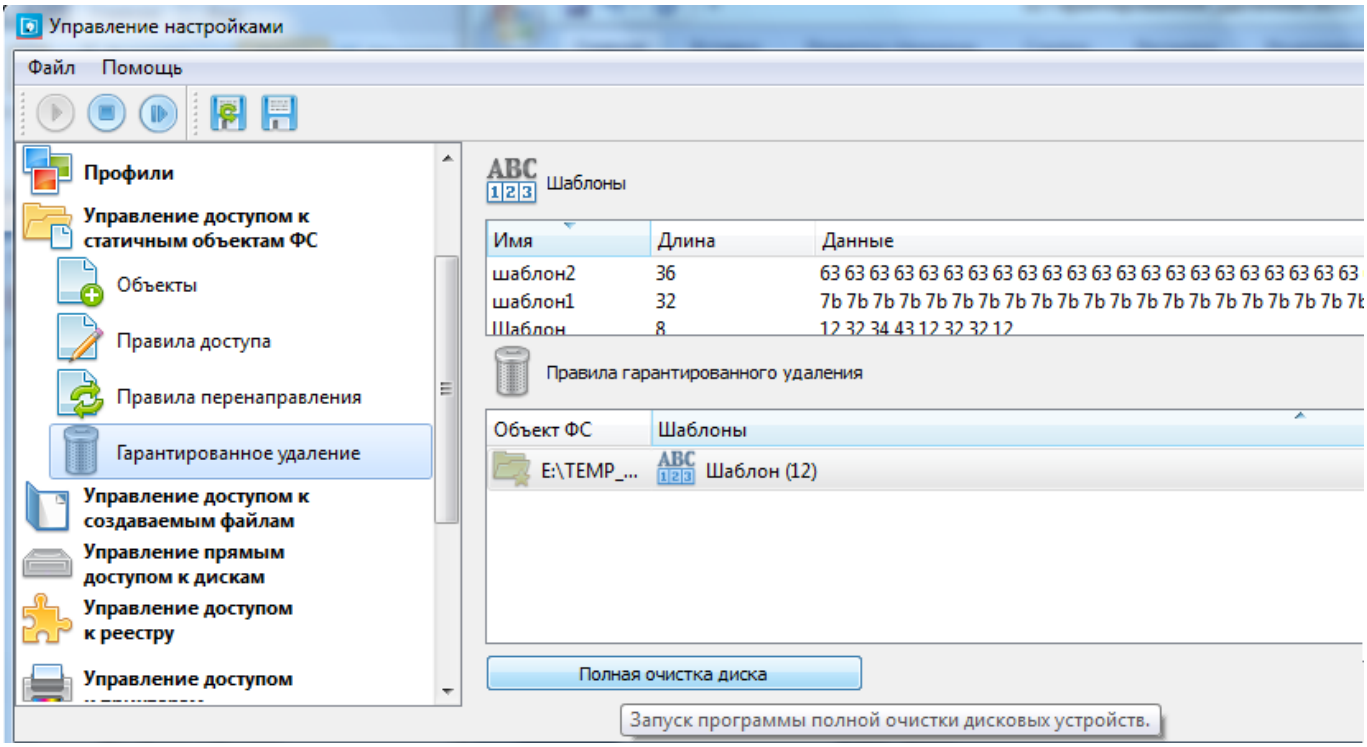


Рис.11.2.5.1. Запуск программы полной очистки дисковых устройств

В появившемся окне «Очистка устройств хранения данных» необходимо произвести следующие настройки:

1. Выбрать имя диска или раздела, для которого будут заданы шаблоны очистки (рис.11.2.5.2).

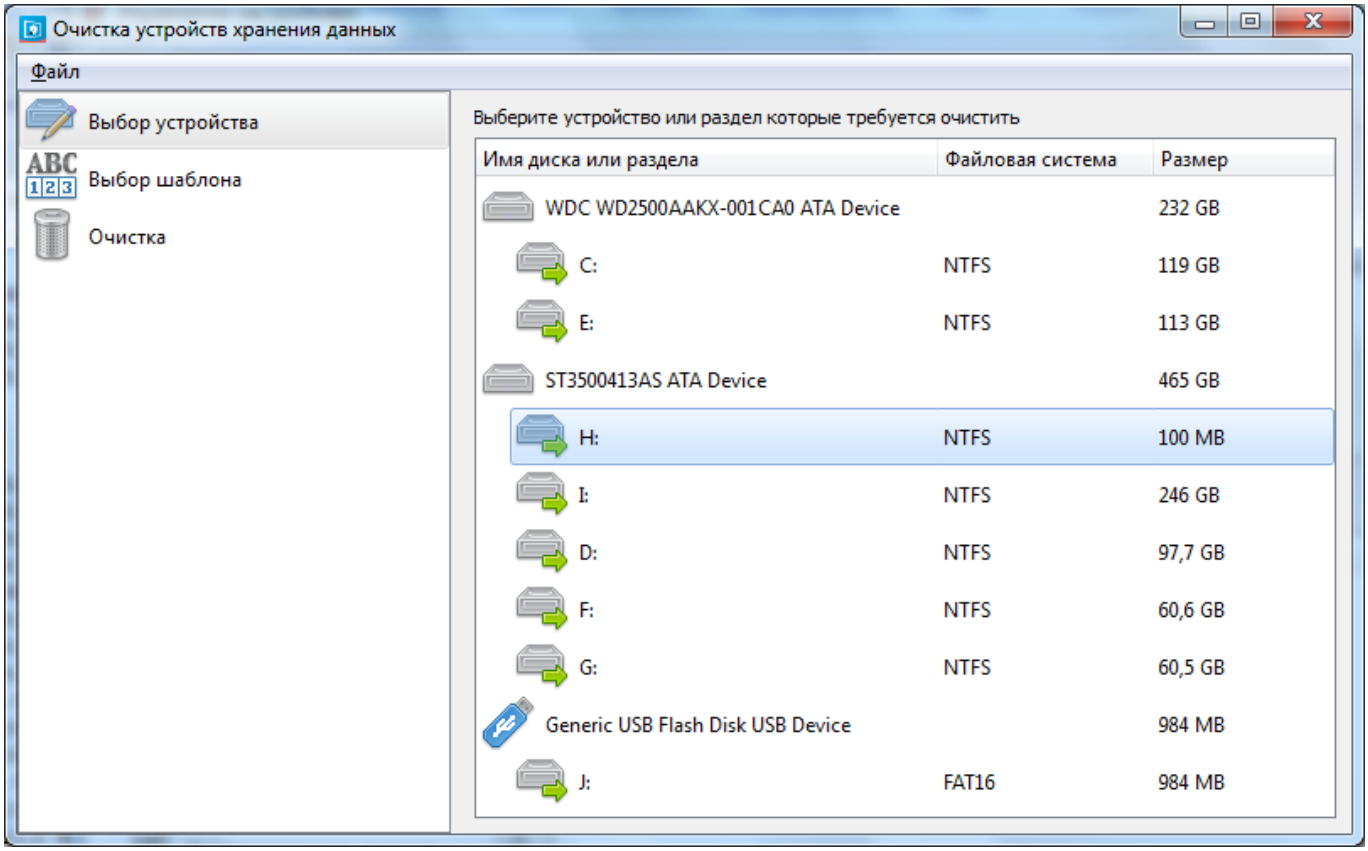


Рис.11.2.5.2. Выбор диска или раздела диска

2. Выбрать шаблон или шаблоны, по которым будет производиться очистка диска или раздела диска, и в появившемся окне ввести количество проходов (число циклов перезаписи) (рис.11.2.5.3).

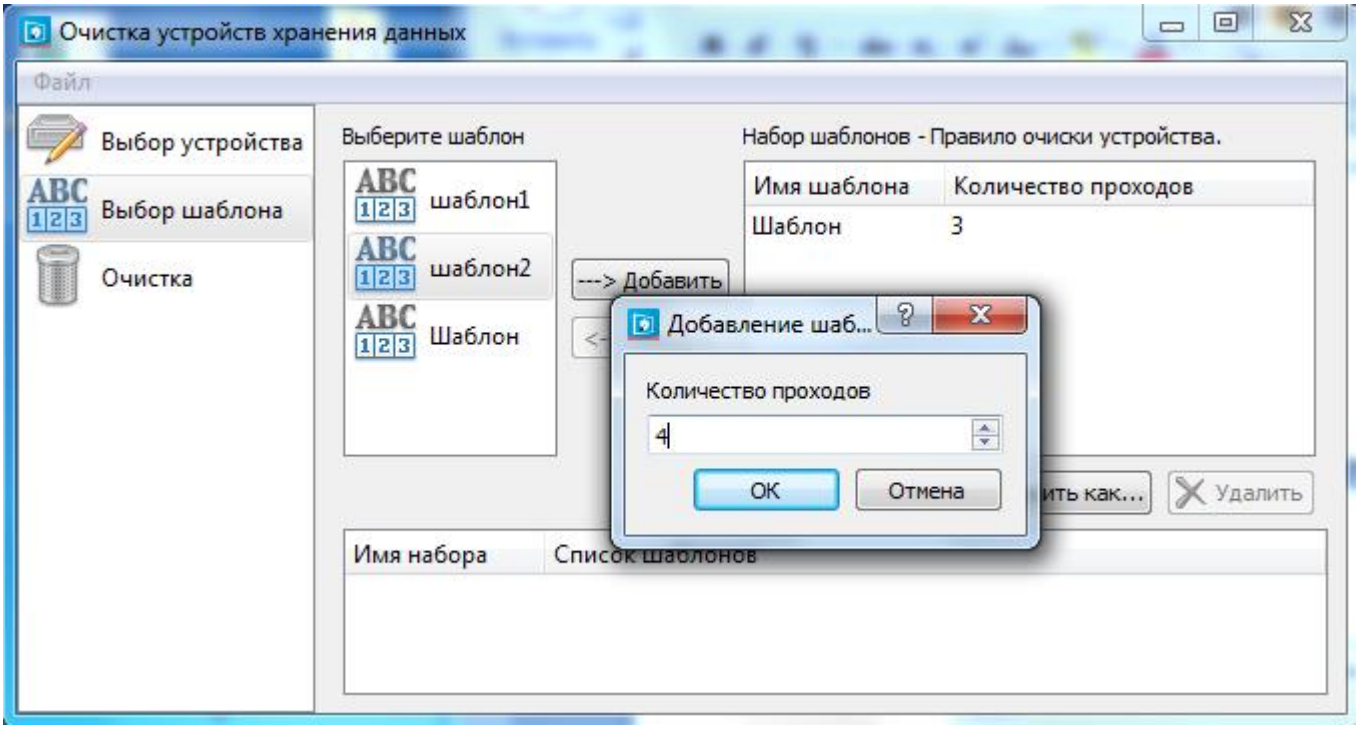


Рис.11.2.5.3. Выбор шаблонов записи

Механизм полной очистки дисковых устройств использует шаблоны очистки, которые задаются для гарантированного удаления статичных объектов файловой системы.

3. Сохранить набор (шаблоны очистки и количества их проходов), воспользовавшись клавишами «Сохранить» (для создания нового набора или внесения изменений в текущий) или «Сохранить как» (для сохранения изменений набора, в виде нового), и задать имя набора в появившемся окне (рис.11.2.5.4).

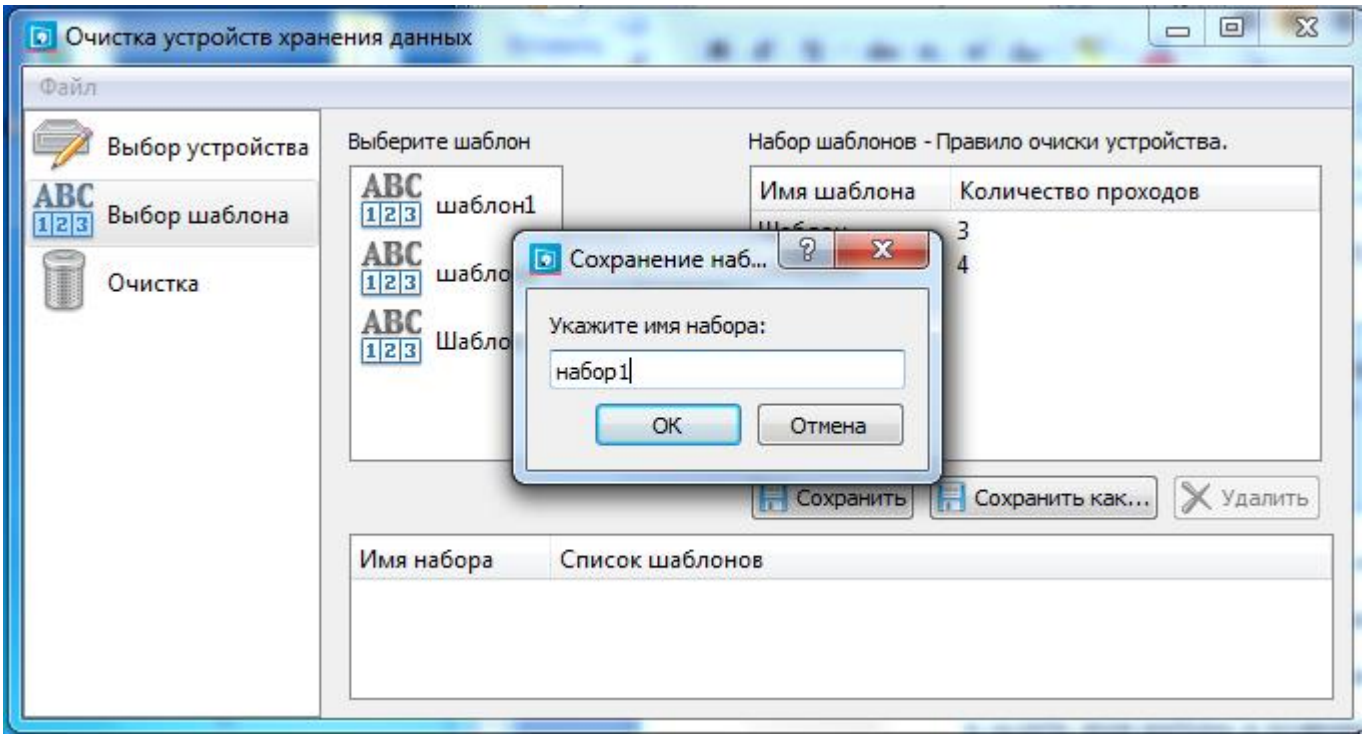


Рис.11.2.5.4. Сохранение набора шаблонов записи

4. В меню «Очистка» нажать «Начать очистку устройства» (рис.11.2.5.5).

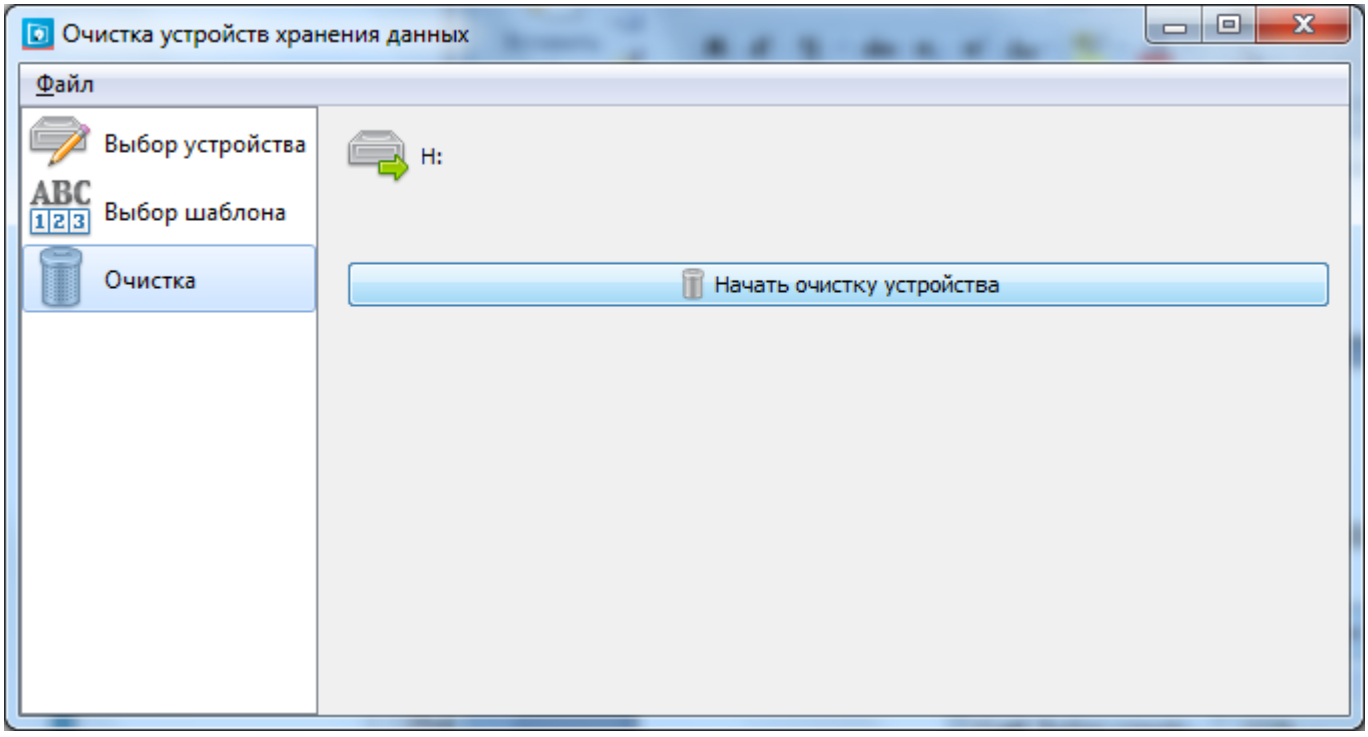


Рис.11.2.5.5. Запуск очистки устройств хранения данных

5. В появившемся окне «Подтвердите очистку» выбрать необходимый вариант.

В окне «Очистка устройств хранения данных» отражается прогресс процесса очистки устройств (рис.11.2.5.6).

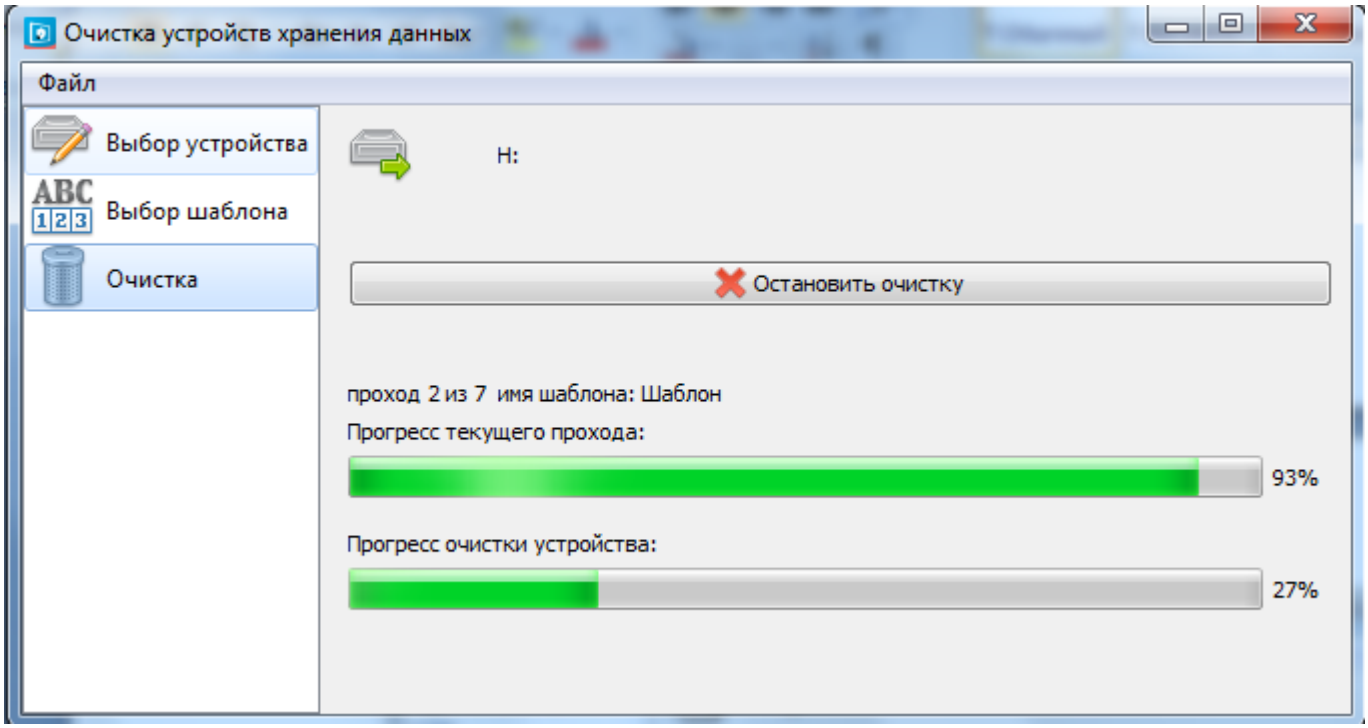


Рис.11.2.5.6. Отражение прогресса процесса очистки устройств

После завершения очистки устройств хранения данных, окно «Очистка устройств хранения данных» примет следующий вид (рис.11.2.5.7):

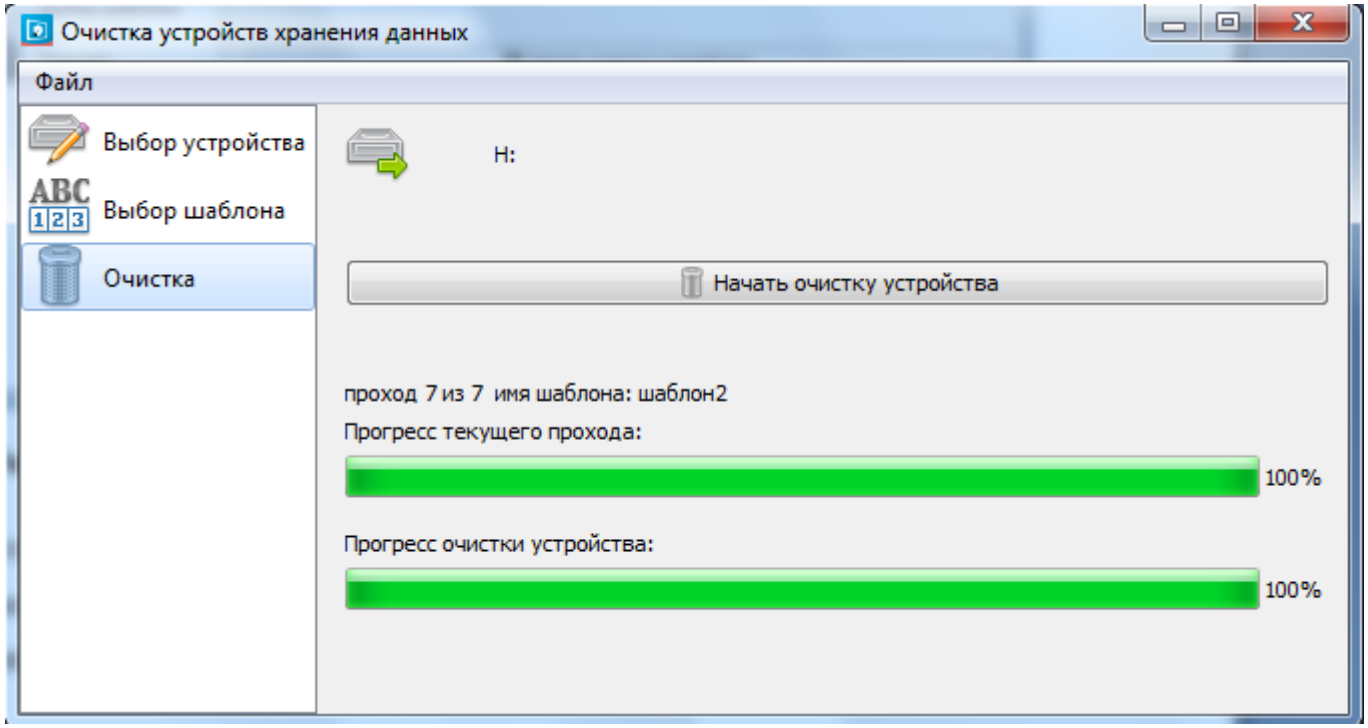


Рис.11.2.5.7. Окончание процесса очистки устройств хранения данных

При очистке флэш накопителей, после очистки их средствами СЗИ «ViPNet SafePoint», для дальнейшего использования устройства, необходимо произвести его форматирование средствами ОС.

11.3. МЕХАНИЗМ ОЧИСТКИ ОЗУ. ИНТЕРФЕЙС

Окно интерфейса механизма очистки ОЗУ представлено на рис.11.3.1. В окне отображается информация о правиле очистки ОЗУ: имя процесса или пользователя, когда происходит очистка ОЗУ (при старте или при завершении сеанса), режим аудита.

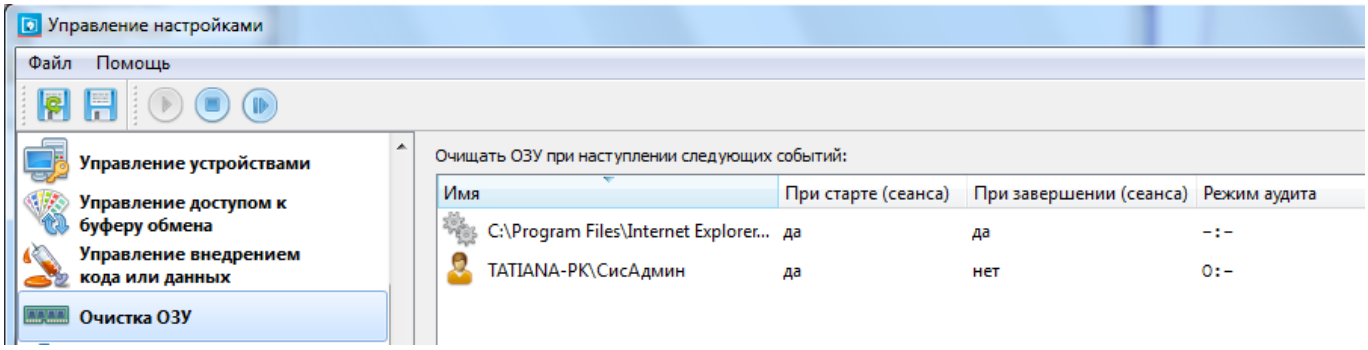


Рис.11.3.1. Интерфейс механизма очистки ОЗУ

Для настройки механизма очистки ОЗУ по событиям, необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Очистка ОЗУ».
2. Нажать правой кнопкой мыши по пустой области интерфейса «Очитка ОЗУ» и в контекстном меню (рис.11.3.2) выбрать «Добавить новое событие «пользователь»» или «Добавить новое событие «процесс»».

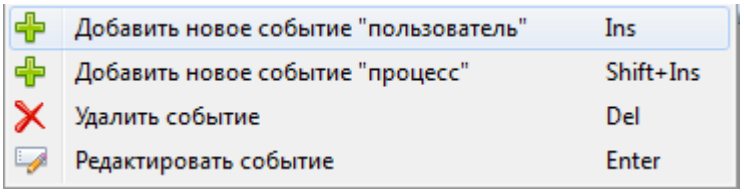


Рис.11.3.2. Контекстное меню окна «Очитка ОЗУ»

3. В появившемся окне «Добавление нового события» (рис.11.3.3) произвести следующие настройки:

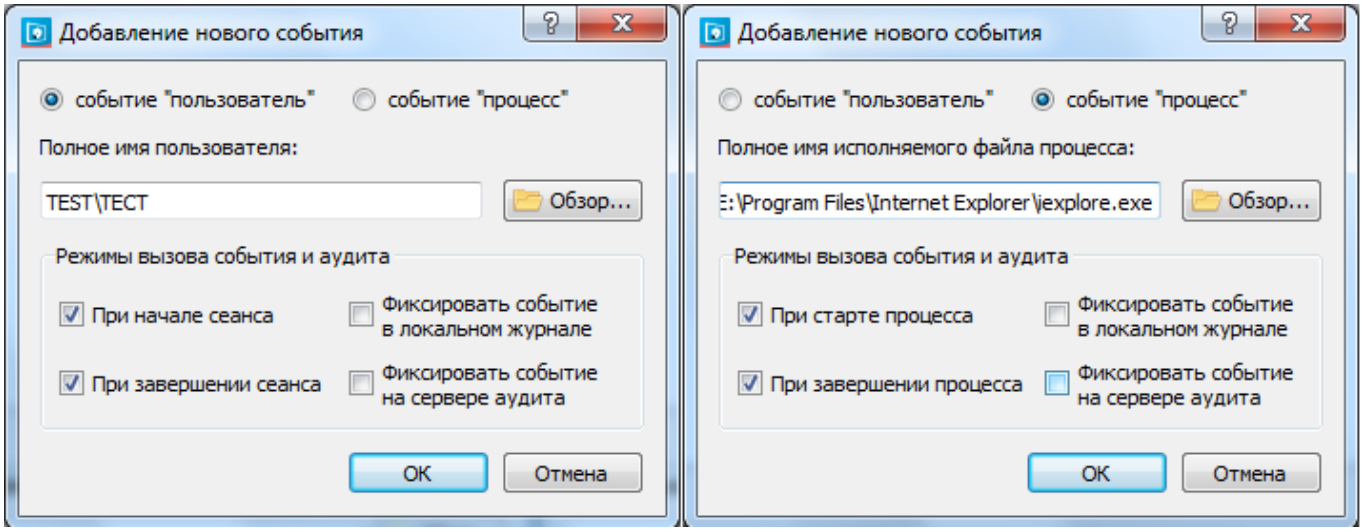


Рис.11.3.3. Окно добавления нового события в случае события «пользователь» и в случае события «процесс»

1) Выбрать тип события «пользователь» или «процесс».
2) Если выбрано событие «пользователь» задать имя пользователя, если выбрано событие «процесс» задать имя исполняемого файла процесса, используя «Обзор» или вручную.

При выборе события «процесс» имя исполняемого файла можно задать с использованием масок.

3) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).
4. Нажать кнопку «ОК».

Для **просмотра** настроек механизма очистки ОЗУ необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Очистка ОЗУ» (рис.11.3.4). В интерфейсе отражается имя события (процесс или пользователь), в какой момент происходит очистка ОЗУ (при старте или при завершении сеанса) и режим аудита. При наведении курсора на имя или режим аудита, появляется всплывающее окно с пояснением.

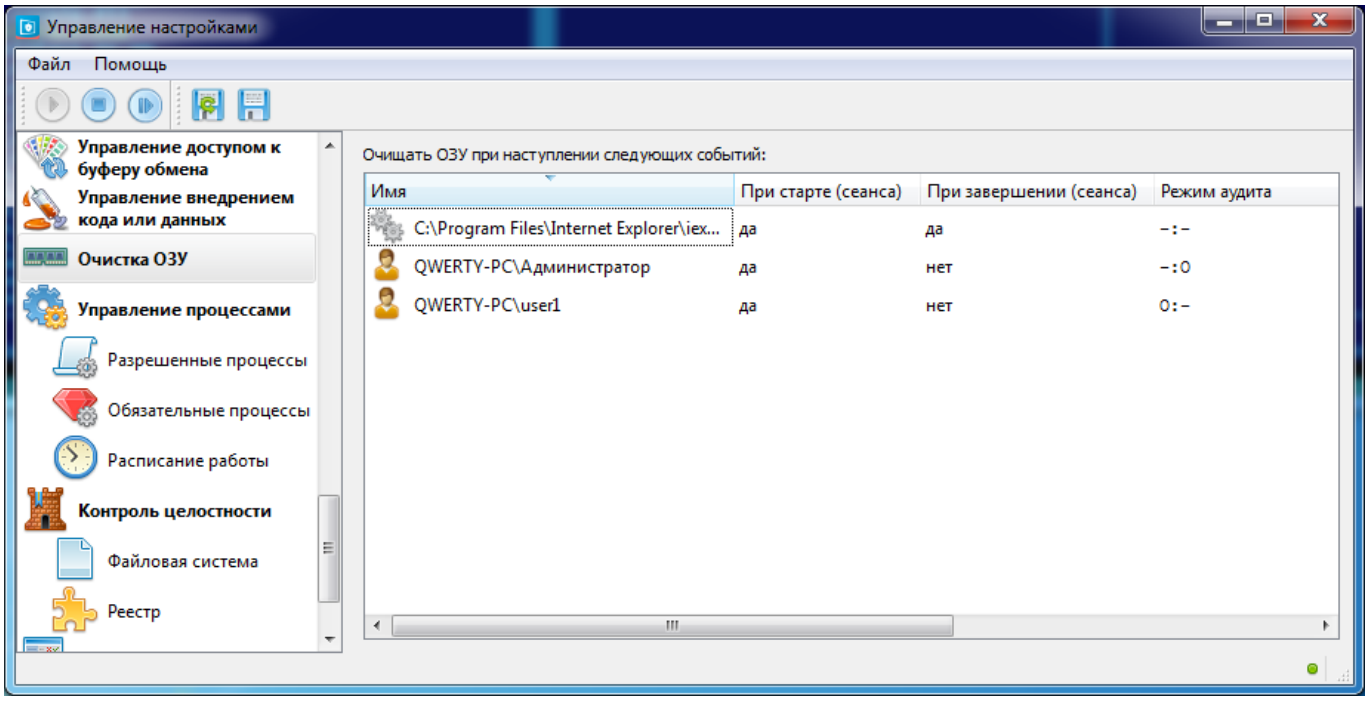


Рис.11.3.4. Интерфейс просмотра настроек механизма очистки ОЗУ

Для **редактирования** или **удаления** правил очистки ОЗУ необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Очистка ОЗУ» выбрать правило и воспользоваться контекстным меню окна (рис.11.3.2), для внесения изменений или удаления правила.

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

12. МЕХАНИЗМ УПРАВЛЕНИЯ ВНЕДРЕНИЕМ КОДА И ДАННЫХ

Механизмом защиты реализуется контроль и разграничение доступа внедрения исполняемого кода и данных в соответствии с заданными правилами.

По умолчанию разрешено внедрение кода и данных субъекту в самого себя.

Учетная информация субъекта при контроле внедрения исполняемого кода и данных задается тремя сущностями: первичный идентификатор пользователя; эффективный идентификатор пользователя; процесс.

В данном механизме защиты в разграничительной политике доступа используются не профили, а именно субъекты доступа, определяемые соответствующими тремя сущностями, т.к. именно в этом случае достигается принципиальное упрощение задачи администрирования.

В отношении, как системы в целом, так и в отношении любого субъекта доступа может быть реализована, как разрешительная (рекомендуемая) – «Все, что явно не разрешено, то запрещено», так и запретительная (вспомогательная) – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа.

Интерфейс механизма представлен на рисунке 12.1.

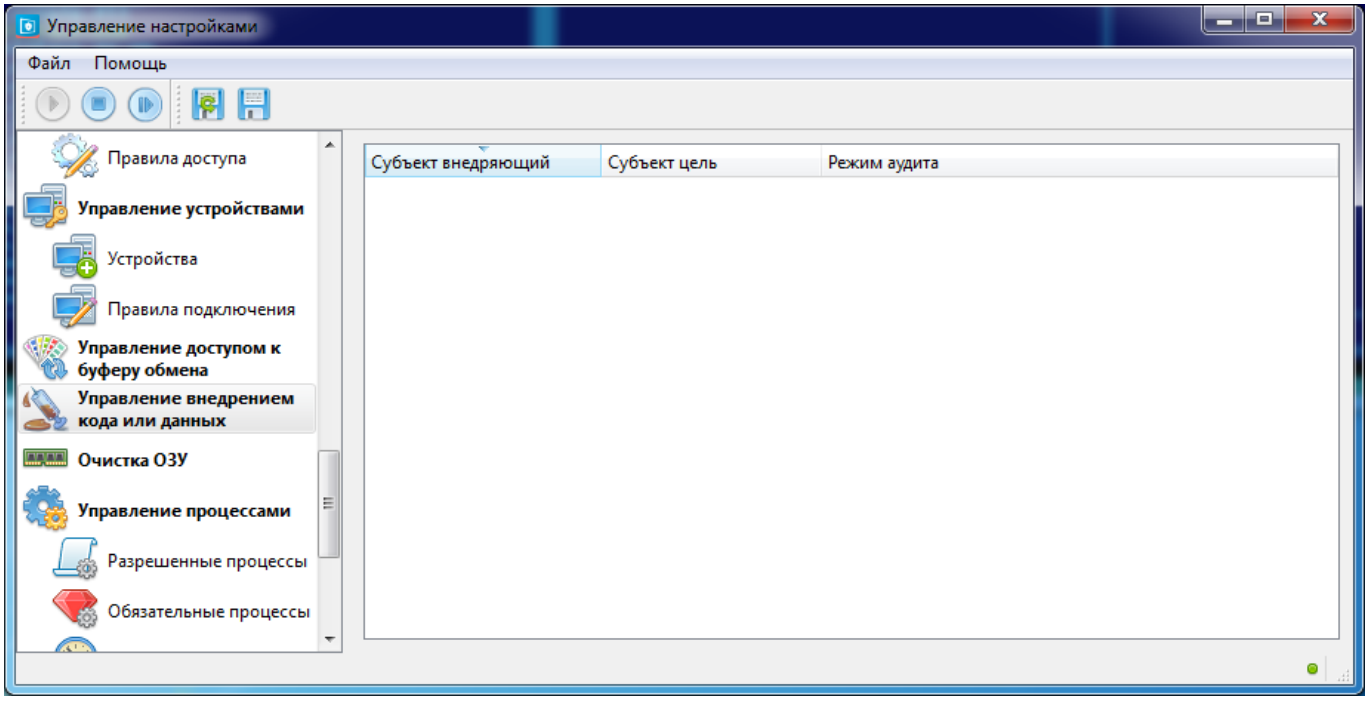


Рис.12.1. Интерфейс механизма управления внедрением кода и данных

Назначение правил управления внедрением исполняемого кода и данных

Сначала необходимо завести субъектов доступа (см. раздел 6.2. Создание, изменение и удаление субъекта доступа), для которых в дальнейшем будут назначены правила управления внедрением исполняемого кода и данных.

Для назначения правил управления внедрением исполняемого кода и данных необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление внедрением кода и данных».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Управление внедрением кода и данных» и в контекстном меню (рис.12.2) выбрать «Добавить правило».

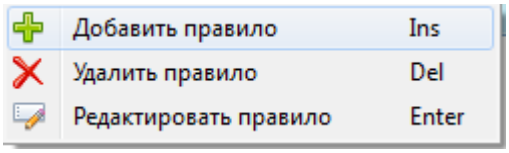


Рис.12.2. Контекстное меню окна «Управление внедрением кода и данных»

3. В появившемся окне «Добавление нового правила» (рис.12.3) произвести следующие настройки:

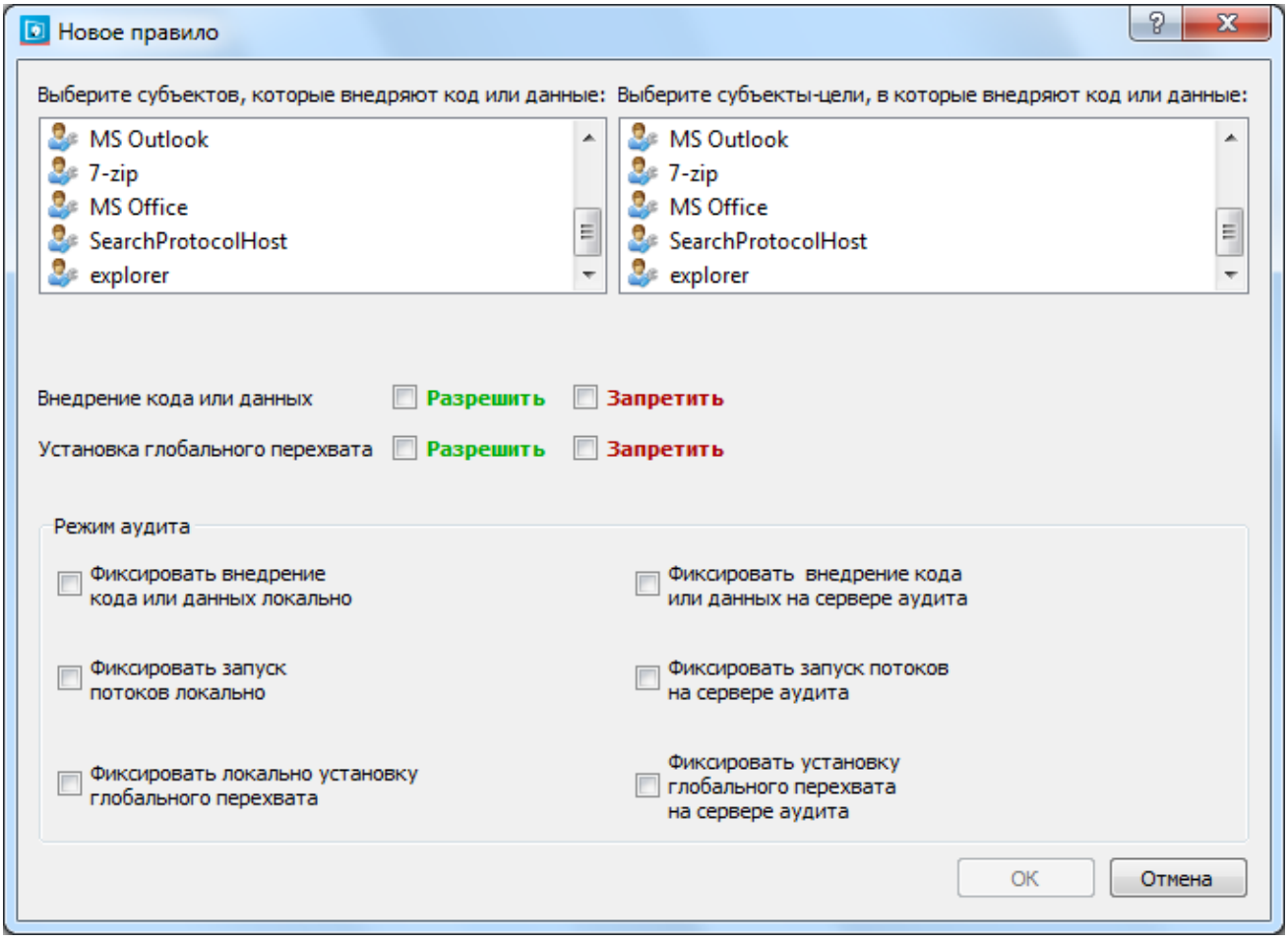


Рис.12.3. Окно добавления нового правила

1) Выбрать субъектов, внедряющих код или данные.

2) Выбрать субъектов, в которые внедряются код или данные.
3) Установить флаг «Запретить» или «Разрешить» для возможности внедрения кода и данных.
4) Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

4. Нажать кнопку «ОК».

Для **просмотра** назначенных правил управления внедрением кода и данных необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление внедрением кода и данных» (рис.12.4). В интерфейсе отражаются внедряющие код или данные субъекты, субъекты-цели и режим аудита.

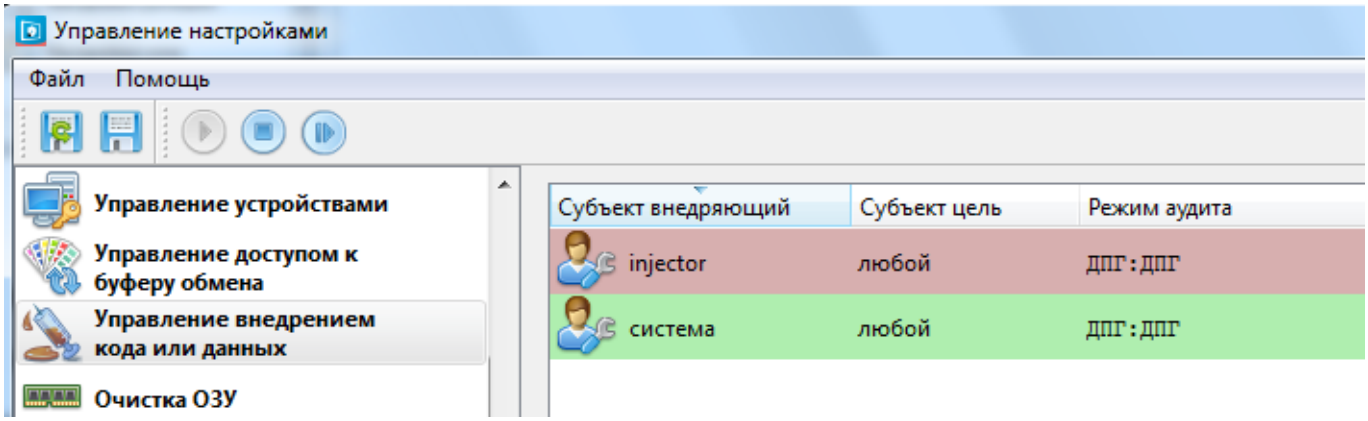


Рис.12.4. Просмотр назначенных правил управления внедрением кода и данных

В интерфейсе разрешающие правила подсвечиваются зеленым, а запрещающие – красным.

Аналогично механизму управления доступом к создаваемым файлам (дискреционное управление доступом), правила могут быть заданы как для отдельных субъектов, так и для нескольких субъектов одновременно.

При задании разрешающего правила и установке режима аудита в журнале аудита «Журнал управления внедрением исполняемого кода и данных» будут отображаться только информационные события. При задании запрещающего правила и установке режима аудита в журнале аудита «Журнал управления внедрением исполняемого кода и данных» будут отображаться только отказы.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления внедрением исполняемого кода и данных».

Для **редактирования** назначенных правил следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление внедрением кода и данных» (рис.12.4) и в контекстном меню выбрать «Изменить», внести нужные изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление внедрением кода и данных» (рис. 12.4) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

14. МЕХАНИЗМ УПРАВЛЕНИЯ ДОСТУПОМ К СЛУЖБАМ WINDOWS

Механизмом защиты реализуется контроль и разграничение доступа к службам Windows в соответствии с заданными правилами.

С правами администратора можно различным способом воздействовать на системные службы. При этом администратор может нарушить работоспособность системы, отключить некоторые ее возможности, в том числе, и возможности защиты, отключить внешние средства защиты, если они не имеют достаточной самозащиты.

СЗИ «ViPNet SafePoint» позволяет контролировать и запрещать реализацию подобных возможностей, которые, в том числе, могут использоваться для реализации атак на средства защиты, используемые совместно с СЗИ «ViPNet SafePoint» – VPN, DLP, антивирусы и т.д.

Интерфейс механизма представлен на рисунке 14.1.

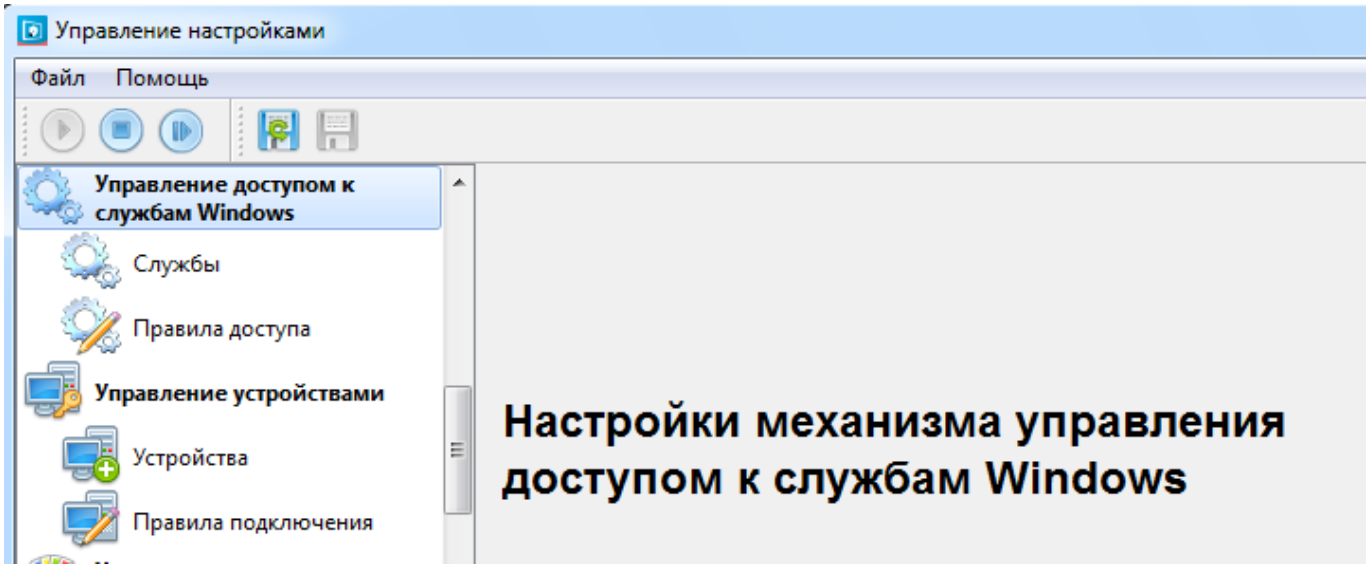


Рис.14.1. Интерфейс механизма управления доступом к службам Windows

Назначение правил управления доступом к службам

Сначала необходимо завести профили доступа (см. раздел 6.3. Создание, редактирование и удаление профиля), для которых в дальнейшем будут назначены правила управления доступом к службам.

Для создания объекта доступа необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к службам Windows» → «Службы».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Службы» в контекстном меню (рис.14.2) выбрать «Добавить службу».

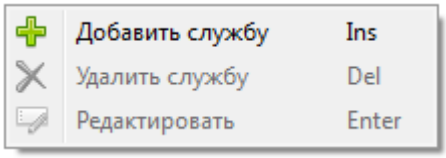


Рис.14.2. Контекстное меню окна управления доступом к службам

3. В появившемся окне «Добавление новой службы» (рис.14.3) произвести следующие настройки.

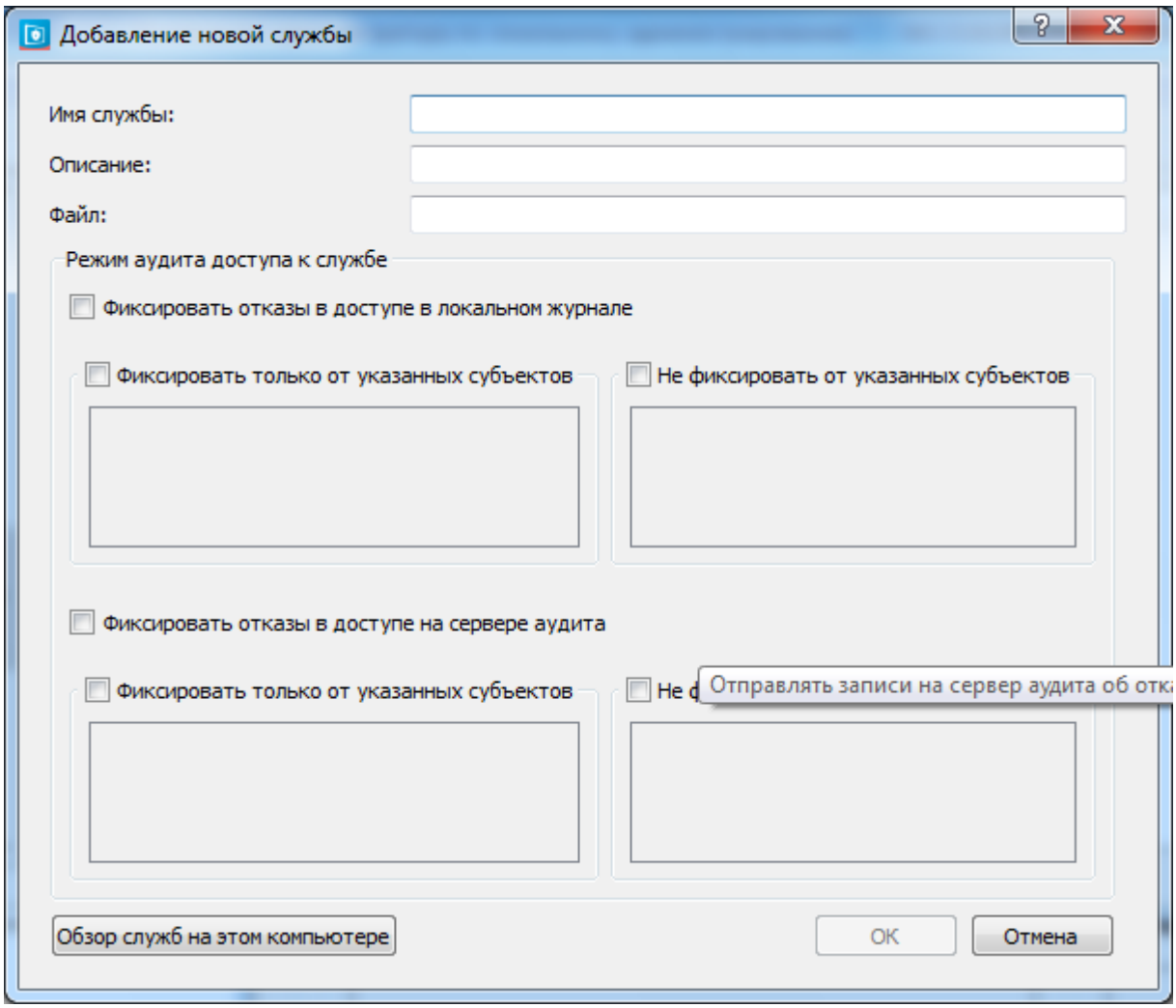


Рис.14.3. Окно создания новой службы

2. Задать службу, используя «Обзор служб на этом компьютере» или задать службу вручную, указав имя и файл (исполняемый модель) службы вручную, путем указания маски или полнопутевого имени.

В обзоре служб будут присутствовать и службы СЗИ «ViPNet SafePoint». Однако задаваемые для них правила будут действовать только в том случае, если будет отключена самозащита.

Для разрешения/запрета создания служб вообще, либо в определенных папках могут использоваться маски (например, «*» везде).

3. Нажать кнопку «ОК».

Для назначения правил управления доступом к службам необходимо:

1. В меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к службам Windows».

2. Нажать правой кнопкой мыши по пустой области интерфейса «Управление доступом к службам Windows» и в контекстном меню (рис.14.4) выбрать «Добавить правило».

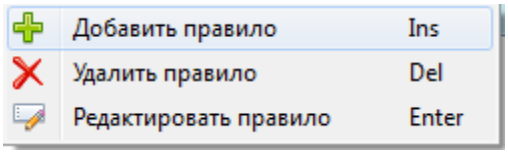


Рис.14.4. Контекстное меню окна «Управление доступом к службам Windows»

3. В появившемся окне «Добавление нового правила» (рис.14.5) произвести следующие настройки:

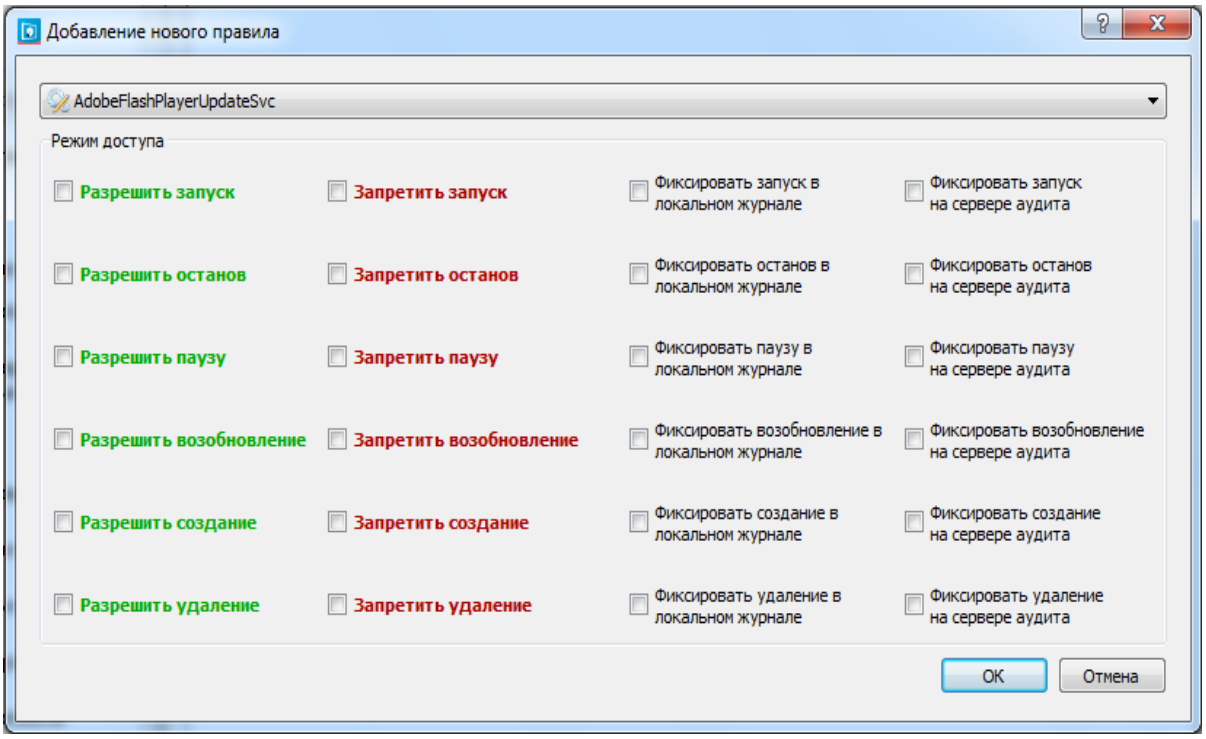


Рис.14.5. Окно добавления нового правила

4. Выбрать службу.

5. Установить флаги «Разрешить запуск» или «Запретить запуск», «Разрешить останов» или «Запретить останов», «Разрешить паузу» или «Запретить паузу», «Разрешить возобновление» или «Запретить возобновление», «Разрешить создание» или «Запретить

создание», «Разрешить удаление» или «Запретить удаление» для возможности модификации выбранной службы.

4. Настроить режим аудита (см. раздел 15.2.4. Аудит событий).

5. Нажать кнопку «ОК».

Для **просмотра** назначенных правил управления доступом к службам необходимо в меню группы настроек механизмов защиты СЗИ «ViPNet SafePoint» выбрать пункт «Управление доступом к службам Windows» (рис.13.1). В интерфейсе для выбранного профиля отражаются службы, режим доступа к ним и режим аудита.

Для **просмотра событий**, связанных с данным механизмом следует открыть в Просмотрщике журналов аудита «Журнал управления доступом к службам».

Для **редактирования** назначенных правил следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление доступом к службам Windows» (рис. 14.1) и в контекстном меню выбрать «Изменить», внести нужные изменения.

Для **удаления** правил доступа следует нажать правой кнопкой мыши по правилу в интерфейсе «Управление доступом к службам Windows» (рис. 14.1) и в контекстном меню выбрать «Удалить».

Для **сохранения** настроек выбрать меню «Файл» → «Сохранить настройки», либо в меню сохранения и загрузки предыдущих настроек нажать кнопку  .

15. АУДИТ

15.1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ

В модели защиты СЗИ «ViPNet SafePoint» предусмотрена реализация следующих возможностей аудита:

- инструментальный аудит;
- интерактивный аудит;
- аудит реального масштаба времени (или реального времени).

Данная классификация реализуемых в СЗИ «ViPNet SafePoint» возможностей аудита основана на классификации задач аудита (назначения аудита), решаемых администратором СЗИ «ViPNet SafePoint», соответственно, на особенностях реализации.

Инструментальный аудит используется на этапе создания разграничительной политики доступа к ресурсам и предназначен для анализа требуемых субъектам, в первую очередь, процессам (приложениям), в том числе, системным процессам, прав доступа к защищаемым ресурсам. Данные права доступа субъектам следует, по возможности (если они не противоречат решаемым задачам защиты), разрешать при реализации разграничительной политики, включая существующую возможность смены имен пользователей (при необходимости запрета, запрещать, но с последующим анализом влияния подобных запретов на корректность функционирования приложения), для обеспечения их корректного функционирования в системе.

Для реализации подобной, крайне важной возможности, предназначенной для построения корректной разграничительной политики доступа к ресурсам, в СЗИ «ViPNet SafePoint» администратором для любого субъекта (субъект определяется соответствующими тремя сущностями, при задании субъекта могут использоваться маски), либо, наоборот, для любого объекта (объект может задаваться масками), или для конкретного субъекта к конкретному объекту, можно выявить, какой доступ запрашивается у системы в процессе ее функционирования, т.е. какие правила доступа следует разрешать в разграничительной политике, считая этот доступ санкционированным. Другими словами, с использованием данной возможности аудита, можно проанализировать работу системы, в том числе, отдельных системных процессов, и приложений, в части реализуемого ими санкционированного доступа к защищаемым ресурсам. С этой целью необходимо разрешить все права доступа соответствующего субъекта к соответствующему объекту (ресурсу), установив для интересующего заданного правила доступа режим аудита. Например, можно установить на аудит запись/чтение процессу интернет-браузера в какой-либо каталог, например, в системный, и посмотреть, обращается ли это приложение к системным файловым объектам, если да, то к каким и с какой целью. Это же можно сделать в отношении права исполнения. Можно посмотреть, какие процессы, в том числе, системные,

олицетворяют себя с правами других пользователей, каких, при доступе к каким объектам. Какие объекты реестра ОС, какими приложениями используются и т.д. В рамках реализации инструментального аудита могут использоваться и запрещения доступа, для которых устанавливается аудит. Можно запретить какие-либо права доступа субъекту к объекту, установив для этих запретов аудит. При выявлении при этом некорректного поведения системы или приложения, по аудиту можно определить, какое заданное правило в разграничительной политике к этому привело. Таким образом, инструментальный аудит – это мощное средство анализа работы системы и приложений, которое может использоваться администратором при создании сложных разграничительных политик доступа к защищаемым ресурсам.

Интерактивный аудит используется уже в процессе эксплуатации защищенной информационной системы (после настройки и ввода в эксплуатацию разграничительной политики доступа к ресурсам, реализуемой механизмами защиты СЗИ «ViPNet SafePoint»). В рамках данного режима аудита администратор имеет возможность регистрировать интересующие его события доступа субъектов к объектам (соответственно, с существующей возможностью задания, как субъектов, так и объектов доступа масками), причем, как несанкционированного, так и санкционированного (не противоречащего заданным правилам). Зафиксированные события сохраняются в журналах аудита (каждым механизмом защиты из состава СЗИ «ViPNet SafePoint» используется собственный журнал аудита), которые могут администратором просматриваться, как локально – из интерфейса клиентской части СЗИ «ViPNet SafePoint», так и удаленно – с сервера безопасности по его запросу. Ввиду потенциальной возможности сбора журналов аудита больших объемов, в помощь администратору в СЗИ «ViPNet SafePoint» реализована мощная система фильтрации журналов (как сквозная для всех журналов, так и локальная – в рамках отдельного журнала), как по любому из регистрируемых параметров, так по любой совокупности регистрируемых параметров. В СЗИ «ViPNet SafePoint» реализована возможность ротации журналов аудита – задания размеров журналов, количество сохраняемых журналов, автоматической очистки (удаления) журналов по задаваемым администратором правилам.

В модели защиты СЗИ «ViPNet SafePoint» предусмотрена возможность сбора и обработки аудита критичных событий в реальном времени. Для критичных регистрируемых аудитом событий (которые в разграничительной политике доступа к ресурсам задаются администратором) принципиальным является оперативность реакции администратора на подобные зарегистрированные события. Как следствие, информация о подобных произошедших в системе событиях должна предоставляться администратору не по его запросу (в интерактивном режиме), а в реальном времени, причем со всех защищаемых СЗИ «ViPNet SafePoint» компьютеров в сети. С этой целью в состав СЗИ «ViPNet SafePoint» включена самостоятельная компонента – сервер

аудита. Те события доступа субъектов к объектам (соответственно, с существующей возможностью задания, как субъектов, так и объектов доступа масками), для которых администратором задается режим регистрации на сервере аудита, в реальном времени передаются клиентской частью СЗИ «ViPNet SafePoint» (в этом режиме аудита, в отличие от интерактивного, администратору не требуется осуществлять какого-либо запроса) на сервер аудита, где автоматически (с указанием адреса или имени компьютера, с которого получено соответствующее сообщение) выводятся в окне сервера аудита, причем в одном окне выводятся соответствующие сообщения, поступающие от различных клиентских частей СЗИ «ViPNet SafePoint». В рамках данного режима аудита администратор в реальном времени уведомляется СЗИ «ViPNet SafePoint» о зафиксированном критичном событии, в отношении которого администратор может оперативно отреагировать, в том числе, некоторые возможности для этого ему предоставляются сервером аудита. Кроме того, в части реализации оперативных реакций на зафиксированное критичное событие, администратор может воспользоваться соответствующими возможностями сервера безопасности.

Таким образом, механизмами аудита СЗИ «ViPNet SafePoint» администратору предоставляются все необходимые ему возможности аудита, связанные, как с вводом СЗИ «ViPNet SafePoint» в эксплуатацию, так с последующей эксплуатацией СЗИ «ViPNet SafePoint».

15.2. НАСТРОЙКА АУДИТА

15.2.1. Аудит входа в систему, идентификации и аутентификации

При настройке механизма идентификации и аутентификации существует возможность редактировать параметры аудита. Для этого следует в меню группы настроек выбрать «Учетные записи» и нажать кнопку «Аудит» в нижнем правом углу. Окно редактирования параметров аудита представлено на рис.15.2.1.1.

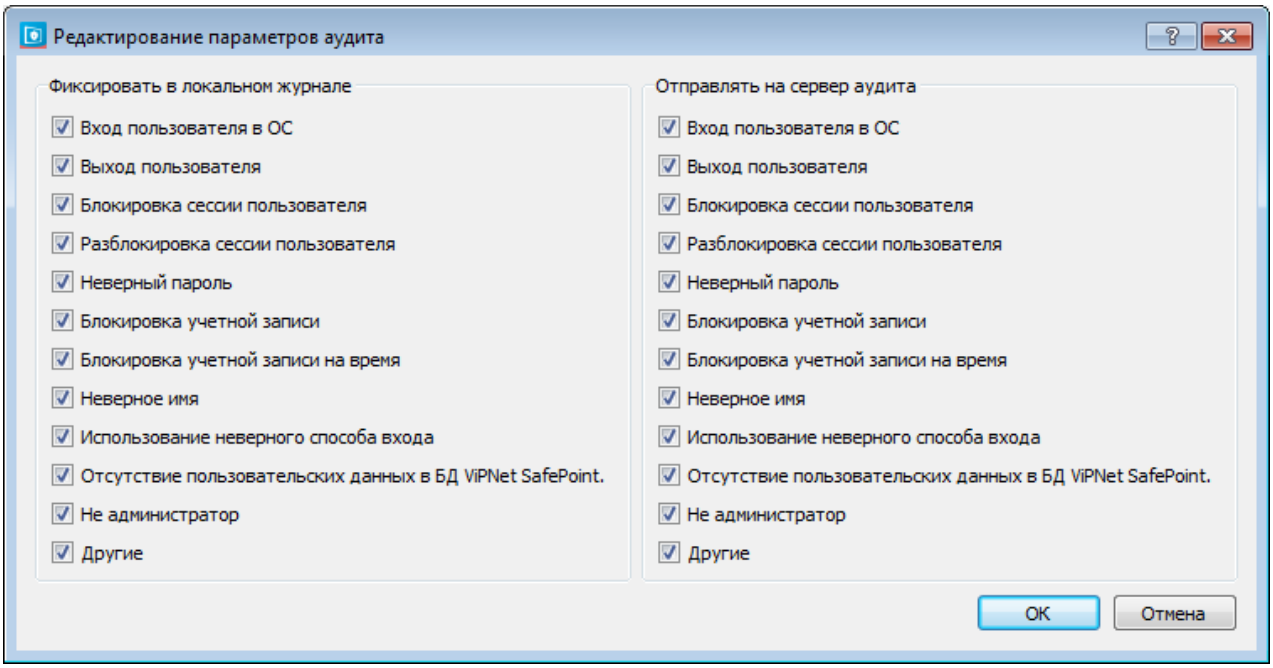


Рис.15.2.1.1. Окно редактирования параметров аудита

Значение флагов в окне редактирования параметров аудита:

Флаг	**Значение**
Вход пользователя в ОС	Фиксирование всех успешных входов в ОС.
Выход пользователя	Фиксирование выходов из ОС.
Блокировка сессии пользователя	Фиксирование блокировки сессии в ОС
Разблокировка сессии пользователя	Фиксирование разблокировки сессии в ОС
Неверный пароль	Фиксирование ошибки входа, вызванного вводом неверного пароля.
Блокировка учетной записи	Фиксирование блокировки учетной записи пользователя по достижении предельного заданного числа попыток входа.
Блокировка учетной записи на время	Фиксирование блокировки учетной записи пользователя на время по достижении предельного заданного числа попыток входа.
Неверное имя	Фиксирование указания неверного или несуществующего имени пользователя при попытке входа в ОС.
Использование неверного способа входа	Фиксирование попытки пользователя войти в ОС с использованием неразрешенного для него типа

	аутентификации.
Отсутствие пользовательских данных	Фиксирование попытки входа в ОС пользователя, который существует в Windows, но отсутствует в базе данных СЗИ.
Не администратор	Фиксирование попытки входа пользователя в Безопасном режиме, которому это не разрешено.
Другие	Фиксирование остальных ошибок входа в ОС.

Все действия, связанные с входом в систему, идентификацией и аутентификацией пользователей фиксируются в соответствующем журнале аудита только при включенной аутентификации средствами СЗИ «ViPNet SafePoint».

15.2.2. Аудит доступа к объектам

При создании объектов доступа в механизмах контроля (разграничений) прав доступа можно задавать режим аудита доступа к объекту, фиксирование отказов в доступе в локальном журнале и на сервер аудита.

Данные настройки идентичны в следующих механизмах:

- Управление доступом к статичным объектам ФС;
- Управление прямым доступом к дискам;
- Управление доступом к реестру;
- Управление доступом к принтерам;
- Управление доступом к создаваемым файлам (вкладка «Аудит доступа к объектам»).

В механизме управления доступом к создаваемым файлам объект задается субъектом создателем объекта, соответственно правила аудита будут применяться ко всем файлам, созданным выбранным субъектом доступа.

При создании объекта доступа в перечисленных механизмах в окне (Рис.15.2.2.1) следует выполнить следующие действия:

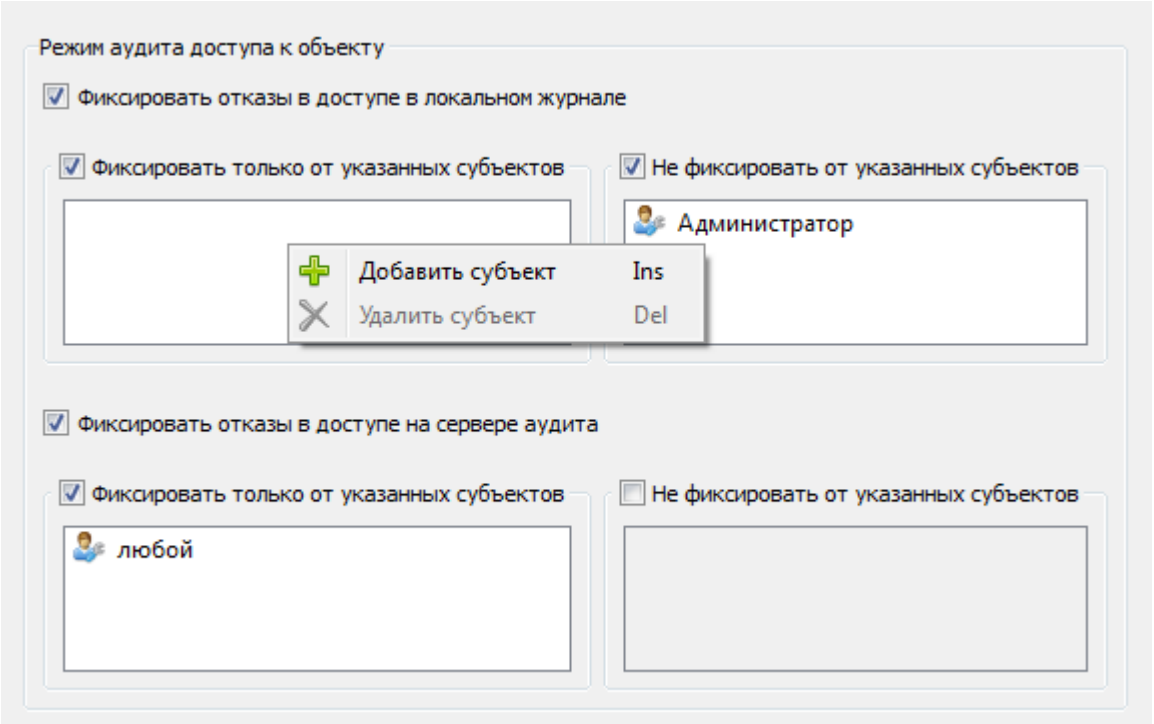


Рис.15.2.2.1 Окно добавления или редактирования объекта доступа

I. **Отказы доступа в локальном журнале:**

- для фиксирования *всех отказов доступа* выбрать флаг «Фиксировать отказы в доступе в локальном журнале».
- для фиксирования отказов в доступе *только от указанных субъектов*:
  1) выбрать флаг «Фиксировать только от указанных субъектов»;
  2) нажать правой кнопки мышь по появившемуся пустому полю и во всплывающем окне выбрать «Добавить субъект»;
  3) в появившемся окне выбрать субъект доступа и нажать «ОК».
- для того чтобы **не** фиксировать отказы в доступе *от указанных субъектов*:
  1) выбрать флаг «Не фиксировать от указанных субъектов»;
  2) нажать правой кнопки мыши по появившемуся пустому полю и во всплывающем окне выбрать «Добавить субъект»;
  3) в появившемся окне выбрать субъект доступа и нажать «ОК».

II. **Отказы доступа на сервере аудита:**

- для фиксирования *всех отказов доступа* выбрать флаг «Фиксировать отказы в доступе на сервере аудита».
- для фиксирования отказов в доступе *только от указанных субъектов*:
  1) выбрать флаг «Фиксировать только от указанных субъектов»;
  2) нажать правой кнопки мыши по появившемуся пустому полю и во всплывающем окне выбрать «Добавить субъект»;

3) в появившемся окне выбрать субъект доступа и нажать «ОК».

- для того чтобы **не** фиксировать отказы в доступе *от указанных субъектов*:
  1) выбрать флаг «Не фиксировать от указанных субъектов»;
  2) нажать правой кнопки мыши по появившемуся пустому полю и во всплывающем окне выбрать «Добавить субъект»;
  3) в появившемся окне выбрать субъект доступа и нажать «ОК».

В СЗИ «ViPNet SafePoint» присутствует возможность добавления одного и того же субъекта доступа в списки «Фиксировать только от указанных субъектов» и «Не фиксировать от указанных субъектов». Данная возможность применима, например, при отладке правил доступа, когда заведено большое количество субъектов и необходимо исключить одного из них, либо в случае, если необходимо на время отключить фиксирование событий одного из субъектов доступа.

15.2.3. Аудит действий субъектов доступа

При создании правил доступа в механизмах контроля (разграничений) прав доступа можно задавать режим аудита действий субъектов доступа.

Настройка заключается в выставлении флага нужного режима аудита. Существует возможность выставить все флаги одновременно. Для этого следует нажать правой клавишей мыши по полю с флагами режимов аудита, появится контекстное меню (рис.15.2.3.1), в котором следует выбрать нужное.

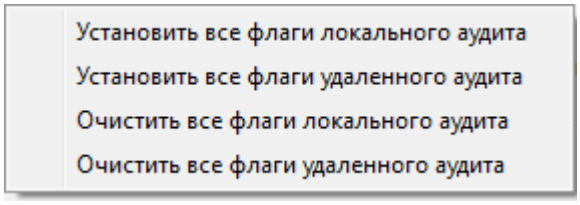


Рис.15.2.3.1. Контекстное меню окна редактирования правил доступа

В механизме *Управление доступом к статичным объектам ФС* в случае создания прав доступа существует возможность фиксировать факт чтения, записи, исполнения, удаления, переименования, также в случае создания правил перенаправления факт перенаправления. Окно редактирования правил представлено на рис.15.2.3.2.

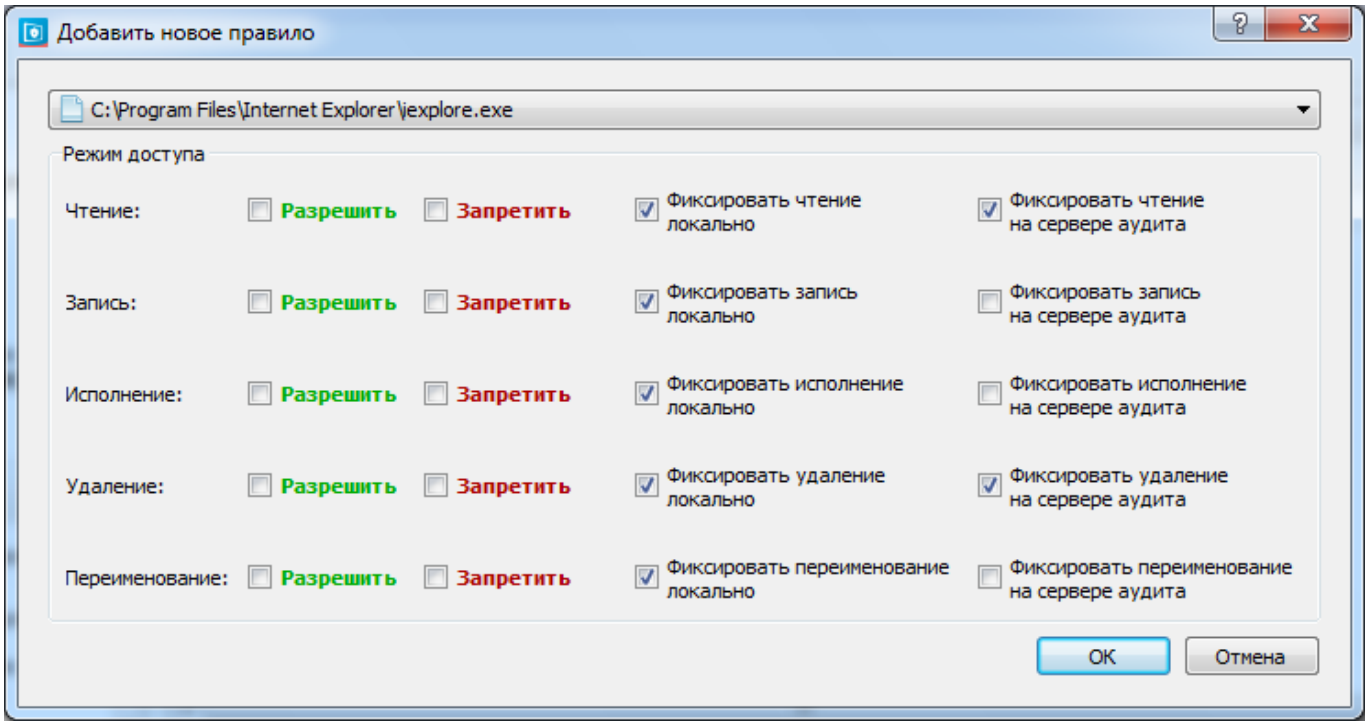


Рис.15.2.3.2. Пример окна редактирования правил

В механизме *Управление доступом к создаваемым файлам* в случае дискреционного управления доступом существует возможность фиксировать факт чтения, записи, удаления, переименования, исполнения, в случае управления доступом на основе меток безопасности существует возможность фиксировать факт чтения, записи и попытки запуска. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

В механизме *Управление прямым доступом к диску* существует возможность фиксировать факт чтения и записи. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

В механизме *Управление доступом к реестру* существует возможность фиксировать факт чтения, записи, удаления, переименования. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

В механизме *Управление доступом к принтерам* существует возможность фиксировать факт подключения принтера. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

В механизме *Управление доступом к службам* существует возможность фиксировать факт запуска, останова, паузы, возобновления, создания и удаления служб Windows. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

В механизме *Управление устройствами* существует возможность фиксировать факт подключения, отключения и управления подключением устройства. Окно редактирования правил аналогично представленному на рис.15.2.3.2.

15.2.4. Аудит событий

В механизмах защиты от скрытых действий пользователей, контроля целостности, очистки ОЗУ существует возможность настроить аудит событий.

Настройка заключается в выставлении флага нужного режима аудита.

В механизме *Управление олицетворением* существует возможность фиксировать отказы в олицетворении локально и на сервере аудита.

В механизме *Очистки ОЗУ* существует возможность фиксировать факт совершения очистки ОЗУ локально и на сервере аудита.

В механизме *Управление процессами* в случае управления разрешенными процессами существует возможность фиксировать события старта и завершения процесса, в случае управления обязательными процессами существует возможность фиксировать события старта и завершения процесса и перезапуска, в случае использования расписания работы процессов существует возможность фиксировать начало и конец работы, факт управлением процессом.

В механизме *Контроля целостности* существует возможность фиксировать факт нарушения целостности, отсутствия копии, восстановления или ошибки восстановления, создания копии или ошибки создания копии.

В механизме *Управления доступом к буферу обмена* существует возможность фиксировать факт помещения информации в буфер обмена, взятия информации из буфера обмена, очистки буфера обмена.

15.3. РАБОТА С ЖУРНАЛАМИ

Журналы аудита имеют два режима отображения:

- с автоматическим переходом на появляющееся в журнале сообщение во время просмотра журнала (установлен флаг «Автоматическая прокрутка»);
- без автоматического перехода на появляющееся в журнале сообщение во время просмотра журнала (не установлен флаг «Автоматическая прокрутка»).

Флаг «Автоматическая прокрутка» устанавливается в контекстном меню каждого журнала (рис.15.3.6).

Для просмотра журналов следует запустить интерфейс «Просмотрщик журналов аудита» из каталога ..\INFOTECS\VIPNET SAFEPOINT\bin\logview.exe.

Интерфейс просмотрщика журналов представлен на рисунке 15.3.1.

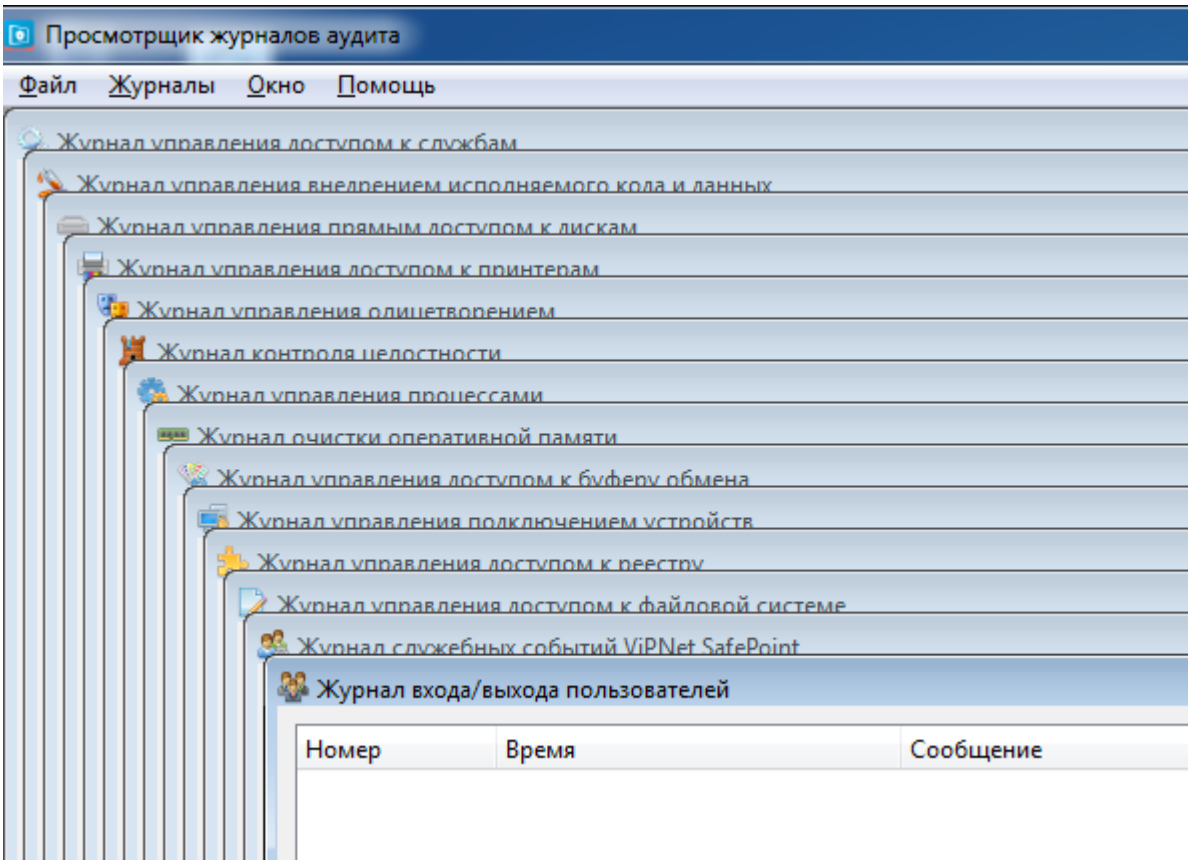


Рис.15.3.1. Интерфейс просмотрщика журналов

Соответствие журналов механизмам СЗИ «ViPNet SafePoint»:

Название механизма	**Название журнала**
Механизмы защиты от скрытых действий пользователей (механизм управления прямым доступом к дискам)	Журнал управления прямым доступом к дискам
Механизм контроля (разграничения) прав доступа (механизм управления доступом к принтерам)	Журнал управления доступом к принтерам
Механизмы защиты от скрытых действий пользователей (механизм управления олицетворением)	Журнал управления олицетворением
Механизмы контроля (механизм контроля целостности объектов файловой системы, объектов реестра и объектов СЗИ «ViPNet SafePoint»)	Журнал контроля целостности
Механизмы контроля (механизм управления процессами)	Журнал управления процессами

Механизмы гарантированного удаления и очистки памяти (механизм очистки ОЗУ)	Журнал очистки оперативной памяти
Механизм управлением монтированием устройств	Журнал управления подключением устройств
Механизм контроля (разграничения) прав доступа (механизм управления доступом к реестру)	Журнал управления доступом к реестру
Механизм контроля (разграничения) прав доступа (механизм управления доступом к статичным объектам ФС и создаваемым файлам)	Журнал управления доступом к файловой системе
Работа ОС и службы	Журнал служебных событий СЗИ «ViPNet SafePoint»
Механизм идентификации и аутентификации пользователя	Журнал входа/выхода пользователей
Механизм управления доступом к буферу обмена	Журнал управления доступом к буферу обмена
Механизм управления внедрением кода и данных	Журнал управления внедрением исполняемого кода и данных
Механизм управления доступом к службам	Журнал управления доступом к службам

Интерфейс просмотрщика журналов содержит следующие пункты:

- Файл;
- Журналы;
- Окно;
- Помощь.

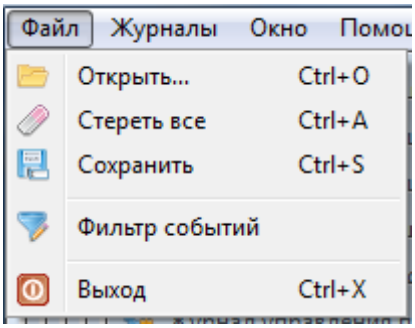


Рис.15.3.2. Меню «Файл»

В **меню «Файл»** существуют возможности:

- Открыть журнал из указанного каталога;

- Стереть все записи из текущего журнала;
- Сохранить текущий журнал;
- Настроить фильтр событий;
- Выйти из просмотрщика журналов.

Чтобы **открыть** журнал из указанного каталога следует:

1. Зайти в меню «Файл».
2. Выбрать пункт «Открыть» или нажать сочетание клавиш «Ctrl» и «O».
3. В появившемся окне выберите файл журналов.
4. Нажать на кнопку «Открыть».

Чтобы **стереть все записи** из открытых журналов следует:

1. Зайти в меню «Файл».
2. Выбрать пункт «Стереть все» или нажать сочетание клавиш «Ctrl» и «A».
3. В появившемся окне «Просмотрщик журналов аудита» нажать «Да».

Чтобы **сохранить** журнал следует:

1. Зайти в меню «Файл».
2. Выбрать пункт «Сохранить» или нажать сочетание клавиш «Ctrl» и «S».
3. В появившемся окне «Сохранить журнал как» выбрать каталог куда сохранить и ввести имя фала журнала.
4. Нажать на кнопку «Сохранить».

В **меню «Журналы»** (рис.15.3.3) существует возможность открыть конкретный журнал, если название журнала неактивно, то данный журнал уже открыт.

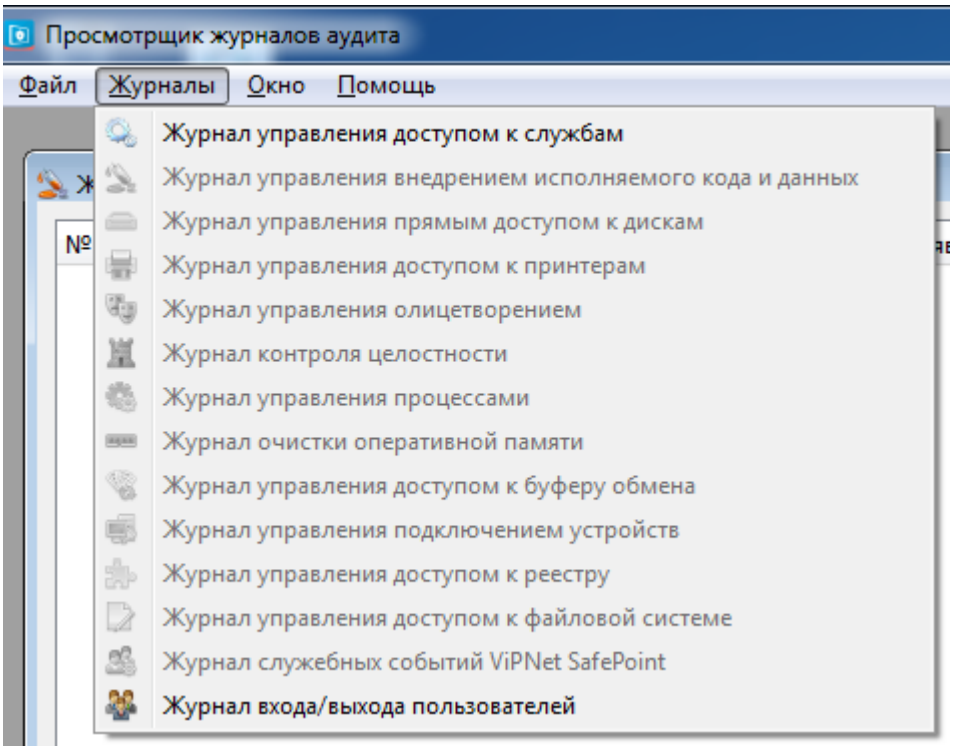


Рис.15.3.3. Меню «Журналы»

В **меню «Окно»** существуют следующие возможности:

- Закрыть текущий журнал или все журналы;
- Выстроить журналы «черепицей» или «каскадом»;
- Переключиться на следующий или предыдущий журнал согласно списку в меню «Журналы»;
- Переключиться к нужному журналу аудита по его названию.

Меню «Окно» представлено на рисунке 15.3.4.

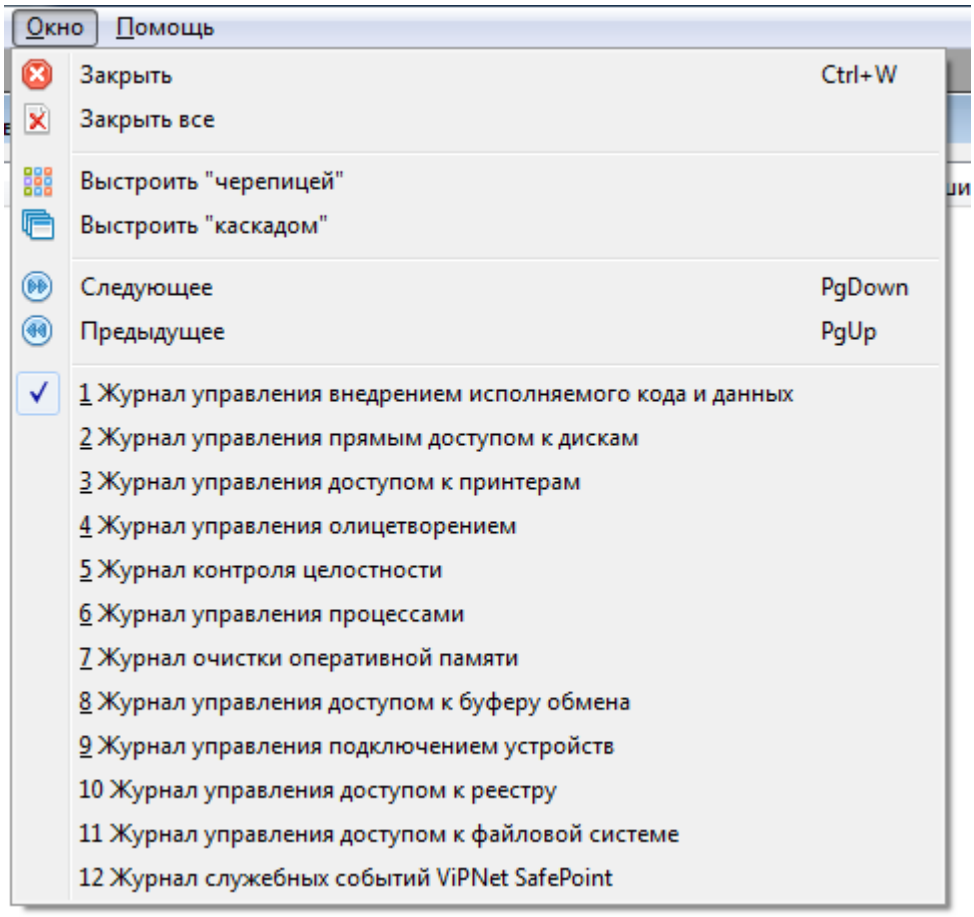


Рис.15.3.4. Меню «Окно»

Для того чтобы **определить очередность построения журналов** следует зайти в основное меню «Окно» и выбрать:

- «Выстроить «черепицей» (рис.15.3.1);
- «Выстроить «каскадом» (рис.15.3.5).

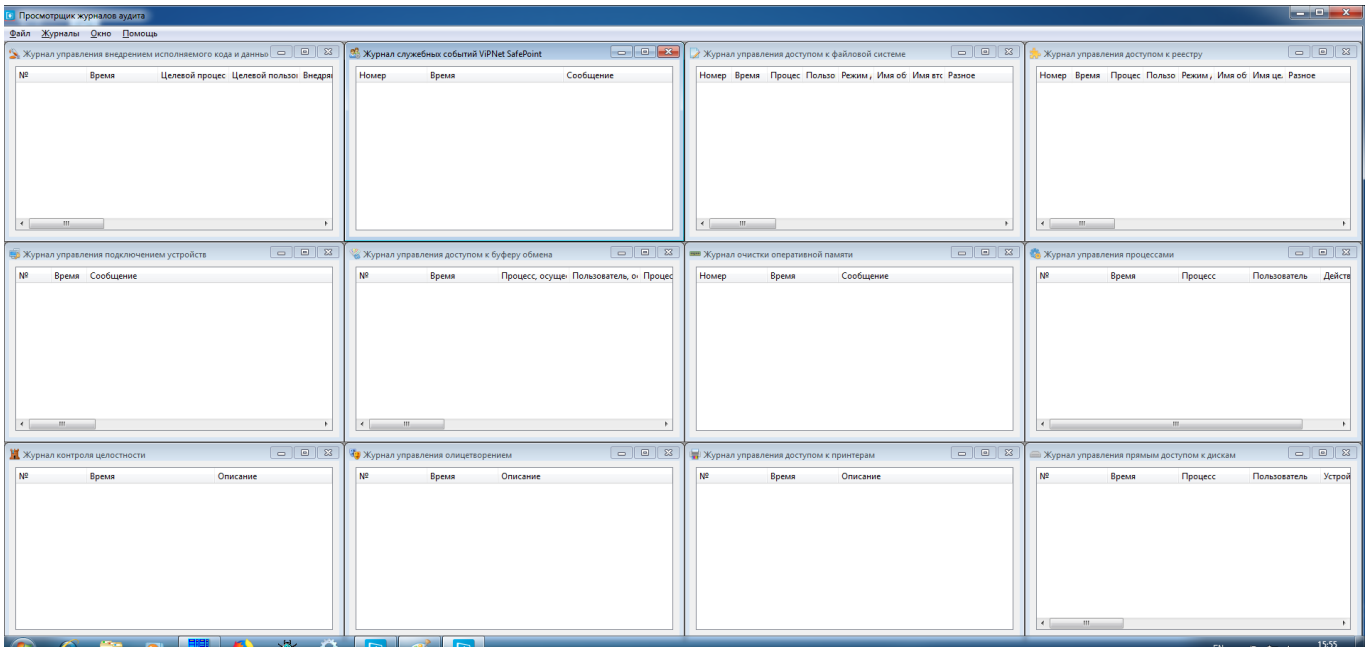


Рис.15.3.5. Отображение журналов «черепицей»

Для **переключения между журналами**:

1. Следует зайти в основное меню «Окно» и выбрать «Следующее» или «Предыдущее»,
2. Для переключения к конкретному журналу следует зайти в меню «Окно» и выбрать нужный вам журнал. Список будет состоять из открытых журналов, в случае если журналы не будут открыты, то список будет неактивен.

Для того чтобы **закрыть все журналы** зайдите в меню «Окно» и выберите «Закрыть все», существует возможность **закрыть конкретный журнал** для этого зайдите в меню «Окно» и выберите «Закрыть», будет закрыт активный журнал.

Журналы аудита в общем случае имеют одинаковый вид (рис.15.3.6). В журнале содержится номер события с иконкой, отображающей его типа, время совершения события и описание события.

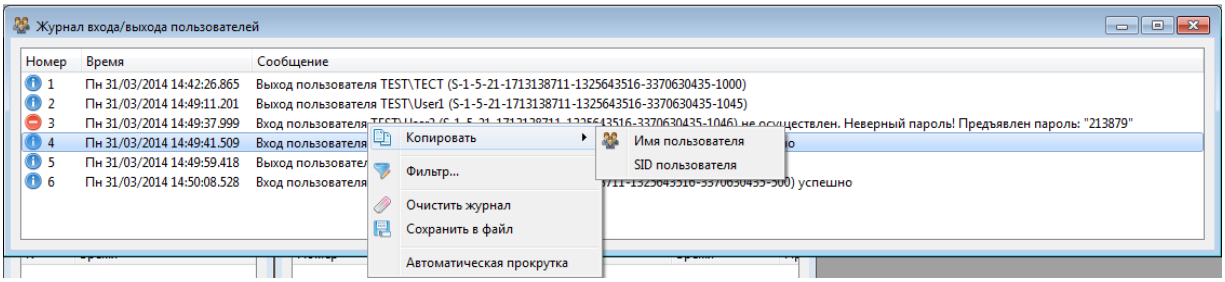


Рис.15.3.6. Пример отображения журнала с контекстным меню

В журналах используются следующие **типы сообщений**:

 информационное сообщение

 сообщение об отказе в доступе

 нарушение целостности

 перенаправление объекта

 пользователи

 процессы

В каждом журнале существует ряд возможностей (рис.15.3.6):

- Скопировать информацию, которую содержит сообщение;
- Открыть меню фильтр;
- Очистить журнал;
- Сохранить журнал в файл;
- Включить/отключить автопрокрутку списка.

В каждом журнале существует возможность **скопировать конкретную информацию**, которая содержится в журнале.

В журнале управления прямым доступом к диску:

- Имя процесса;
- Имя пользователя;
- Имя устройства;
- Идентификатор устройства.

В журнале управления доступом к принтерам:

- Имя процесса;
- Имя пользователя;
- Имя принтера.

В журнале управления олицетворением:

- Имя процесса;
- Имя исходного пользователя;
- Имя целевого пользователя.

В журнале контроля целостности:

- Имя объекта;
- Имя резервной копии.

В журнале управления процессами:

- Имя процесса;
- Имя пользователя.

В журнале очистки оперативной памяти:

- Имя процесса.

В журнале управления подключением устройств:

- Имя устройства;
- Идентификатор класса;
- Идентификатор модели;
- Идентификатор экземпляра.

В журнале управления доступом к реестру и в журнале управления доступом к файловой системе:

- Имя процесса;
- Имя пользователя;
- Имя объекта.

В журнале служебных событий СЗИ «ViPNet SafePoint»:

- Адрес сервера;
- Имя пользователя.

В журнале входа/выхода пользователей:

- Имя пользователя;
- SID Пользователя.

В журнале управления доступом к буферу обмена:

- Имя процесса, осуществляющего доступ;
- Имя пользователя, осуществляющего доступ;
- Имя процесса, поместившего информацию;
- Имя пользователя, поместившего информацию.

В журнале управления внедрением исполняемого кода и данных:

- Имя целевого процесса;
- Имя целевого пользователя;
- Имя процесса, осуществляющего операцию внедрения;
- Имя пользователя, осуществляющего внедрение.

В журнале управления доступом к службам:

- Имя процесса;
- Имя пользователя;

- Имя службы.

15.4. РЕДАКТИРОВАНИЕ ФИЛЬТРОВ

Строки в журналах безопасности могут быть отфильтрованы при помощи:

1. Общего фильтра для всех журналов (основное меню «Файл» → «Фильтр событий»). Данный фильтр предназначен для фильтрации записей одновременно по всем журналам. Автоматически заполняется только список пользователей во вкладке «Пользователь», списки процессов и объектов во вкладках «Процесс» и «Объект» заполняются вручную. Записи будут отображаться в журналах аудита в том случае, если они подходят по всем параметрам, заданным в фильтре. Редактирование общего фильтра описано в разделе 15.4.1.

2. Частного фильтра отдельного журнала. Фильтры предназначены для фильтрации записей конкретного журнала аудита. Для удобства работы с журналами в фильтрах будут отображаться те объекты, пользователи, процессы, порты, службы и т.д., информация о которых присутствует в данном журнале. Редактирование частных фильтров журналов аудита описано в разделе 15.4.2.

15.4.1. Редактирование общего фильтра

Для **редактирования общего фильтра**, необходимо:

1. Открыть в главном меню «Файл», далее «Фильтр событий».

Во вкладке **«Общие»** существует возможность выбрать вид сообщения, которые должны быть выведены (рис.15.4.1.1):

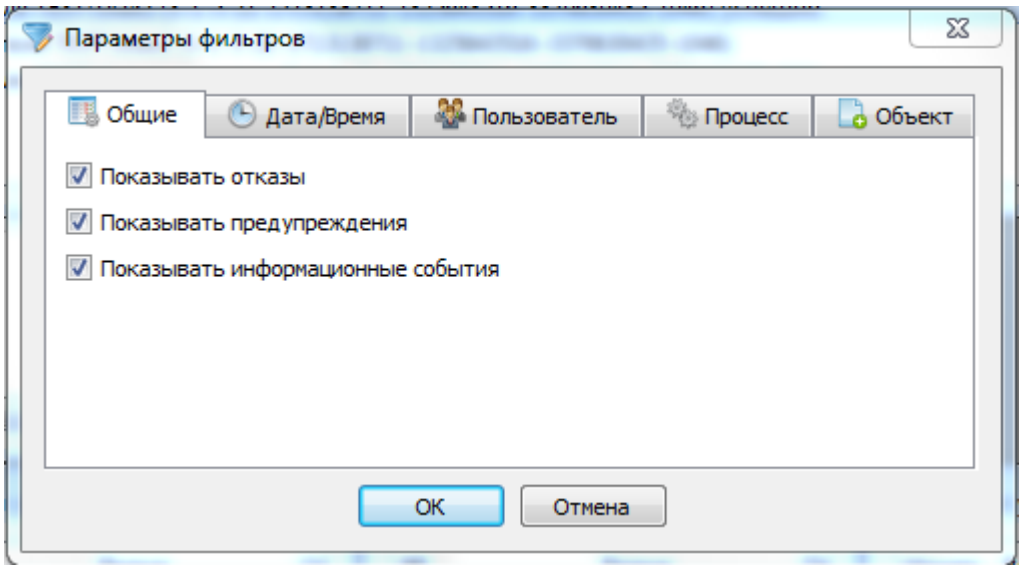


Рис.15.4.1.1. Окно параметров фильтра, меню «Общие»

В меню **«Дата/Время»** для использования данного фильтра следует:

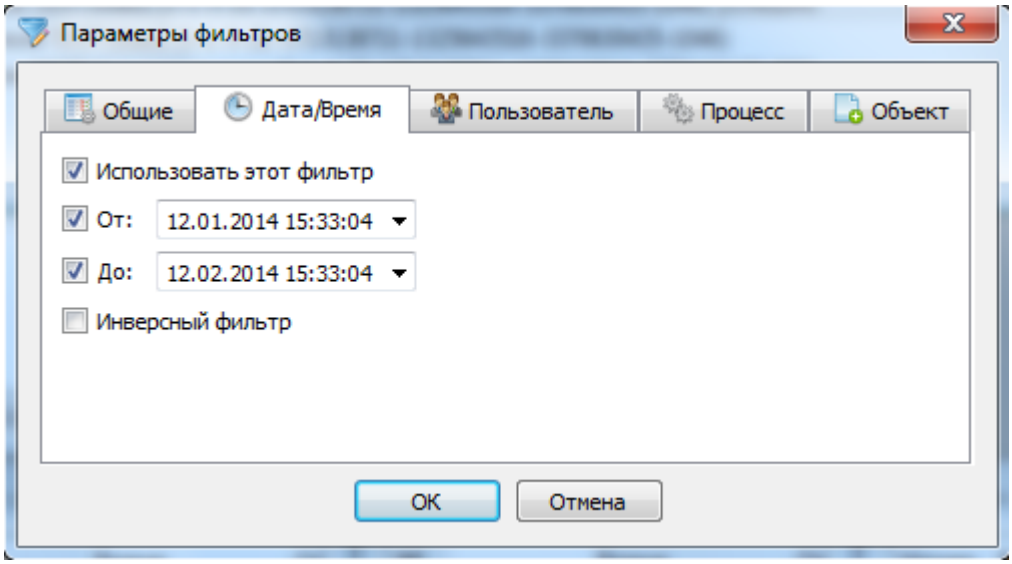


Рис.15.4.1.2. Окно параметров фильтра, меню «Дата/Время»

1. Установить флаг «Использовать этот фильтр».
2. Установить период времени «От» и «До».
3. В случае если требуется исключить данный промежуток времени, следует установить флаг «Инверсный фильтр».

В меню **«Пользователь»** для использования данного фильтра следует:

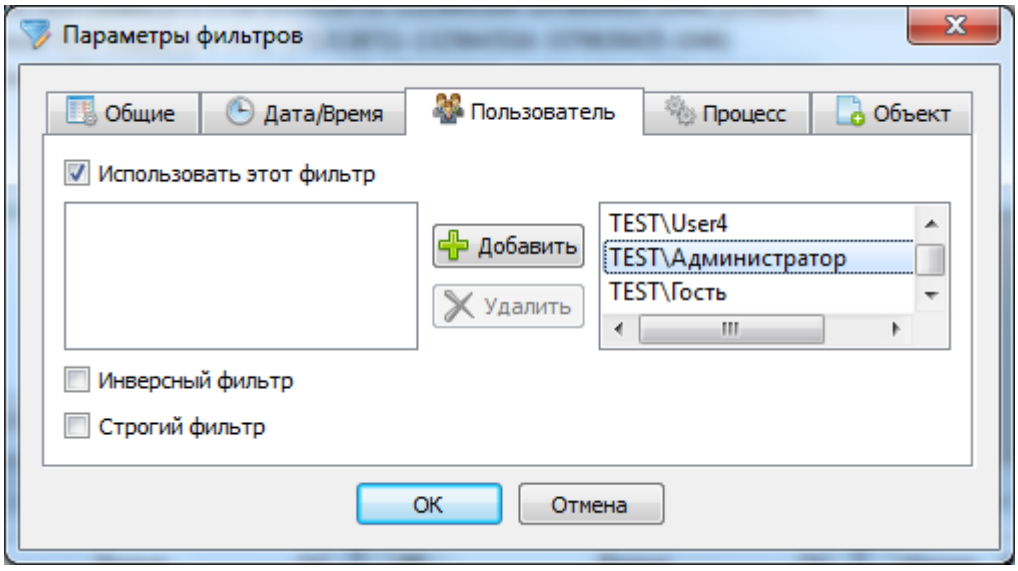


Рис.15.4.1.3. Окно параметров фильтра, меню «Пользователь»

1. Установить флаг «Использовать этот фильтр».
2. В правом поле будет список пользователей, из которого следует выбрать нужных и нажать кнопку «Добавить», возможен выбор нескольких пользователей при зажатой клавише «Ctrl».
3. В случае если требуется исключить данных пользователей, следует установить флаг «Инверсный фильтр».

4. В случае, когда требуется строго соответствовать данному списку, следует установить флаг «Строгий фильтр».

Для **удаления** пользователя из списка следует:

1. Выделить пользователя.
2. Нажать кнопку «Удалить».

В меню **«Процесс»** для использования данного фильтра следует:

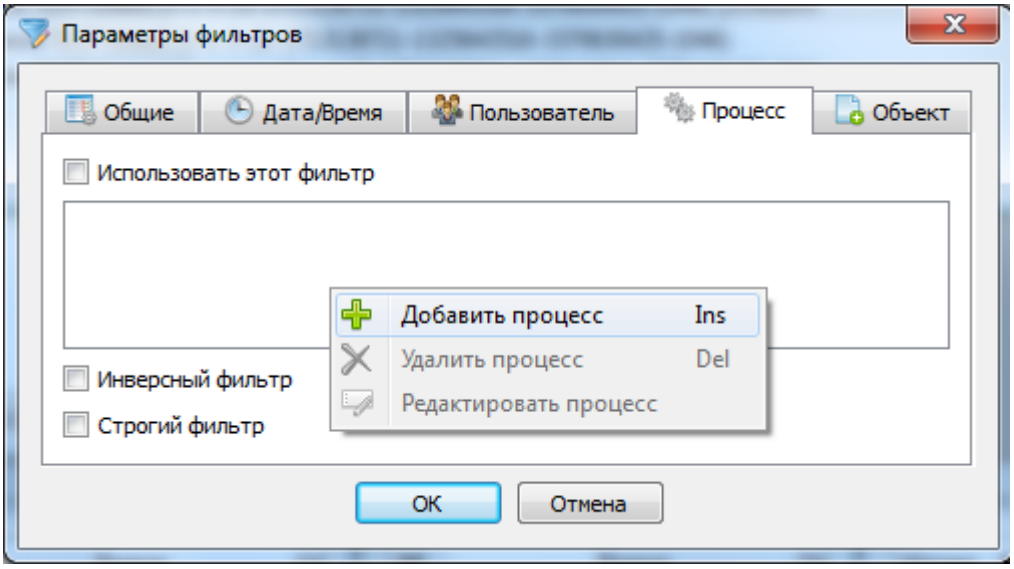


Рис.15.4.1.4. Окно параметров фильтра, меню «Процесс»

1. Установить флаг «Использовать этот фильтр».
2. Нажать правой клавишей мыши и выбрать «Добавить процесс» или нажать клавишу «Ins».
3. В появившемся окне «Новый процесс» ввести полное имя процесса или маску и нажать «ОК».
4. В случае если требуется исключить указанные процессы, следует установить флаг «Инверсный фильтр».
5. В случае, когда требуется строго соответствовать данному списку, следует установить флаг «Строгий фильтр».

Для **удаления** процесса из списка следует:

1. Выделить имя процесса.
2. Нажать правой клавишей мыши по процессу и выбрать «Удалить процесс» или нажать клавишу «Del».

Для **редактирования** процесса следует:

1. Выделить имя процесса.
2. Нажать правой клавишей мыши по процессу и выбрать «Редактировать процесс».
3. Изменить путь или имя процесса.

В меню **«Объект»** для использования данного фильтра следует:

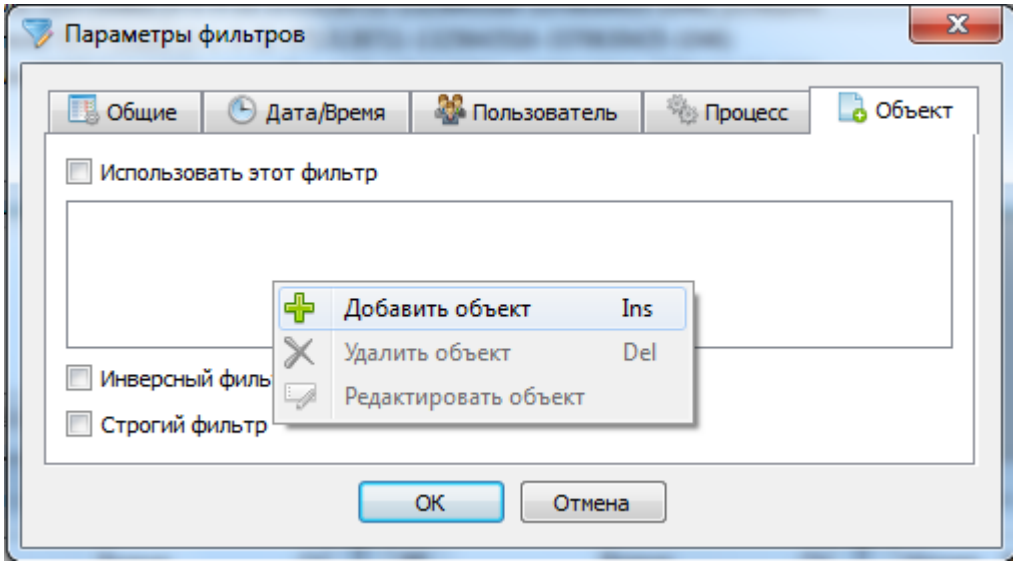


Рис.15.4.1.5. Окно параметров фильтра, меню «Объект»

1. Установить флаг «Использовать этот фильтр».
2. Нажать правой клавишей мыши и выбрать «Добавить объект» или нажать клавишу «Ins».
3. В появившемся окне «Новый объект» ввести полное имя объекта или маску и нажать кнопку «ОК».
4. В случае если требуется исключить указанные объекты, следует установить флаг «Инверсный фильтр».
5. В случае, когда требуется строго соответствовать данному списку, следует установить флаг «Строгий фильтр».

Для удаления объекта из списка:

1. Выделить имя объекта.
2. Нажать правой клавишей мыши по процессу и выбрать «Удалить объект» или нажать клавишу «Del».

Для редактирования объекта:

1. Выделить имя объекта.
2. Нажать правой клавишей мыши по процессу и выбрать «Редактировать объект».
3. Изменить путь или имя объекта.

15.4.2. Редактирование фильтра отдельного журнала

Для редактирования фильтра конкретного журнала, необходимо:

1. В окне любого журнала нажать правой кнопкой мыши по событию.
2. В появившемся контекстном меню выбрать «Фильтр событий».

Далее следует выполнять действия в зависимости от журнала.

15.4.2.1. Журнал управления доступом к файловой системе

В «Журнале управлением доступом к файловой системе» в «Фильтре событий ФС»:

- Настройка фильтра ***«Доступ»***:
  1. В появившемся окне «Фильтр событий ФС» перейти во вкладку «Доступ».
  2. Установить необходимые флаги для желаемого отображения записей (чтение, запись, исполнение, удаление, переименование).
  3. Нажать кнопку «ОК».
- Настройка фильтра ***«Процесс»***:
  1. В появившемся окне «Фильтр событий ФС» перейти во вкладку «Процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левая кнопка мыши.
  3. Установить флаг «Фильтровать события по имени процесса».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий ФС» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левая кнопка мыши.
  3. Установить флаг «Фильтровать события по пользователям».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра ***«Объект»***:
  1. В появившемся окне «Фильтр событий ФС» перейти во вкладку «Объект».
  2. Выделить необходимый объект или объекты путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтр события по имени объекта».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра ***«По времени»***:
  1. В появившемся окне «Фильтр событий ФС» снять флаг «показывать все строки»
  2. Установить значение.
  3. Нажать кнопку «ОК».

Если при включенном фильтре «По времени» открыть окно «Фильтр событий ФС» и нажать «Отмена», фильтр автоматически выключится.

15.4.2.2. Журнал входа/выхода пользователей

В «Журнале входа/выхода пользователей» в «Фильтре событий регистрации пользователей»:

- Настройка фильтра ***«События»***:
  1. В появившемся окне «Фильтр событий регистрации пользователей» перейти во вкладку «События».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий регистрации пользователей» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации «Ctrl»+левая кнопка мыши.
  3. Установить флаг «Фильтровать события по пользователям».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.3. Журнал управления подключением устройств

В «Журнале управления подключением устройств» в «Фильтре событий подключения устройств»:

- Настройка фильтра события ***«Доступ»***:
  1. Нажать правой кнопкой мыши по любой записи в «Журнале управления подключением устройств».
  2. В выпадающем меню выбрать строку «Фильтр».
  3. В появившемся окне «Фильтр событий подключения устройств» перейти во вкладку «Доступ».
  4. Установить необходимые флаги для желаемого отображения записей.
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Имя»***:

1. Нажать правой кнопкой мыши по любой записи в «Журнале управления подключением устройств».
2. В выпадающем меню выбрать строку «Фильтр».
3. В появившемся окне «Фильтр событий подключения устройств» перейти во вкладку «Имя».
4. Выделить необходимое имя или имена путем одновременной комбинации Ctrl+левая кнопка мыши.
5. Установить флаг «Фильтровать события по имени устройства».
6. Установить при необходимости флаг «Инверсия фильтра».
7. Нажать кнопку «ОК».

- Настройка фильтра события ***«Экземпляр»***:
  1. В появившемся окне «Фильтр событий подключения устройств» перейти во вкладку «Экземпляр».
  2. Выделить необходимый экземпляр или экземпляры путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по идентификатору экземпляра устройства».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.4. Журнал контроля целостности

В «Журнале контроля целостности» в «Фильтре событий контроля целостности»:

- Настройка фильтра ***«События»***:
  1. В появившемся окне «Фильтр событий контроля целостности» перейти во вкладку «События».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Объект»***:
  1. В появившемся окне «Фильтр событий контроля целостности» перейти во вкладку «Объект».
  2. Выделить необходимый объект или объекты путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени объекта».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.5. Журнал управления прямым доступом к дискам

В «Журнале управления прямым доступом к дискам» в «Фильтре событий прямого доступа к дискам»:

- Настройка фильтра события ***«Доступ»***:
    1. В появившемся окне «Фильтр событий прямого доступа к дискам» перейти во вкладку «Доступ».
    2. Установить необходимые флаги для желаемого отображения записей.
    3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь»***:
    1. В появившемся окне «Фильтр событий прямого доступа к дискам» перейти во вкладку «Пользователь».
    2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
    3. Установить флаг «Фильтровать события по пользователям».
    4. Установить при необходимости флаг «Инверсия фильтра».
    5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Устройство»***:
    1. В появившемся окне «Фильтр событий прямого доступа к дискам» перейти во вкладку «Устройство».
    2. Выделить необходимое устройство или устройства путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
    3. Установить флаг «Фильтровать события по имени устройства».
    4. Установить при необходимости флаг «Инверсия фильтра».
    5. Нажать кнопку «ОК».

15.4.2.6. Журнал управления доступом к принтерам

В «Журнале управления доступом к принтерам» в «Фильтре событий печати»:

- Настройка фильтра события ***«Доступ»***:
    1. В появившемся окне «Фильтр событий печати» перейти во вкладку «Доступ».
    2. Установить необходимые флаги для желаемого отображения записей.
    3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс»***:
    1. В появившемся окне «Фильтр событий печати» перейти во вкладку «Процесс».

2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени процесса».
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий печати» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по пользователям».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Принтер»***:
  1. В появившемся окне «Фильтр событий печати» перейти во вкладку «Принтер».
  2. Выделить необходимое устройство или устройства путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени принтера».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.7. Журнал очистки оперативной памяти

В «Журнале очистки оперативной памяти» в «Фильтре событий очистки оперативной памяти»:

- Настройка фильтра события ***«Тип»***:
  1. В появившемся окне «Фильтр событий очистки оперативной памяти» перейти во вкладку «Тип».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс»***:
  1. В появившемся окне «Фильтр событий очистки оперативной памяти» перейти во вкладку «Процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса».

4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий очистки оперативной памяти» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени пользователя».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.8. Журнал управления процессами

В «Журнале управления процессами» в «Фильтре событий управления процессами»:

- Настройка фильтра ***«События»***:
  1. В появившемся окне «Фильтр событий управления процессами» перейти во вкладку «События».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс»***:
  1. В появившемся окне «Фильтр событий управления процессами» перейти во вкладку «Процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий управления процессами» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по пользователям».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.9. Журнал управления доступом к реестру

В «Журнале управления доступом к реестру» в «Фильтре событий доступа к реестру»:

- Настройка фильтра события ***«Доступ»***:
  1. В появившемся окне «Фильтр событий доступа к реестру» перейти во вкладку «Доступ».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс»***:
  1. В появившемся окне «Фильтр событий доступа к реестру» перейти во вкладку «Процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр событий доступа к реестру» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по пользователям».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Объект»***:
  1. В появившемся окне «Фильтр событий доступа к реестру» перейти во вкладку «Объект».
  2. Выделить необходимый объект или объекты путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени объекта».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра ***«По времени»***:
  1. В появившемся окне «Фильтр событий ФС» снять флаг «показывать все строки»

2. Установить значение.
3. Нажать кнопку «ОК».

Если при включенном фильтре «По времени» открыть окно «Фильтр событий ФС» и нажать «Отмена», фильтр автоматически выключится.

15.4.2.10. Журнал управления олицетворением

В «Журнале управления олицетворением» в «Фильтре событий олицетворения»:

- Настройка фильтра события ***«Доступ»***:
  1. В появившемся окне «Фильтр событий олицетворения» перейти во вкладку «Доступ».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс»***:
  1. В появившемся окне «Фильтр событий олицетворения» перейти во вкладку «Процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«ИЗ пользователя»***:
  1. В появившемся окне «Фильтр событий олицетворения» перейти во вкладку «ИЗ пользователя».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени исходного пользователя»
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«В пользователя»***:
  1. В появившемся окне «Фильтр событий олицетворения» перейти во вкладку «В пользователя».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени целевого пользователя».

4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

15.4.2.11. Журнал служебных событий СЗИ «ViPNet SafePoint»

В «Журнале служебных событий СЗИ «ViPNet SafePoint» в «Фильтре служебных событий ViPNet SafePoint»:

- Настройка фильтра события ***«Тип»***:
  1. В появившемся окне «Фильтр служебных событий СЗИ «ViPNet SafePoint» перейти во вкладку «Тип».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Сервер»***:
  1. В появившемся окне «Фильтр служебных событий СЗИ «ViPNet SafePoint» перейти во вкладку «Сервер».
  2. Выделить необходимый IP-адрес сервера или серверов путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по адресу сервера».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь»***:
  1. В появившемся окне «Фильтр служебных событий СЗИ «ViPNet SafePoint» перейти во вкладку «Пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени пользователя»
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».

15.4.2.12. Журнал управления доступом к буферу обмена

В «Журнале управления доступом к буферу обмена» в «Фильтре событий доступа к буферу обмена»:

- Настройка фильтра события ***«Доступ»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Доступ».

2. Установить необходимые флаги для желаемого отображения записей.
3. Нажать кнопку «ОК».

- Настройка фильтра события ***«Процесс, осуществляющий доступ»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Процесс, осуществляющий доступ».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса, осуществляющего доступ».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь, осуществляющий доступ»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Пользователь, осуществляющий доступ».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени пользователя, осуществлявшего доступ»
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Процесс, поместивший информацию в буфер обмена»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Процесс, поместивший информацию в буфер обмена».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса, поместившего информацию в буфер обмена».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Пользователь, поместивший информацию в буфер обмена»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Пользователь, поместивший информацию в буфер обмена».

2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени пользователя, поместившего информацию в буфер обмена»
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

15.4.2.13. Журнал управления внедрением исполняемого кода и данных

В «Журнале управления внедрением исполняемого кода и данных» в «Фильтре событий внедрения кода и данных»:

- Настройка фильтра события ***«Доступ»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Доступ».
  2. Установить необходимые флаги для желаемого отображения записей.
  3. Нажать кнопку «ОК».
- Настройка фильтра события ***«Целевой процесс»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Целевой процесс».
  2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени процесса, осуществляющего доступ».
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Целевой пользователь»***:
  1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Целевой пользователь».
  2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
  3. Установить флаг «Фильтровать события по имени пользователя, осуществлявшего доступ»
  4. Установить при необходимости флаг «Инверсия фильтра».
  5. Нажать кнопку «ОК».
- Настройка фильтра события ***«Внедряющий процесс»***:

1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Внедряющий процесс».
2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени процесса, поместившего информацию в буфер обмена».
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

- Настройка фильтра события ***«Пользователь, осуществляющий внедрение»***:

1. В появившемся окне «Фильтр событий доступа к буферу обмена» перейти во вкладку «Пользователь, осуществляющий внедрение».
2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени пользователя, поместившего информацию в буфер обмена»
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

15.4.2.14. Журнал управления доступом к службам

В «Журнале управления доступом к службам» в «Фильтре событий управления службами»:

- Настройка фильтра события ***«Доступ»***:

1. В появившемся окне «Фильтр событий доступа к службам» перейти во вкладку «Доступ».
2. Установить необходимые флаги для желаемого отображения записей.
3. Нажать кнопку «ОК».

- Настройка фильтра события ***«Процесс, осуществляющий доступ»***:

1. В появившемся окне «Фильтр событий доступа к службам» перейти во вкладку «Процесс».
2. Выделить необходимый процесс или процессы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени процесса».
6. Установить при необходимости флаг «Инверсия фильтра».
7. Нажать кнопку «ОК».

- Настройка фильтра события ***«Пользователь, осуществляющий доступ»***:

1. В появившемся окне «Фильтр событий доступа к службам» перейти во вкладку «Пользователь».
2. Выделить необходимого пользователя или пользователей путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по пользователям»
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

- Настройка фильтра события ***«Имя службы»***:

1. В появившемся окне «Фильтр событий доступа к службам» перейти во вкладку «Имя службы».
2. Выделить необходимую службу или службы путем одновременной комбинации клавиши «Ctrl» и левой кнопки мыши.
3. Установить флаг «Фильтровать события по имени службы».
4. Установить при необходимости флаг «Инверсия фильтра».
5. Нажать кнопку «ОК».

СПИСОК СОКРАЩЕНИЙ

СЗИ – система защиты информации;

НСД – несанкционированный доступ;

СВТ - средства вычислительной техники;

ЛВС – локальная вычислительная сеть;

ИСПДн – информационная система персональных данных;

ПРД – правила разграничения доступа;

ОС – операционная система;

ПО – программное обеспечение;

ПРД – правила разграничения доступа;

ФС – файловая система;

БД – база данных.

Приложение 1

Дополнительные настройки СЗИ «ViPNet SafePoint»

Дополнительные настройки СЗИ «ViPNet SafePoint» осуществляются путем создания или изменения определенных значений параметров реестра, отвечающих за функционал средства защиты.

1. Общие настройки СЗИ «ViPNet SafePoint». Задание значений параметра реестра «**HKLM \SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config**» (DWORD) позволяет настроить устанавливаемую на компьютер СЗИ «ViPNet SafePoint» следующим образом:

- Отключить возможность «Фиксировать «какое-либо событие» на сервере аудита» и настройку соединения с сервером аудита - **Бит 0** (*десятичное значение – «1»*).
- Назначить сервер безопасности главным по пользователям домена (с данного сервера будет происходить синхронизация списка доменных пользователей) - **Бит 1** (*десятичное значение – «2»*).
- Отключить возможность настройки правил мандатного управления доступом - **Бит 2** (*десятичное значение – «4»*).
- Разрешить управление доменными пользователями с использованием локального интерфейса настройки клиентской части - **Бит 3** (*десятичное значение – «8»*).
- Отключить выполнение клиентской частью СЗИ «ViPNet SafePoint» команд сервера безопасности и сервера аудита об удаленном управлении ФС и реестром (обзор и действия в нем), остановке и запуске программ - **Бит 4** (*десятичное значение – «16»*).

Параметр реестра создается при установке СЗИ «ViPNet SafePoint» со значением «0», значение следует изменять в ходе установки СЗИ «ViPNet SafePoint» до перезагрузки ОС. Параметр представляет собой целочисленное значение, где каждый бит – флаг. Если необходимо установить несколько флагов, то следует сложить десятичные значения и присвоить параметру данное суммарное значение.

2. Отключение/включение анализа запроса параметров устройств (дисководов гибких дисков, флоппи-дисководов), монтируемых к буквам дисков «A:» и «B:». Включение и отключение данной проверки осуществляется заданием значения параметра реестра «**HKLM \SYSTEM\CurrentControlSet\services\fileCtrl3\Parameters\ Determine Floppy Devices**» (DWORD). Параметр не создается при установке, по умолчанию анализ запросов параметров устройств, монтируемых к буквам дисков «A:» и «B:» включен. Для отключения проверки необходимо создать данный параметр реестра и присвоить ему значение «0».

3. Осуществление перезагрузки ОС при невозможности восстановить работу службы СЗИ «ViPNet SafePoint» после непредвиденной аварии. Данная функция по умолчанию отключена. Для ее активации необходимо создать параметр реестра «**HKLM \SYSTEM\CurrentControlSet\services\armour service\FailureActions»** (BINARY) и присвоить ему значение «hex:3c,00,00,00,00,00,00,00,00,00,00,00,01,00,00,00,14,00,00,00,01,00,00,00,98,3a,00,00».

4. Установка аутентификации средствами СЗИ «ViPNet SafePoint» в безопасном режиме ОС. Для установки аутентификации средствами СЗИ «ViPNet SafePoint» при входе в безопасном режиме ОС необходимо создать в ветви реестра «**HKLM\Software \Microsoft\Windows\CurrentVersion\Authentication\Credential Providers**» параметр «**ProhibitFallbacks**», типа «DWORD» и присвоить ему значение «1». Данный параметр следует установить после проведения настройки СЗИ «ViPNet SafePoint». Параметр не создается автоматически при установке СЗИ «ViPNet SafePoint», поскольку в случае некорректной настройки, при установленном параметре и включенной аутентификации средствами СЗИ «ViPNet SafePoint» вход в ОС в безопасном режиме будет невозможен.

5. Настройка параметров собственного контроля целостности СЗИ «ViPNet SafePoint». Изменение параметров, заданных по умолчанию производится только в тех случаях, когда контроль целостности объектов СЗИ «ViPNet SafePoint» вносит дополнительную нагрузку на процессор, что может проявляется при работе на слабых компьютерах. Для изменения параметров контроля целостности объектов СЗИ «ViPNet SafePoint» необходимо создать в ветви реестра «**HKLM\Software\INFOTECS\VIPNET SAFEPOINT Service**» следующие параметры:

- Включение/отключение проверки целостности, создание резервной копии – параметр «**Integrity Flags**» (DWORD), значения:
  - 0x00000001 – периодические проверки целостности включены;
  - 0x00000002 – создание резервных копий при их отсутствии;
  - 0x00000003 – работа с параметрами, заданными по умолчанию.

Для полного отключения функций контроля собственной целостности СЗИ «ViPNet SafePoint» необходимо присвоить данному параметру значение «0».

- Задание интервалов проверки целостности – параметр «**Integrity Check Delay**» (DWORD). Интервалы измеряются секундах (от 10 до 999999999), по умолчанию интервал задан равным 600 секундам.
- Задание интервалов проверки наличия внесенных изменений – параметр «**Integrity Updates Check Delay**» (DWORD). Интервалы измеряются секундах (от 10 до 999999), по умолчанию интервал задан равным 60 секундам.

6. Настройка возможности управления формированием имен объектов файловой системы. Для управления данной возможностью необходимо создать в ветви реестра «**HKLM \SYSTEM\CurrentControlSet\Services\FileCtrl3\Parameters**» **параметр** «**Name Options**» (DWORD) и, в зависимости от задач, присваивать параметру различные значения, например, присвоив параметру значение равное «0» будет полностью отключена нормализация имен и использование функции Name Provider. По умолчанию нормализация имен и функции Name Provider включены. Включение/отключение возможностей определяется установленными/очищенными битами:

- 0x00000010 – использование функций Name Provider разрешено;
- 0x00000001 – разрешено использование нормализованных имен для сетевых томов;
- 0x00000002 – разрешено использование нормализованных имен для томов со сменного носителя;
- 0x00000004 – разрешено использование нормализованных имен для томов с жесткого диска.

В СЗИ «ViPNet SafePoint» присутствует возможность отслеживания и сбора информации о работе средства защиты. Данная информация не содержит пользовательских данных, таких как пароли, описание структур сети, разграничений и т.д. Данная возможность включается добавлением в реестр ОС параметров, определяющих количество собираемой информации. Данная информация собирается в отдельный журнал. Данная функция включается путем добавления параметров «LevelMin», «LevelMax» и «Mask» типа DWORD в ветвь реестра «HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT Service\Debug Options» и задания им значений, указанных специалистами технической поддержки ОАО «ИнфоТеКС».

Также при возникновении непредвиденных аварий СЗИ «ViPNet SafePoint» собирает собственный файл дампа памяти.

Вся собранная информация сохраняется в каталоге «..\INFOTECS\VIPNET SAFEPOINT\logs\».

Приложение 2

Особенности использования СЗИ «ViPNet SafePoint» для защиты терминальных серверов и систем виртуализации

Защита терминальных серверов

Отличием функционирования терминальных серверов является создание отдельных сессий для регистрируемых на сервере пользователей, что осуществляется с использованием сервисов олицетворения системных процессов и их запуска с правами интерактивных пользователей.

Возможности СЗИ «ViPNet SafePoint» для терминальных серверов ничем не отличаются от рассмотренных ранее, отличаются лишь некоторые требования к настройке ее механизмов защиты. В частности, здесь появляется дополнительный субъект доступа – системный процесс, олицетворивший себя с правами интерактивного пользователя, либо запущенный с такими правами. Подобный процесс наиболее подвержен инжектированию в него вредоносного кода.

Защита систем виртуализации

Для включения поддержки субъектов, представляющих собой виртуальные машины необходимо установить значение параметра реестра «**HKLM\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config**» (DWORD) равным **0x00000020** (*десятичное значение – «32»*). После этого в диалоге создания субъектов появятся новые поля (рис.1).

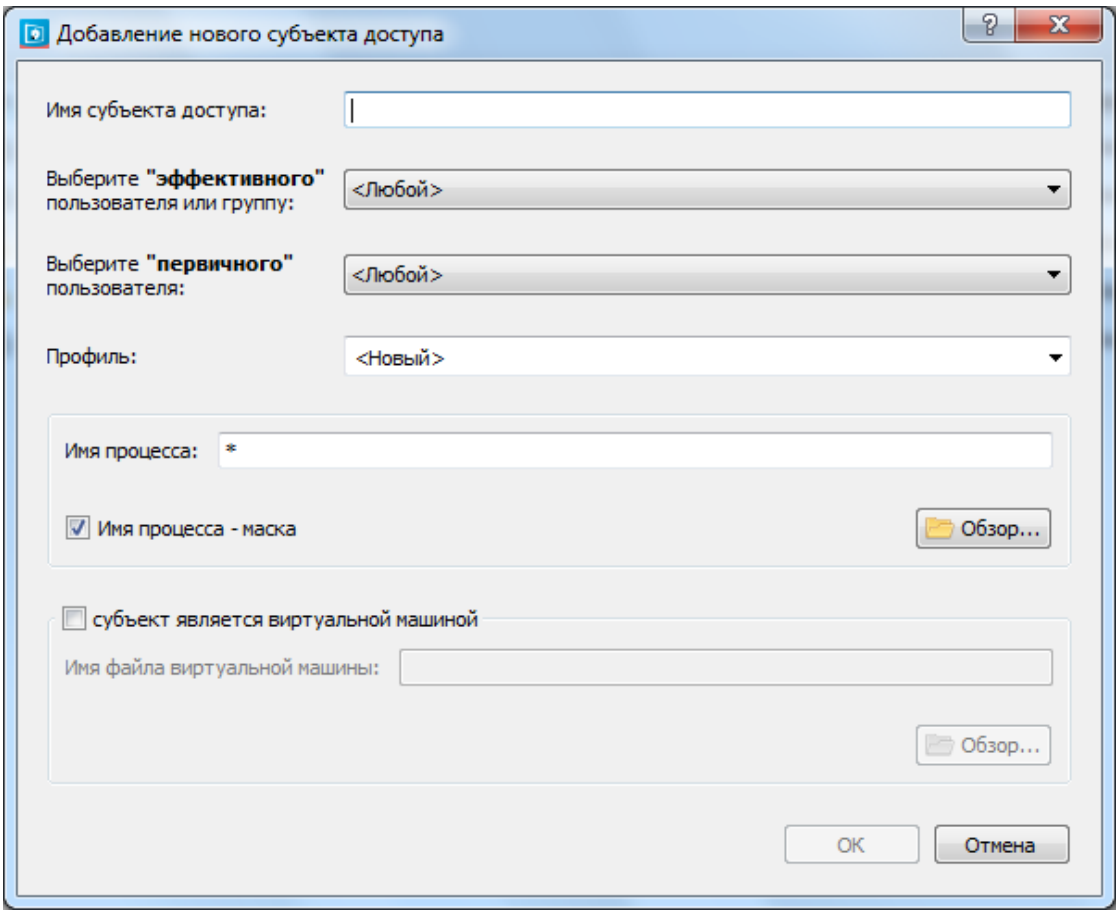


Рис. 1 – Окно добавления субъекта

В системе виртуализации СЗИ «ViPNet SafePoint» может устанавливаться и на гостевые (виртуальные) машины, и на средство виртуализации – гипервизор (хост-машину), на которых могут быть реализованы изложенные возможности защиты.

Гипервизор – это управляющий элемент, в задачи которого в том числе входит обеспечение изолированной обработки данных как между виртуальными машинами, так и между виртуальными машинами и хост-машиной.

СЗИ «ViPNet SafePoint» решаются задачи изолирования обработки данных субъектами доступа (пользователь, процесс), как следствие, СЗИ «ViPNet SafePoint» на хост-машине может решать и соответствующие задачи изолирования обработки данных.

Идентификация субъекта доступа «Виртуальная машина» в СЗИ «ViPNet SafePoint» (для Microsoft Hyper-V).

Виртуальные машины Microsoft Hyper-V представляют собою процесс "Рабочий процесс виртуальной машины» vmwp.exe, исполнимый файл которого хранится в папке System32, который работает в контексте создаваемого при запуске машины пользователя. Этот пользователь нигде не фигурирует в оснастках ОС, т.е. представляет собою такого же «псевдо-пользователя», как SYSTEM, LOCAL SERVICE и т.п. Имя этого пользователя в системе выглядит как фиксированный домен "NT VIRTUAL MACHINE" и некий уникальный идентификатор вида GUID. SID такого "пользователя" начинается так "S-1-5-83-…", тогда как SID обычного, интерактивного, пользователя начинается с "S-1-5-21-…" (рис. 2).

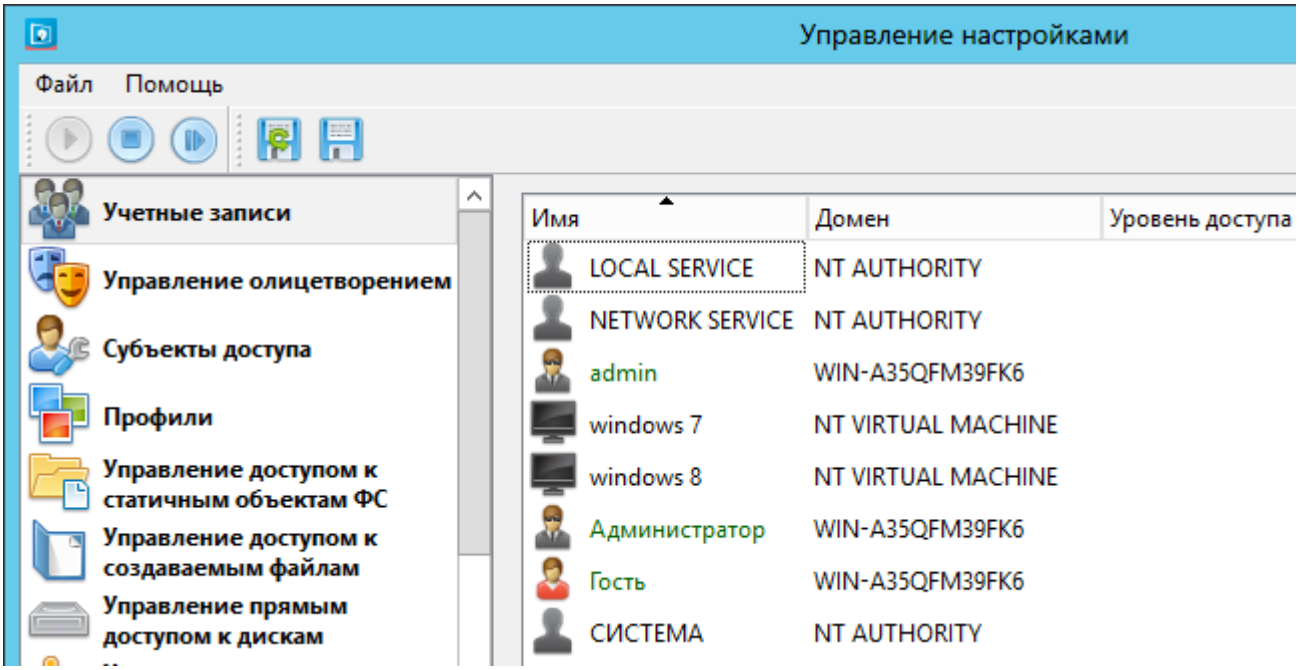


Рис. 2 – Учетные записи виртуальных машин Hyper-V

В СЗИ «ViPNet SafePoint» виртуальная машина в разграничительной политике доступа идентифицируется парой сущностей: пользователь виртуальной машины, процесс виртуальной машины. Для заданного подобным образом субъекта назначаются правила доступа к объектам. Задание в разграничительной политике на хост-машине субъекта доступа «Виртуальная машина» (для Microsoft Hyper-V) представлено на рис 3.

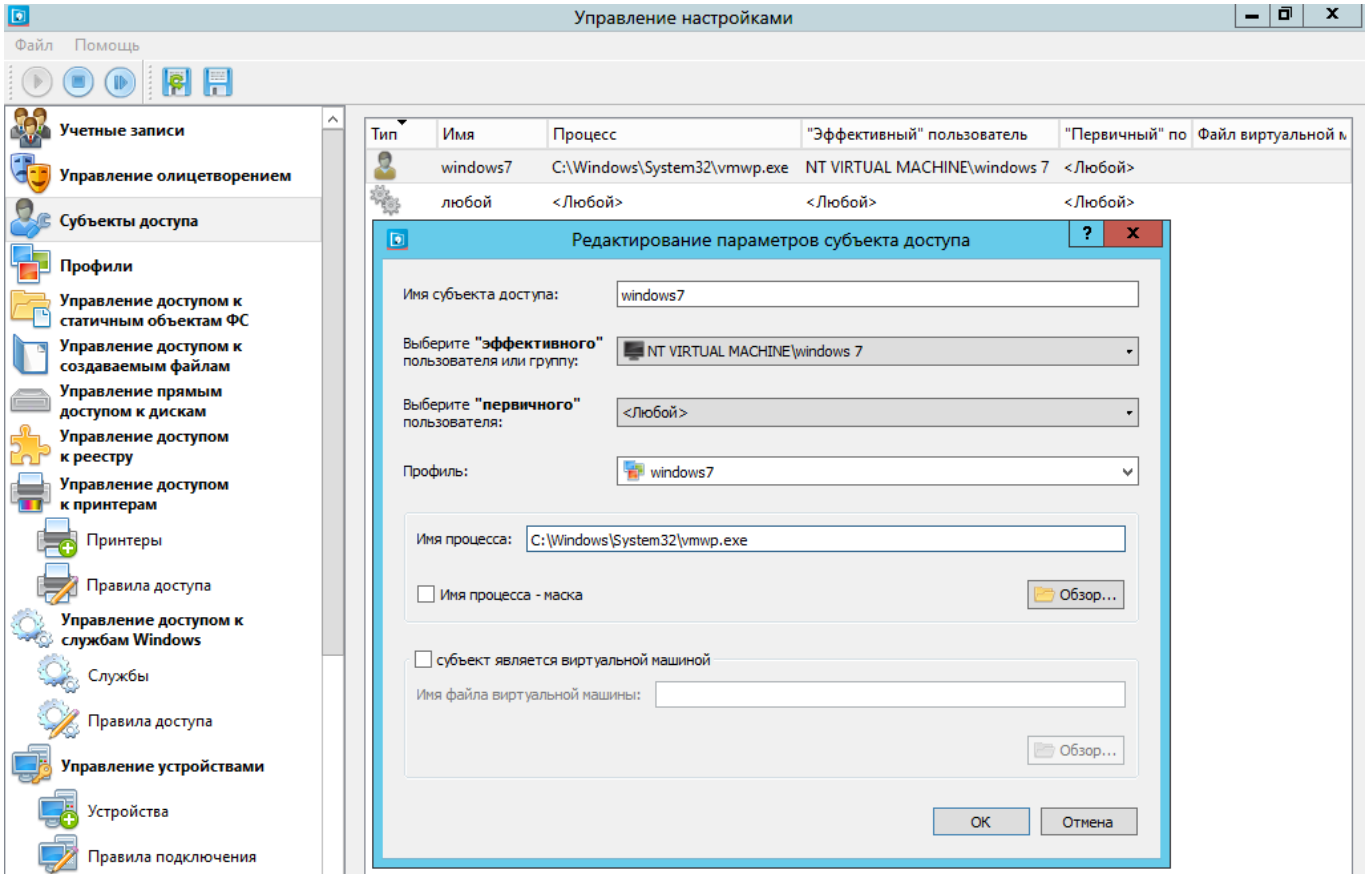


Рис. 3 – Добавление субъекта виртуальной машины Hyper-V

Для VMware Workstation субъекты доступа определяются соответствующими системными процессами виртуальных машин. Для субъекта-ВМ VMWare Workstation требуется указать имя файла конфигурации виртуальной машины в формате .vmx.