Министерство науки и высшего образования РФ

Томский государственный университет
систем управления и радиоэлектроники

И.А. Рахманенко, А.Ю. Якимук

АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск
2022

УДК 004.056
ББК 32.973.26-018.2
Р 64

Рахманенко И.А., Якимук А.Ю.
Р 64 Администрирование средств защиты информации объектов критической информационной инфраструктуры: учебно-методическое пособие. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 166 с.

Настоящее учебно-методическое пособие содержит описания лабораторных и самостоятельных работ по дисциплине «Администрирование средств защиты информации объектов критической информационной инфраструктуры» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

СОДЕРЖАНИЕ

Введение

Целью преподавания дисциплины является освоение методов управления программными средствами защиты информации, реализованными на основе клиент-серверной технологии. Задачи изучения дисциплины – получение студентами:

– Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации;

– Получение умений и навыков централизованного управления клиентскими модулями и реагирования на угрозы безопасности;

– Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации;

– Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети;

– Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

Самостоятельная работа

Самостоятельная работа включает следующие виды работ:

- Проработка лекционного материала (проверка на зачете);
- Подготовка к лабораторным работам (проверка на лабораторной работе);
- Написание отчета по лабораторной работе (проверка на лабораторной работе);
- Выполнение ИДЗ (проверка на практическом занятии).

1. Проработка лекционного материала

Проработка лекционного материала направлена на изучение следующих тем:

- Secret Net – архитектура.
- Secret Net - Защитные механизмы.
- Secret Net - Программа оперативного управления.
- Централизованная инвентаризация ресурсов локальной сети .
- Централизованная защита от вирусов в локальной сети.
- Централизованное управление средствами защиты от несанкционированного доступа в локальной сети.
- Централизованный учет и управление программно-аппаратными средствами защиты информации.
- Анализ нормативных требований по управлению средствами защиты информации

Контрольные вопросы, которые могут быть заданы для проверки степени проработки лекционного материала:

- Для чего предназначен механизм контроля целостности (КЦ)?
- Для чего предназначен механизм замкнутой программной среды?
- Для каких устройств может осуществляться теневое копирование?
- Для чего предназначена программа оперативного управления Secret Net?
- Для чего предназначена программа SAM?
- Для чего предназначен сайт SAM Management Center?
- Из каких программных компонентов состоит система КБИ?
- Основные функции системы КБИ.
- В каких режимах может работать Kaspersky Security Center?

2. Подготовка к лабораторным работам

Самостоятельная работа в ходе подготовки к лабораторным работам включает в себя оформление отчета и повторение материала, изученного на лабораторной работе.

3.Написание отчета по лабораторной работе

Данный этап самостоятельной работы включает в себя подготовку студентом отчета по итогам выполнения лабораторной работы. Отчет должен быть оформлен согласно ОС ТУСУР 01-2021. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления.

В структуре отчета должны содержаться:

- титульный лист,
- цель лабораторной работы,
- индивидуальное задание,
- ход выполнения работы,
- итоги и анализ выполнения индивидуального задания по варианту.

После выполнения работы студенту необходимо оформить отчет, включающий в себя как описание хода работы, так и выполнение индивидуального задания по варианту. Помимо скриншотов в отчет должно быть включено описание произведенных действий с полученным результатом. Файл с отчетом должен быть прикреплен к соответствующему заданию в электронной образовательной среде MOODLE (sdo.tusur.ru) в формате Microsoft Word (doc,docX) или PDF. Оценивается как выполнение хода работы (50 % баллов), так и выполнение индивидуального задания (оставшиеся 50%).

Лабораторная работа №1
«Secret Net. Разграничение доступа к устройствам»

1. Цель работы

Целью данной работы является изучение и приобретение навыков настройки и управления основными защитными механизмами СЗИ от НСД «Secret Net». Рассмотрены принципы разграничения доступа устройствам, механизмы контроля печати.

2. Краткие теоретические сведения

Для защиты доступа к устройствам компьютера в Secret Net используются механизм контроля подключения и изменения устройств и механизм разграничения доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля подключения и изменения устройств предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера, а также для поддержания в актуальном состоянии списка устройств компьютера. По списку устройств с помощью второго механизма выполняется разграничение доступа пользователей к устройствам. Часть функций разграничения доступа к устройствам реализуется с использованием механизма полномочного управления доступом.

Для представления множества устройств, установленных или подключаемых к защищаемым компьютерам (рис. 1), используется иерархическая схема списка устройств. Устройства группируются в классы, а классы, в свою очередь, включены в состав групп. Группы являются элементами объединения верхнего уровня. Количество групп фиксировано.

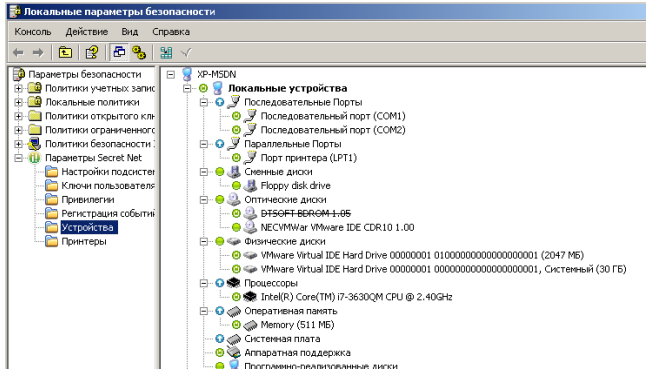


Рисунок 1 – Группы устройств, контролируемые «Secret Net»

Предусмотрены следующие группы устройств:

–Локальные устройства – объединяют фиксированные устройства компьютера, для которых не предполагается ограничивать подключение (например, последовательные и параллельные порты, процессоры, оперативная память);

–Устройства USB – объединяет устройства, подключаемые к шине USB;

–Устройства PCMCIA – объединяет устройства, подключаемые к шине PCMCIA;

–Устройства IEEE1394 – объединяет устройства, подключаемые к шине IEEE1394;

–Устройства SecureDigital – объединяет устройства, подключаемые к шине SecureDigital;

–Сеть – объединяет устройства, являющиеся сетевыми интерфейсами (адаптеры).

Если сетевым интерфейсом является нефиксированное подключаемое устройство, такое устройство может также присутствовать и в другой группе. Это даёт возможность настроить реакцию системы на подключение устройства до его регистрации в качестве сетевого интерфейса.

Некоторые классы допускают дополнительное разбиение устройств по моделям. Модели объединяют устройства с одинаковыми идентификационными кодами, присвоенными производителем. В списке устройств присутствуют предопределенные модели — например, модели электронных идентификаторов. Также в список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды. В дальнейшем при обнаружении нового устройства с такими же идентификационными кодами это устройство автоматически будет добавлено в качестве экземпляра к той же модели. За счет этого можно управлять одинаковыми устройствами без необходимости настройки параметров каждого устройства по отдельности.

Для объектов каждого уровня (группа, класс, модель, устройство) определённого параметров, с помощью которых настраиваются механизмы контроля подключения и изменения устройств, разграничения доступа к устройствам, теневого копирования и полномочного управления доступом. Иерархия списка устройств в большинстве случаев позволяет выполнять настройку, как на уровне отдельного устройства, так и на уровне классов и групп.

3. Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player, VMware Workstation или Virtual Box, а также скачать архив с виртуальной машиной «Secret Net Client». Скачанный архив необходимо разархивировать.

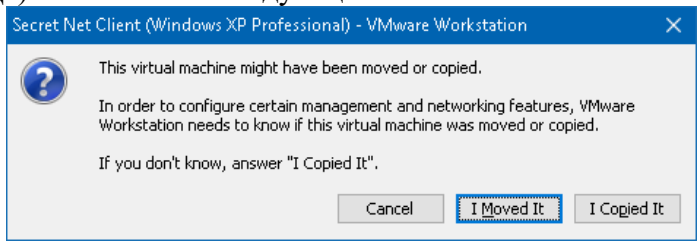
Убедитесь, что вы запускаете виртуальную машину на системе виртуализации, соответствующей названию скачанного архива.

Желательно убедиться, что в настройках виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only») в случае, если используется система виртуализации VMware. При наличии на хосте оперативной памяти большого объема, можно увеличить выделяемый виртуальной машине объем ОЗУ (по умолчанию установлен 256 МБ).

4. Ход работы

1. Запустите виртуальную машину «Secret Net Client». Для настройки конфигурации виртуальной машины VMware задаст вопрос о том была ли она скопирована или перемещена (рис. 2), выберите вариант «I Moved It» (виртуальная машина перемещена).

После загрузки операционной системы войдите под локальной учётной записью **«Администратор»** (рис.3). Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». После этого будет выведено сообщение об изменении аппаратной конфигурации. Снимите блокировку рабочей станции (Да) и выполните следующее:



Рисинок 2 - Запрос конфигурации при запуске виртуальной машины

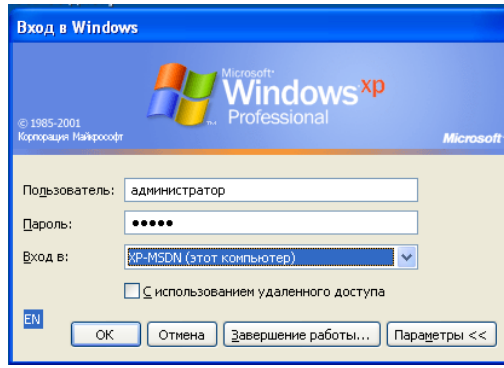


Рисунок 3 – Вход в систему под локальной учётной записью

Откройте свойства учетной записи **Администратор** (Мой компьютер - Управление - Локальные пользователи - Пользователи - Администратор). Измените уровень допуска на «строго конфиденциально» (Вкладка Secret Net 7 - Доступ), разрешите управление категориями конфиденциальности, вывод и печать конфиденциальных документов (рис. 4). Создайте учетные записи **user** и **conf**. Настройте пользователю **conf** категорию доступа конфиденциально и добавьте возможность печати конфиденциальных документов (рис. 5). Для пользователя **user** по умолчанию задан уровень допуска «Неконфиденциально».

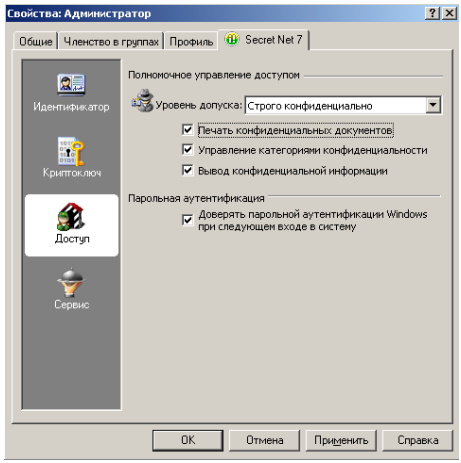


Рисунок 4 – Параметры управления полномочным доступом для пользователя Администратор

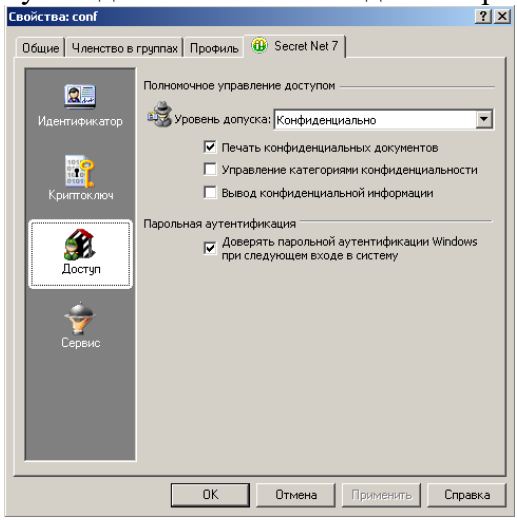


Рисунок 5 – Параметры управления полномочным доступом для пользователя conf

2. Вызовите оснастку для управления параметрами объектов групповой политики (Пуск – Программы - Код безопасности - Secret Net -

Локальная политика безопасности) и перейдите к разделу «Параметры безопасности | Параметры Secret Net»

– Выберите папку «Устройства». Утвердите изменения. В правой части окна появится общий список устройств;

– Выберите в списке оптический диск «VMWare IDE CDR» (или другой CD – дисковод, который будет предоставлен средством виртуализации VMware), вызовите контекстное меню и выберите команду «Свойства». В группе настройки выберите «Подключение устройства разрешено» (рис. 6). В группе «полномочный доступ» выберите параметр доступа «Для устройств задана категория конфиденциальности» и выберите категорию конфиденциальности «Строго конфиденциально» (рис. 7).

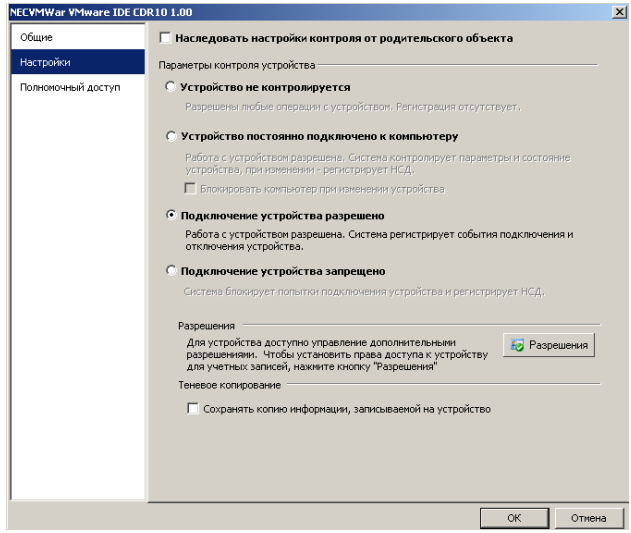


Рисунок 6 – Настройки виртуального CD – привода в групповых политиках Secret Net

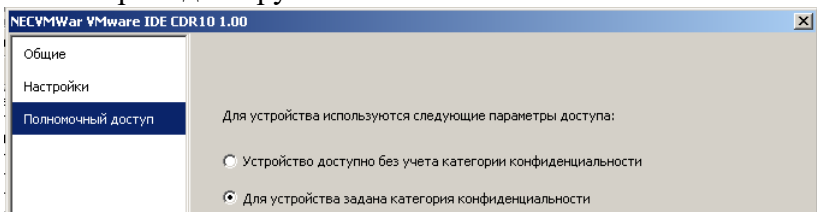


Рисунок 7 – Настройки конфиденциальности виртуального CD – привода в групповых политиках Secret Net

–Войдите под учетной записью «user» и убедитесь что вход в систему, при наличии устройства с категорией конфиденциальности выше, чем у пользователя, недоступен. Приведите результат в отчете.

3. Войдите под учетной записью **«Администратор»**, измените назад параметры конфиденциальности оптического диска на «Устройство доступно без учета категории конфиденциальности», запретите использование оптических дисков для пользователя **«user»** следующим образом: откройте разрешения в свойствах CD-дисковода (Настройки - Разрешения), добавьте пользователя **user** и запретите все разрешения к данному CD-приводу (рис. 8) - галочки «запретить».

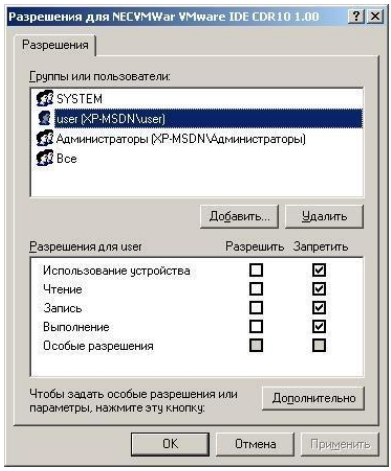


Рисунок 8 – Изменение прав доступа к CD-приводу для пользователя user

–Войдите под учетной записью user и убедитесь в запрете доступа, попытавшись открыть CD-привод в проводнике.

4. Настройку политик контроля устройств можно выполнить индивидуально для каждого устройства (отдельной модели), класса или группы устройств с использованием принципа наследования параметров. Для настройки политики контроля устройств выполнить следующее:

–Войдите под учетной записью **«Администратор»**. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net»

–Выберите папку «Устройства». В правой части окна появится общий список устройств.

–Выберите в списке объект «Устройства USB», вызовите контекстное меню и выберите команду «Свойства».

На экране появится диалог для настройки параметров объекта. По умолчанию в диалоге отображаются параметры группы «Общие» (рис. 9), представляющие основные сведения об объекте.

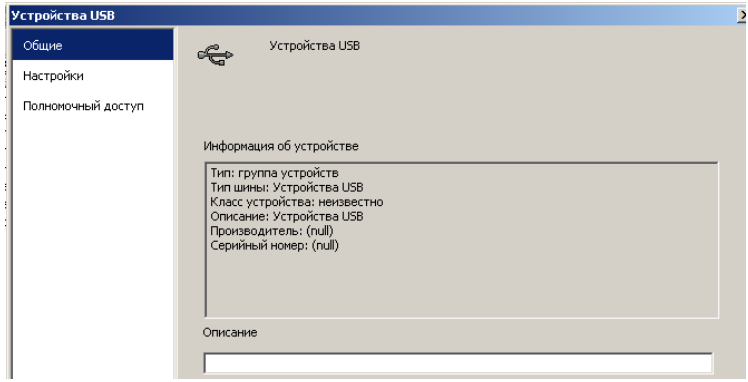


Рисунок 9 – Вкладка общие для группы устройства USB

–Перейдите к группе параметров «настройки» и поставьте значения параметров в соответствии с рисунком 10. Примените настройки ко всем дочерним объектам.

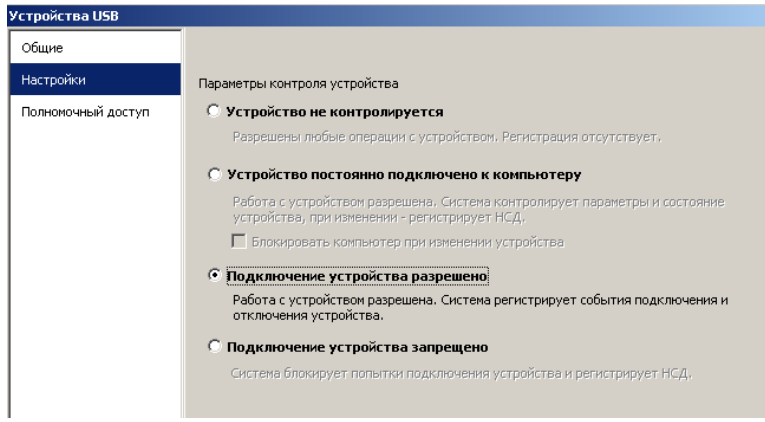


Рисунок 10 – Вкладка «Настройки» для группы устройства USB

При этом для подключения устройств можно задать следующие параметры:

–Поле «Устройство не контролируется». Если в поле установлена отметка — для объекта отключен режим контроля.

–Поле «Устройство постоянно подключено к компьютеру». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру. В случае изменения состояния устройства в журнале регистрируются события несанкционированного доступа (НСД), и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности. Для усиления защиты можно дополнительно включить режим автоматического блокирования компьютера при изменении состояния устройства: для этого установите отметку в поле «Блокировать компьютер при изменении устройства». Возможность разблокировки

компьютера будет иметь только администратор безопасности.

–Поле «Подключение устройства разрешено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование.

–Поле «Подключение устройства запрещено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. Попытки подключения устройства регистрируются в журнале как события НСД. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование.

4.1. Разграничение доступа к принтерам. Работа с принтерами.

5. В список принтеров групповой политики можно добавлять элементы, соответствующие конкретным принтерам. По умолчанию ни один принтер в системе не контролируется. Добавление осуществляется с помощью специальной программы - мастера. При необходимости принтер можно удалить из списка — для этого вызовите контекстное меню принтера и активируйте команду «Удалить». Добавьте принтер в групповую политику Secret Net. Для добавления принтера в список групповой политики необходимо выполнить следующее:

–Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности \ Параметры Secret Net».

–Выберите папку «Принтеры». В правой части окна появится список принтеров.

–В меню оснастки выберите команду «Действие | Добавить принтер». На экране появится стартовый диалог мастера добавления принтеров.

–Выберите вариант добавления принтера (подключенный к компьютеру -> Microsoft XPS Document Writer) (рис.11)

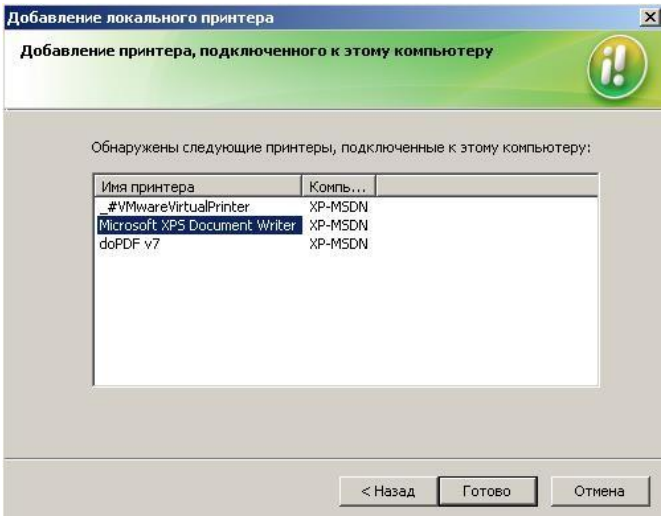


Рисунок 11 – Добавление принтера, контролируемого Secret Net

После того, как добавлен принтер, необходимо настроить права пользователей для печати. В оснастке для управления параметрами объектов групповой

политики Secret Net («Параметры безопасности | Параметры Secret Net»), выберите папку «Принтеры» и вызовите контекстное меню принтера «Microsoft XPS Document Writer» - параметр «Свойства» (рис.12).

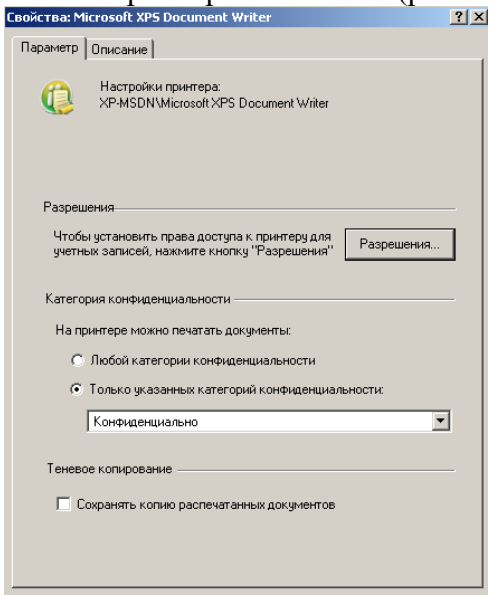


Рисунок 12 – Настройка разрешений печати для принтера Microsoft XPS Document Writer

6. В окне свойств принтера выберите «Только указанных категорий конфиденциальности», а категорию – «Конфиденциально». Стоит отметить, что для печати документов соответствующей категории конфиденциальности пользователя должна быть включена возможность печати конфиденциальных документов (было выполнено ранее). Измените разрешения на доступ к диску «D:\» (Диск D – Свойства – Безопасность – Все – Полный доступ). Измените у папки «D:\temp» категорию конфиденциальности на «Конфиденциально», изменив

категорию и у всех вложенных файлов (рис. 13). Отдельно файлу «D:\temp\Неконф.txt» задайте категорию «Неконфиденциально».

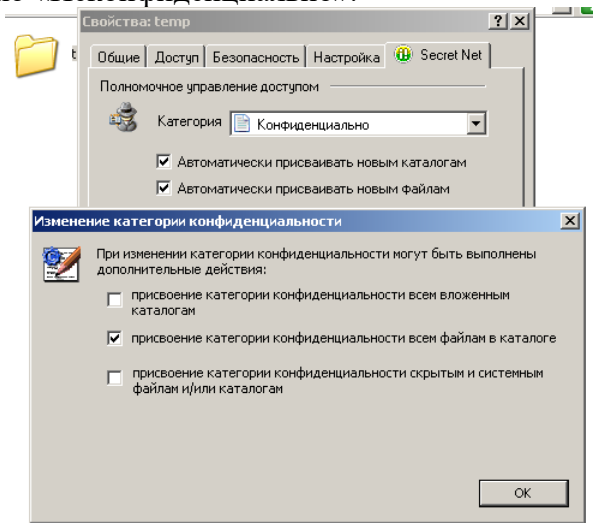


Рисунок 13 – Изменение уровня конфиденциальности папки temp

7. Зайдите под учетной записью conf и убедитесь в возможности печати документов «D:\temp\Конф.txt» с категорией «К онфиденциально» и документа «D:\temp\Неконф.txt» « Неконфиденциально». В параметрах печати необходимо задать настройку «Печать в файл» (рис. 14). При наличии права на печать конфиденциального документа, будет предложено заполнить гриф, добавляемый в распечатываемый документ (рис. 15). Попробуйте распечатать данные документы с помощью принтеров «Microsoft XPS Document Writer» и «doPDF» (рис. 16). Проанализируйте полученные результаты, зафиксируйте их в отчете.

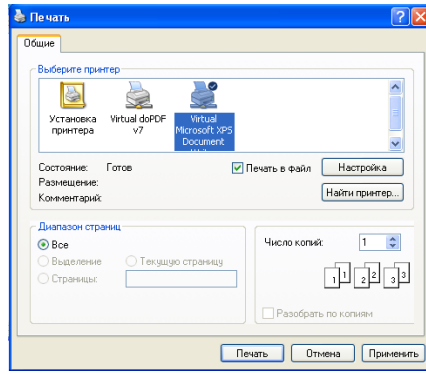


Рисунок 14 – Параметры печати конфиденциального документа

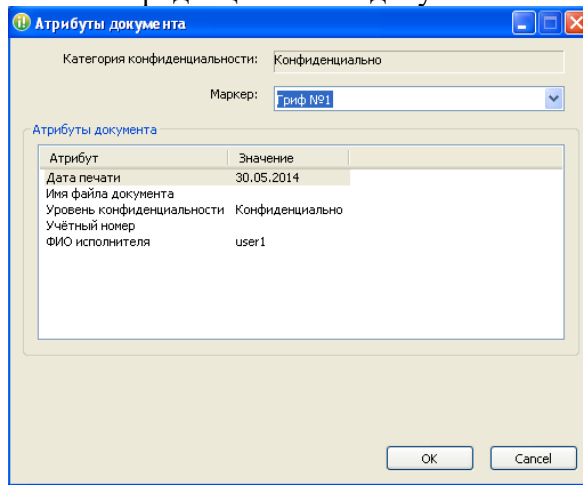


Рисунок 15 – Выбор и заполнение грифа для распечатываемого документа

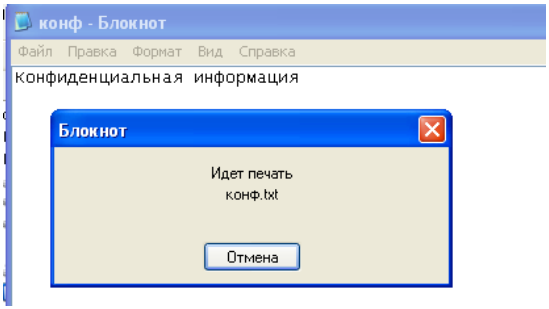


Рисунок 16 – Процесс печати конфиденциального документа

5. Задание на лабораторную работу

Проделайте ход работы, зафиксировав полученные результаты в отчете. Создайте учетную запись, соответствующую имени в факультетской сети (либо из ФИО). В зависимости от номера варианта задайте учетной записи пользователя категорию конфиденциальности и запретите подключение устройств:

Таблица 1

Варианты заданий работы с пользователями

Вариант	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
В зависимости от номера варианта задайте учётной пользователя категорию конфиденциальности													
Конфиденцально		+				+			+		+		

Строго конфиденциально			+		+		+			+		+	
Не конфиденциально	+			+				+					+
Запретить подключение устройств													
Устройства SD			+		+	+		+		+			+
Принтеры	+			+		+	+						
Электронные идентификаторы и считыватели		+						+	+			+	
Сетевые платы			+	+	+						+		
Оптические диски	+		+			+		+		+			+
USB Устройства		+		+			+					+	

Примечание: “+” означает, что для данного устройства нужно запретить подключение.

Также для данной учётной записи и устройства проделайте следующие действия:

1. Для соответствующего класса устройств по варианту измените разрешения, для созданного пользователя, на запрет «чтения», «записи» и «выполнения». Проверьте, выполняются ли данные разрешения.

2. Для принтера разрешите вывод на печать документов с категорией «Строго конфиденциально». Попытайтесь из под созданной учетной записи распечатать документ с категорией конфиденциальности «Конфиденциально» («D:\temp\Конф.txt») и документ с категорией

конфиденциальности «Не конфиденциально» («D:\Неконф.txt»).

6. Контрольные вопросы

1. Для чего предназначен механизм контроля подключения и изменения устройств?
2. Для каких устройств реализован механизм контроля подключения и изменения?
3. Какие группы устройств предусмотрены в Secret Net?
4. Что значит параметр контроля «Наследуется»?
5. Перечислите существующие параметры контроля?

Лабораторная работа № 2
«Secret Net. Замкнутая программная среда. Контроль целостности»

1. Цель работы

Целью данной работы является изучение и приобретение навыков настройки и управления основными защитными механизмами СЗИ от НСД «Secret Net». Рассмотрены принципы обеспечения замкнутой программной среды и настройки контроля целостности.

2. Краткие теоретические сведения

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале

безопасности регистрируются события несанкционированного доступа (НСД).

На этапе настройки механизма ЗПС составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически на основании сведений об установленных на компьютере программах или по записям журналов, содержащих сведения о запусках программ, библиотек и сценариев. Также предусмотрена возможность ручного формирования списка. Для файлов, входящих в список, можно включить режим контроля целостности. По этой причине механизм замкнутой программной среды и механизм контроля целостности используют единую модель данных.

При включенном «мягком» режиме работы подсистемы замкнутой программной среды контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО. Этот режим обычно используется на этапе настройки механизма ЗПС. Помимо параметра «Мягкий» режим в свойствах субъекта управления есть еще три параметра:

–Проверять целостность модулей перед запуском. Этот параметр отвечает за проверку целостности программ перед их запуском.

–Проверять заголовки модулей перед запуском. При установке этого параметра в процессе контроля включается дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке.

–Контролировать исполняемые скрипты. Этот параметр отвечает за блокировку выполнение

сценариев (скриптов), не входящих в перечень разрешенных для запуска и не зарегистрированных в базе данных системы Secret Net.

Для управления режимами замкнутой программной среды и контроля целостности, а также моделью данных используется программа «Контроль программ и данных». Окно программы (рис. 1) содержит следующие элементы:

(1) – Меню. Содержит команды управления программой.

(2) – Панель инструментов. Содержит кнопки быстрого вызова команд управления.

(3) – Информационный заголовок. Содержит название выбранной для отображения категории объектов.

(4) – Панель категорий. Содержит ярлыки для выполнения одноименных команд меню «вид».

(5) – Область списка объектов.

(6) – Окно структуры.

(7) – Окно зависимостей. Содержит список объектов, связанных с объектом, который выбран в области списка объектов. В верхней части окна расположены кнопки, управляющие фильтрацией объектов списка.

(8) – Строка состояния. Содержит служебные сообщения программы.

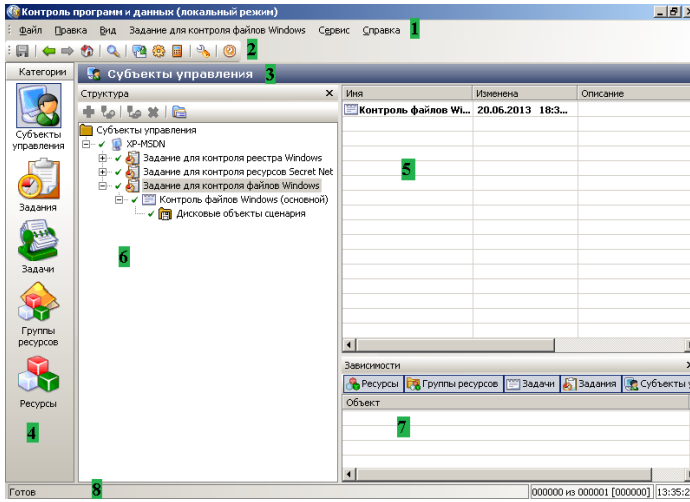


Рисунок 1 – Окно программы “Контроль программ и данных”

3. Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player, VMware Workstation или Virtual Box, а также скачать архив с виртуальной машиной «Secret Net Client». Скачанный архив необходимо разархивировать.

Убедитесь, что вы запускаете виртуальную машину на системе виртуализации, соответствующей названию скачанного архива.

Желательно убедиться, что в настройках виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only») в случае, если используется система виртуализации VMware. При наличии на хосте оперативной памяти большого объема, можно увеличить выделяемый виртуальной машине объем ОЗУ (по умолчанию установлен 256 МБ).

4. Ход работы

1. Запустите виртуальную машину «Secret Net Client». Для настройки конфигурации виртуальной машины VMware задаст вопрос о том была ли она скопирована или перемещена (рис. 2), выберите вариант «I Moved It» (виртуальная машина перемещена). После загрузки операционной системы войдите под локальной учетной записью «Администратор», пароль 12345 (рис. 3). Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». После этого будет выведено сообщение об изменении аппаратной конфигурации. Снимите блокировку рабочей станции (Да) и выполните следующее:

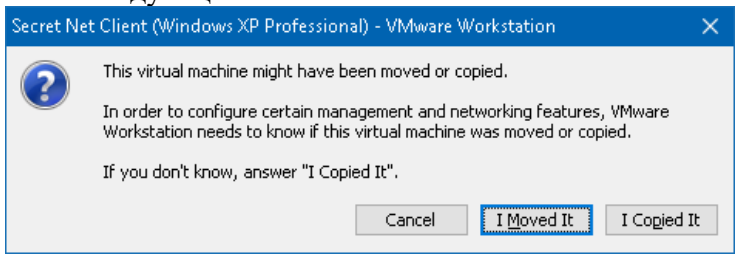


Рисунок 2 – Запрос конфигурации при запуске виртуальной машины

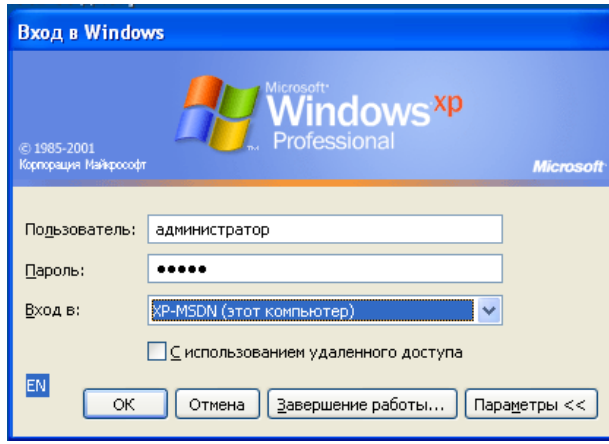


Рисунок 3 – Вход в систему под локальной учетной записью

Откройте свойства учетной записи **Администратор** (Мой компьютер - Управление - Локальные пользователи - Пользователи - Администратор). Измените уровень допуска на «строго конфиденциально» (Вкладка Secret Net 7 - Доступ), разрешите управление категориями конфиденциальности, вывод и печать конфиденциальных документов (рис. 4). Создайте учетные записи **user** и **conf**. Настройте пользователю **conf** категорию доступа конфиденциально и добавьте возможность печати конфиденциальных документов (рис. 5). Для пользователя **user** по умолчанию задан уровень допуска «Неконфиденциально».

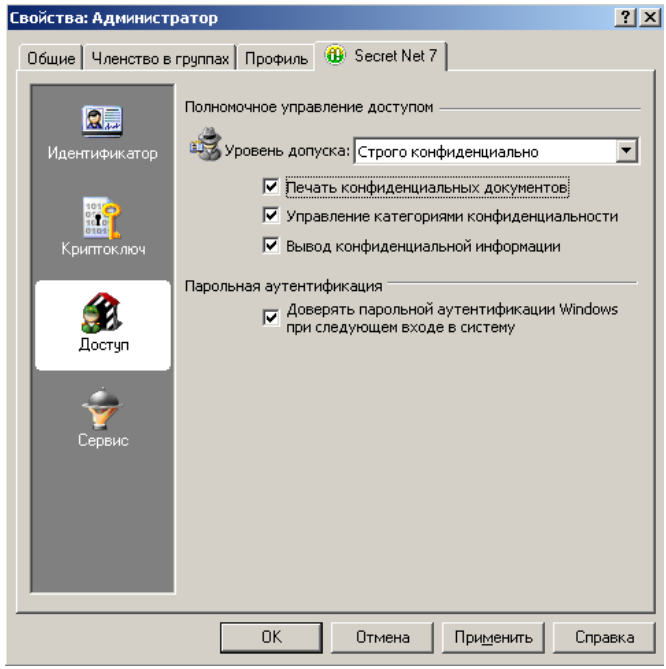


Рисунок 4 – Параметры управления полномочным доступом для пользователя Администратор

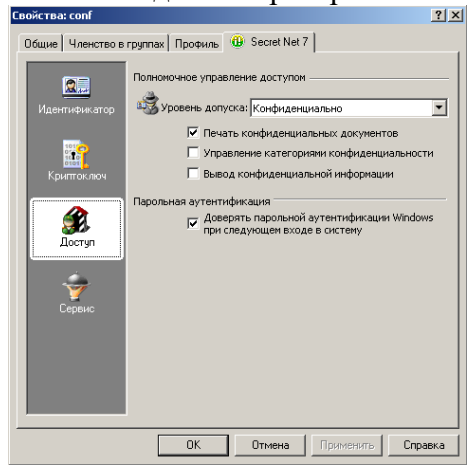


Рисунок 5 – Параметры управления полномочным доступом для пользователя conf

Измените разрешения на доступ к диску «D:\» (Диск D – Свойства – Безопасность – Все – Полный доступ). Измените у папки «D:\temp» категорию конфиденциальности на «Конфиденциально», изменив категорию и у всех вложенных файлов (рис. 6). Отдельно файлу «D:\temp\Неконф.txt» задайте категорию «Неконфиденциально».

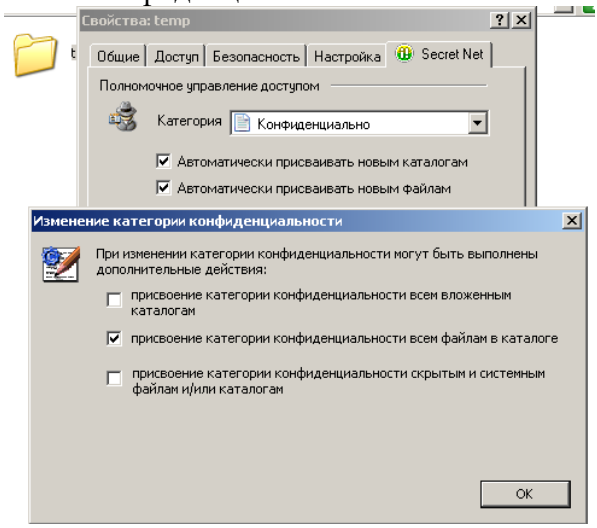


Рисунок 6 – Изменение уровня конфиденциальности папки temp

4.1. Настройка механизмов контроля целостности и замкнутой программной среды

2. Войдите под учетной записью **Администратор**. Для запуска программы необходимо выбрать следующую команду «Пуск \Все программы \Код Безопасности\SecretNet \Контроль программ и данных».

Перед тем как произвести построение фрагмента модели данных системой проводится анализ размещения программного обеспечения и данных на защищаемом компьютере, формируются требования к настройке контроля целостности и замкнутой программной среды, который включает в себя:

−сведения о защищаемом компьютере (установленное ПО, пользователи и их функциональные обязанности, задачи, решаемые пользователями в рамках бизнес- процессов);

−перечень ресурсов, подлежащих контролю целостности;

−перечень программ, с которыми разрешено работать разным группам пользователей;

−задачи (список задач и их краткое описание).

Для построения фрагментов модели данных в программе КЦ-ЗПС выбираем команду «Файл \Новая модель данных». В ней предоставляется возможность детальной настройки параметров для формирования новой модели данных (рис. 7). Нажмите ОК для создания стандартной модели (для тех файлов, где появятся ошибки выберите вариант снять с контроля). В эту модель можно добавить файлы операционной системы и Secret Net для контроля их целостности и создания ЗПС. Помимо стандартных задач, в модель можно добавить задачи, сформированные на основе ресурсов приложений. Добавление таких задач осуществляется с помощью параметра «Добавить другие задачи из списка». После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура, включающая в себя субъект «Компьютер» с назначенными для него заданиями.

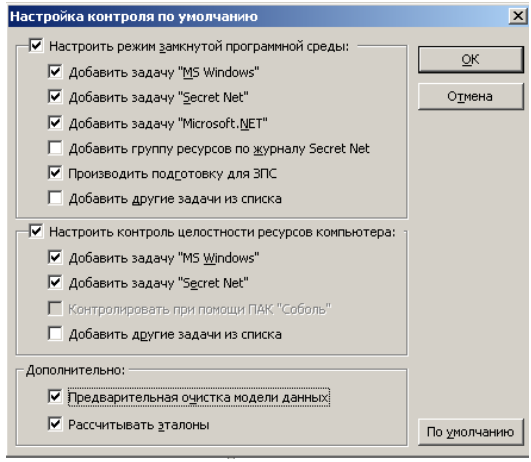


Рисунок 7 – Настройка контроля целостности и ЗПС для стандартных объектов.

3. После того, как произойдет подготовка ресурсов для использования замкнутой программной среды, в левой части окна выберите категорию «Задания» и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Замкнутая программная среда» и нажимаем на кнопку «ОК» (рис. 8). Затем введите имя задания и продолжите работу, нажав на кнопку «ОК».

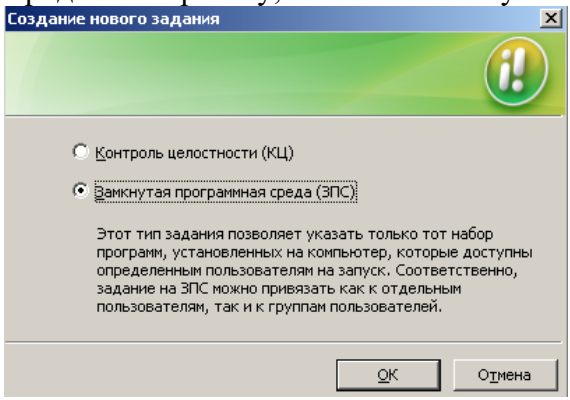


Рисунок 8 – Выбор типа задания

После чего, новое задание будет отображаться в окне структуры.

4. Выделите созданное задание на ЗПС. Открыв правой кнопкой мыши контекстное меню выберите «Добавить задачи \группы-Новую группу по каталогу…» (рис. 9). В окне выбора добавьте каталог «C:\Program Files\Movie Maker» и нажмите «ОК». На панели категорий выберите «Субъекты управления» и нажмите «Добавить в список» (рис.10). Введите имя выбираемого объекта **«user»** и нажмите «ОК» (рис. 11).

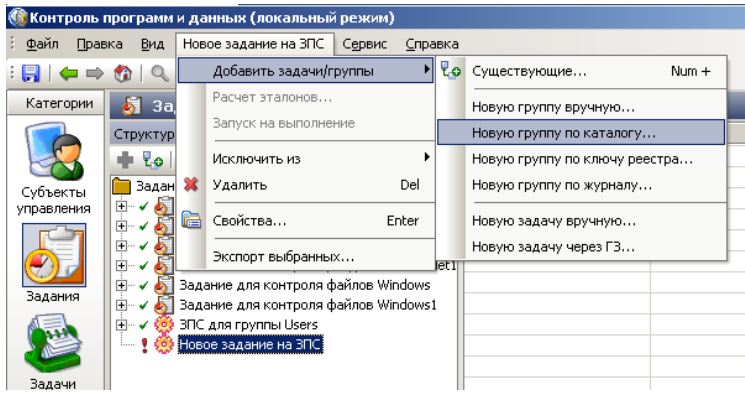


Рисунок 9 – Добавление группы ресурсов в задание на ЗПС

Рисунок 10 – Добавление контролируемого пользователя

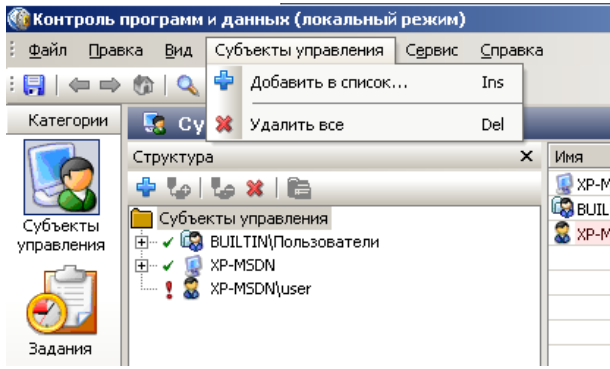


Рисунок 11 – Выбор пользователя user

5. Выделите 11. Выделите добавленного пользователя. В меню выберите «XP - MSDN\user >Добавить задания > Существующие...», в открывшимся окне выберите «Новое задание на ЗПС»

и нажмите «ОК». Теперь пользователя **user** выбранный каталог будет входить в ЗПС, а следовательно, программы находящиеся в каталоге будут разрешены к запуску. Для того, чтобы ЗПС функционировала необходимо включить «Жесткий режим». Для этого необходимо выполнить следующее:

–выбрать категорию «Субъекты управления» на панели категорий.

–выбрать в дополнительном окне структуры группу «XP-MSDN», вызовите контекстное меню и выберите команду «Свойства». В появившемся окне перейдите к вкладке «Режимы» (рис. 12).

–установите отметку в поле «Режим ЗПС включен» и удалите отметку в поле «Мягкий режим».

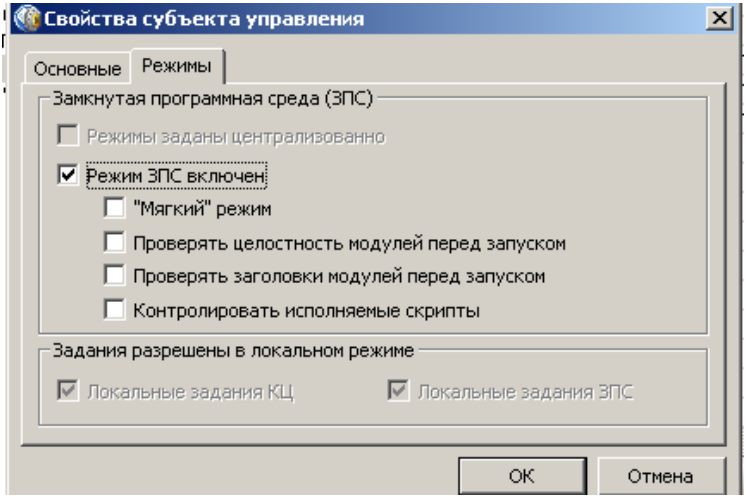


Рисунок 12 – Настройка режима ЗПС

После проделанных действий замкнутая программная среда будет работать в «Жестком режиме». То есть будут разрешены для запуска только те программы, которые добавлены в задания на ЗПС.

На учетную запись **«Администратор»** ЗПС не действует, так как в групповых политиках была задана данная привилегия.

6. Закройте программу, сохранив модель. Войдите под учетной записью **«user»**. Попробуйте поработать в операционной системе, результаты зафиксируйте в отчете. Интерфейс Windows должен отображаться некорректно, так как не все файлы, нужные для корректной работы системы были добавлены в ЗПС. Для того чтобы это исправить необходимо обучить модель в «мягком» режиме.

Войдите под учетной записью **«Администратор»** и включите «мягкий» режим работы ЗПС (как в п. 5). Сохраните модель. Войдите под учетной записью **user** и запустите Movie Maker («C:\Program Files\Movie Maker\moviemk.exe»). Теперь все необходимые для корректной работы программы будут записаны в журнал Secret Net.

Войдите под учетной записью **Администратор** и добавьте в задание на ЗПС файлы из журнала Secret Net: под учетной записью **Администратор** откройте Контроль программ и данных, выберите Файл-Новая модель данных, задав режим ЗПС с добавлением группы ресурсов по журналу Secret Net (рис. 13). В этом случае Secret Net разрешит запускаться программам, записи о попытках запуска которых отмечены журналах Secret Net. Файлы без ЭЦП игнорировать. Далее включите жесткий режим ЗПС (как в п. 5) и сохраните модель.

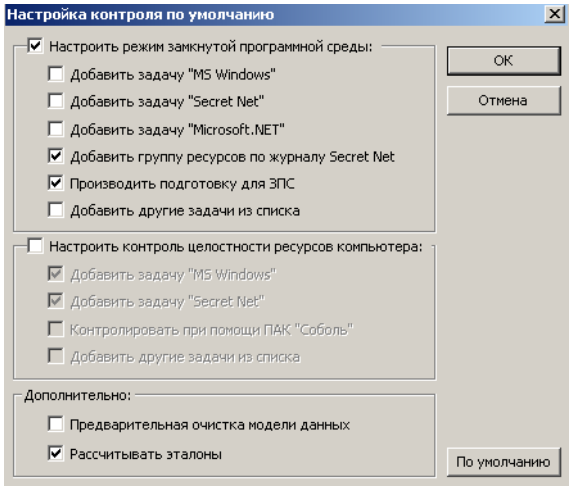


Рисунок 13 – Добавление группы ресурсов по журналу Secret Net

Войдите под учетной записью **user**. Запустите программу Windows Movie Maker и убедитесь в возможности ее запуска.

Запустите Windows Media Player(«C:\Program Files\Windows Media Player\wmplayer.exe»). Попробуйте запустить другие программы. Результаты зафиксируйте в отчете. После проверок выключите ЗПС.

4.2. Настройка контроля целостности

Контроль целостности настраивается для тех файлов, для которых критична их неизменность. Сюда могут входить исполняемые файлы и библиотеки операционной системы и другие важные файлы.

7. Войдите под учетной записью **«Администратор»**. Запустите программу «Пуск\Все программы\Код Безопасности\Secret Net\Контроль программ и данных». Выберите категорию «Задания»

и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Контроль целостности» и нажимаем на кнопку «ОК» (рис.14).

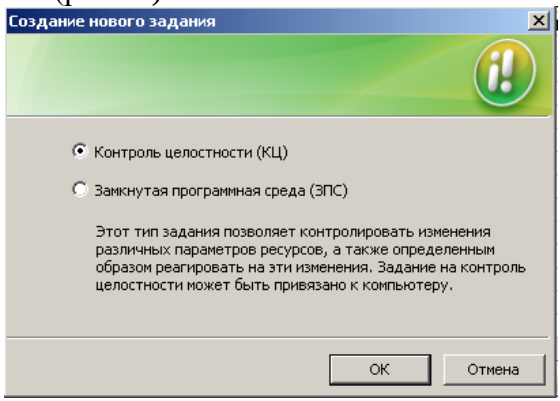


Рисунок 14 – Создание задания на КЦ

После того, как выбран тип «Контроль целостности», появится окно «Создание нового задания на КЦ» (рис.15). В данном окне задайте имя «Новое задание на КЦ». В методе контроля ресурсов выберите «Содержимое», а для параметра «Реакция на отказ» выставить значение «Заблокировать компьютер». Ниже приведены описания методов контроля и то, что будет проверяться.

Метод контроля:

–Содержимое. Проверяется целостность содержимого ресурсов;

–Атрибуты. Проверяются стандартные атрибуты, установленные для ресурсов;

–Права доступа. Проверяются категории конфиденциальности, установленные для ресурсов;

–Существование. Проверяется наличие ресурсов по заданному пути.

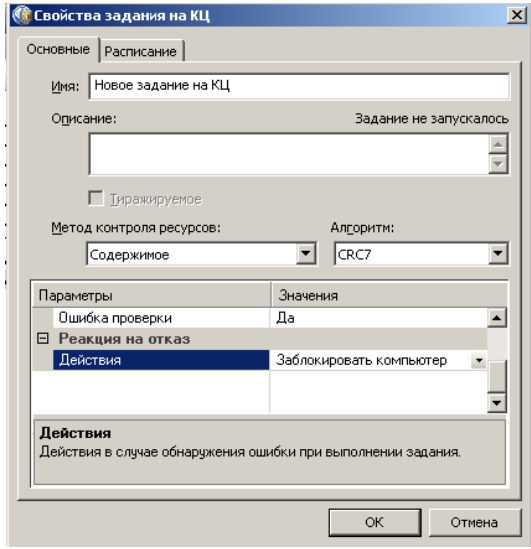


Рисунок 15 – Окно настроек задания на контроль целостности

Перейдите к вкладке «Расписание» (рис.16). Во вкладке «Расписание» выберите поля «При загрузке ОС», «При входе». Также можно настроить по каким дням и месяцам будет выполняться контроль целостности. Для этого установите КЦ с июня по декабрь и с понедельника по воскресенье и нажмите кнопку «ОК».

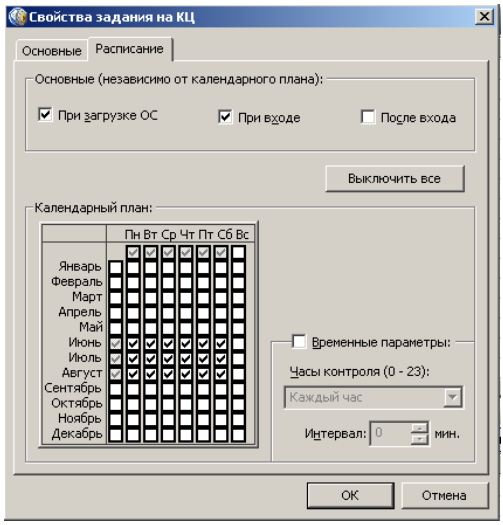


Рисунок 16 – Настройка расписания контроля целостности

8. Необходимо задать контроль целостности для данного компьютера. Для этого перейдите к вкладке «Субъекты управления», выберите «XP-MSDN» и вызовите контекстное меню и добавьте задание «Новое задание на КЦ». Перейдите к категории «Задания», вызовите контекстное меню нового задания на КЦ и добавьте ресурс по каталогу «D:\Temp». Произведите расчет эталонов для файлов, заданных на контроль целостности:

В контекстном меню «Нового задания на КЦ» – Расчет эталонов (или Сервис – Эталоны – Расчет, если нужно рассчитать все эталоны). Установите галочку оставлять старые и нажмите ОК. Сохраните изменения выбрав в меню «Файл» - «Сохранить». Зайдите под учетной записью **«conf»** и измените содержимое файла «Конф.txt» в папке «Temp» находящейся на диске «D:\». Попробуйте заново войти

в систему под учетной записью **«conf»**. Результаты зафиксируйте в отчете.

Для того, чтобы компьютер каждый раз не блокировался по причине нарушения целостности, войдите под учетной записью **«Администратор»** и пересчитайте эталоны для созданного задания на КЦ. Тем самым мы обновляем эталоны для измененных файлов, находящихся на контроле целостности.

5. Задание на лабораторную работу

Проделайте ход работы, зафиксировав полученные результаты в отчете. Создайте учетную запись, соответствующую имени в кафедральной сети (либо из ФИО). В зависимости от номера варианта задайте учетной записи пользователя категорию конфиденциальности:

- Четный – «Строго конфиденциально»;
- Нечетный, делится на 3 – «Конфиденциально»;
- Нечетный, остальные – «Не конфиденциально».

Для данной учетной записи проделайте следующие действия:

1. Создайте замкнутую программную среду в «жестком режиме» для ресурса «C:\Program Files \Internet Explorer» для созданной учетной записи пользователя.

2. Настройте контроль целостности для ресурса « D:\Полный доступ». Попытайтесь подменить содержащийся в данной папке файл «notepad.exe» файлом «C:\Windows\Regedit.exe». Проверьте работу механизма контроля целостности.

6. Контрольные вопросы

1. Для чего предназначен механизм контроля целостности (КЦ)?
2. Для чего предназначен механизм замкнутой программной среды?
3. Чем отличается «мягкий» режим ЗПС от «жесткого»?
4. Перечислите методы контроля целостности, используемые Secret Net.
5. Перечислите реакции на нарушение целостности файлов.
6. Для каких файлов следует настраивать контроль целостности?

Лабораторная работа №3
«Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование»

1. Цель работы

Целью данной работы является изучение функций системы защиты информации от несанкционированного доступа «Secret Net», связанных с регистрацией событий о несанкционированном доступе, получение навыков работы с журналами событий, навыков анализа сведений в журнале регистрации событий, навыков настройки и управления подсистемами аудита и теневого копирования Secret Net.

2. Краткие теоретические сведения

В журнале событий системы Secret Net (далее — журнал Secret Net) накапливается информация о событиях, регистрируемых на компьютере средствами системы защиты. Сведения, содержащиеся в журнале Secret Net, позволяют контролировать работу механизмов защиты (защита входа в систему, контроль аппаратной конфигурации, контроль целостности и др.). Состав регистрируемых событий определяется заданными параметрами действующей политики безопасности. В журнале Secret Net используется такой же формат данных и состав полей записей, как и в штатных журналах ОС Windows. Для локальной работы с записями журнала используется программа просмотра локальных журналов системы Secret Net.

Программа просмотра локальных журналов позволяет осуществлять загрузку и просмотр записей штатных журналов, хранящихся на компьютере локально. При этом сохраняется возможность загрузки

записей в другие средства работы с журналами ОС Windows.

При регистрации событий записи о них помещаются в соответствующие локальные журналы (штатные журналы ОС Windows и журнал Secret Net) и хранятся на компьютере локально. Пока записи хранятся в локальном хранилище, их можно загрузить в программу просмотра локальных журналов или в другие программы, позволяющие осуществлять загрузку журналов (кроме журнала Secret Net).

В сетевом режиме функционирования системы Secret Net локальные журналы хранятся в локальном хранилище до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов.

Окно «Программа просмотра журналов» представлено на рис.1.

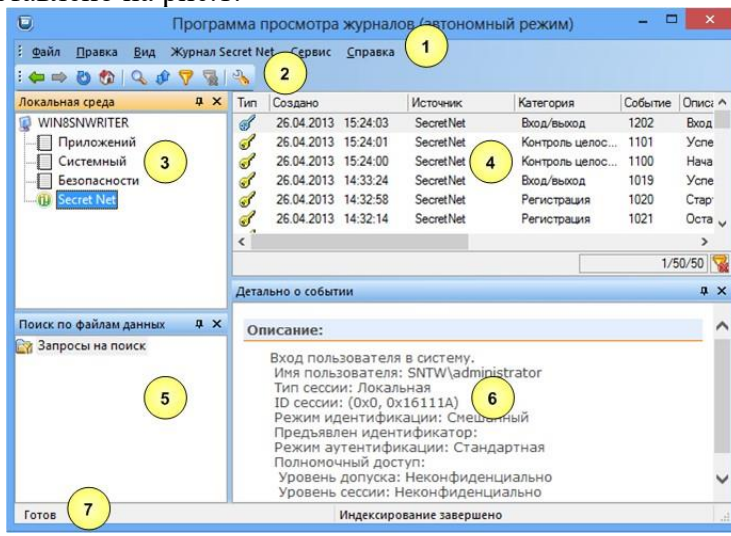


Рисунок 1 – Интерфейс программы просмотра журналов Secret Net

На данном рисунке обозначены следующие элементы программы:

(1) - Меню. Содержит команды управления программой.

(2) - Панель инструментов. Содержит кнопки быстрого вызова команд управления и программных средств.

(3) - Окно структуры. Содержит список, состоящий из журналов компьютера и журналов, загруженных в программу из файлов. Окно используется для выбора журнала.

(4) - Область отображения записей. Отображает записи выбранного журнала или запроса в табличной форме. Строки таблицы можно скопировать в буфер обмена, используя стандартные способы. Для отображения сведений о записи в виде списка полей наведите указатель мыши на нужную строку таблицы — через 1–2 секунды появится всплывающее окно. В зависимости от характеристик событий записи могут выделяться различными цветами. Настройка цветового оформления записей осуществляется при настройке параметров программы.

(5) - Окно запросов на поиск по файлам данных. Содержит список запросов для поиска по файлам данных в хранилище теневого копирования. Результатом поиска являются записи журнала Secret Net, относящиеся к найденным файлам. Список записей выводится в области отображения записей при выборе запроса.

(6) - Окно дополнительных сведений. Содержит подробную информацию о событии. Отображаемые сведения относятся к текущей выбранной записи.

Содержимое окна можно скопировать в буфер обмена, используя стандартные способы.

(7) - Строка сообщений. Отображает служебные сообщения программы, состояние индексирования хранилища теневого копирования, а также краткие подсказки к командам и кнопкам панели инструментов.

3. Теневое копирование

В хранилище теневого копирования помещаются дубликаты (копии) данных, выводимых на отчуждаемые носители информации. Хранилище дубликатов представляет собой специально организованное место в системной папке на локальном диске компьютера. Средства работы с хранилищем обеспечивают бесперебойную запись информации, невозможность несанкционированного доступа к хранящимся данным, а также выполнение различных служебных операций с содержимым (например, поиск, очистка хранилища и др.).

Доступ к хранилищу теневого копирования осуществляется в программе просмотра локальных журналов. При этом учитываются права доступа пользователя: если пользователю предоставлены привилегии для просмотра журналов— он получит доступ к хранилищу только для чтения. При наличии привилегий на управление журналами пользователь может совершать административные операции с хранилищем. Размер хранилища и методы его заполнения определяются заданными параметрами действующей политики безопасности.

В программе просмотра журналов предусмотрена возможность поиска в хранилище теневого копирования. Функция поиска реализована с

использованием компонента Windows Search, в котором для ускорения процесса поиска применяется индекс — база с подробными сведениями о файлах на компьютере. Формирование актуального индекса происходит при периодическом индексировании файлов. Запуск индексирования хранилища теневого копирования осуществляется автоматически в определенные моменты времени.

Новые файлы, поступившие в хранилище теневого копирования, могут отсутствовать в индексе на момент поиска. Поэтому если поиск не дал результатов, это может быть связано с отсутствием новых файлов в индексе. В программе просмотра журналов предусмотрена возможность принудительного запуска процесса индексирования хранилища.

При сохранении дубликата в хранилище теневого копирования для файла генерируется новое внутреннее имя на основе его контрольной суммы и метки времени. Расширение файла не меняется, но оно может быть удалено при достижении ограничения на максимальную длину имени файла. Имя файла дубликата в хранилище теневого копирования и исходное имя файла сопоставляются в записи о событии теневого копирования. Таким образом, с помощью записи журнала можно восстановить файл в том виде, в каком был осуществлен его вывод на отчуждаемый носитель.

При поиске по именам файлов в хранилище теневого копирования рассматриваются внутренние, а не исходные имена файлов. Если требуется выполнить поиск по исходным именам файлов, для этого следует воспользоваться средствами поиска по записям журнала Secret Net — исходные имена файлов указаны

в описаниях событий категории «Теневое копирование».

Компонент Windows Search, на базе которого реализован поиск в хранилище теневого копирования, по умолчанию поддерживает широкий спектр типов файлов для поиска по содержимому. Например, поиск по наличию слова или фразы выполняется в файлах с расширениями txt, htm, html, xml, а также в документах, сохраненных в приложениях пакета Microsoft Office (до версии Microsoft Office 2003 включительно).

4. Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player, VMware Workstation или Virtual Box, а также скачать архив с виртуальной машиной «Secret Net Client». Рекомендуется использовать ту же виртуальную машину, что и была использована в ходе выполнения лабораторной работы № 1 и 2. В противном случае, скачанный архив необходимо разархивировать.

Убедитесь, что вы запускаете виртуальную машину на системе виртуализации, соответствующей названию скачанного архива.

Желательно убедиться, что в настройках виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only») в случае, если используется система виртуализации VMware. При наличии на хосте оперативной памяти большого объема, можно увеличить выделяемый виртуальной машине объем ОЗУ (по умолчанию установлен 256 МБ).

5. Ход работы

1. Запустите виртуальную машину «Secret Net Client». После загрузки операционной системы войдите под локальной учетной записью **«Администратор»**. Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». Отключите ЗПС, если она была включена в ходе выполнения предыдущей лабораторной работы. Настройка событий, регистрируемых в журнале, осуществляется с помощью «Локальной политики безопасности» (Пуск\Все программы\Код безопасности\Secret Net\Локальная политика безопасности) в разделе «Параметры Secret Net\Регистрация событий» (рис. 2). Для каждой политики имеется два параметра «Отключено» и «Включено», которые подразумевают отключение или включение регистрации события (рис. 3). Включите регистрацию события “Контроль целостности: Изменение задачи”.

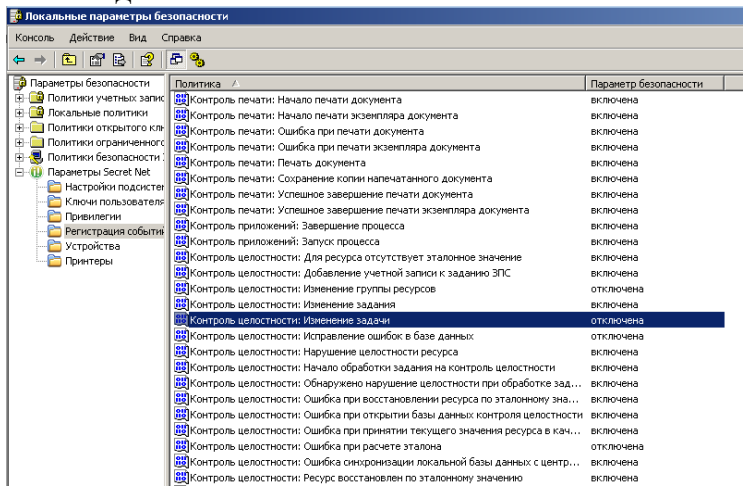


Рисунок 2 – Параметры регистрации событий

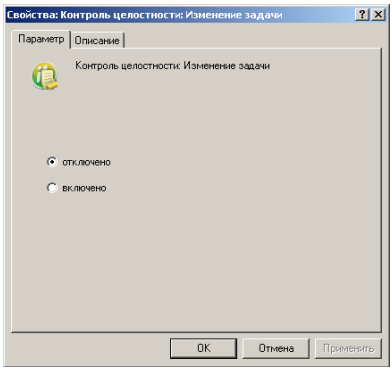


Рисунок 3 – Параметры политики

В Secret Net можно включить фиксацию событий различных категорий, относящихся к защитным подсистемам Secret Net. К ним относятся такие категории событий, как:

–Администрирование;

–Вход/Выход;

–Дискреционное управление доступом;

–Полномочное управление доступом;

–Замкнутая программная среда;

–Контроль конфигурации;

–Контроль печати;

–Контроль приложений;

–Контроль целостности;

–Общие события;

–Разграничение доступа к устройствам;

–Теневое копирование.

По умолчанию включены основные виды событий, необходимые для фиксации событий несанкционированного доступа на компьютере. Однако для снижения нагрузки на систему и уменьшения размеров журналов можно отключить фиксацию ненужных событий. Отключите фиксацию

событий вида «Общие события: Информационное событие». Для каждого из видов событий доступно описание, для ознакомления с которым необходимо открыть соответствующую вкладку в свойствах события (рис. 4).

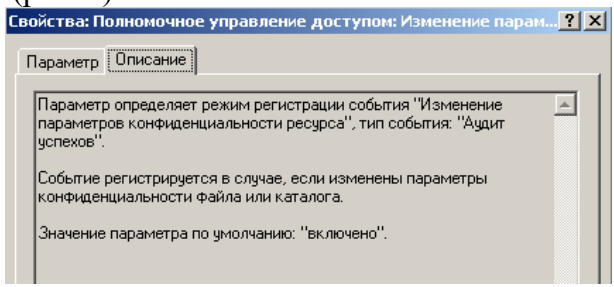


Рисунок 4 – Описание типа события Secret Net

2. Для того, чтобы запустить программу просмотра локальных журналов, необходимо выполнить команду «Пуск\Все программы\Код безопасности\Secret Net\Журналы». После этого появится главное окно программы со статистикой по различным журналам событий и типам событий (рис. 5). При запуске журнала информация может не отобразиться, предварительно откройте в каждый журнал, после этого статистика появится в главном окне (необходимо выделить «XP-MSDN»).

В журналах Secret Net могут фиксироваться следующие категории событий:

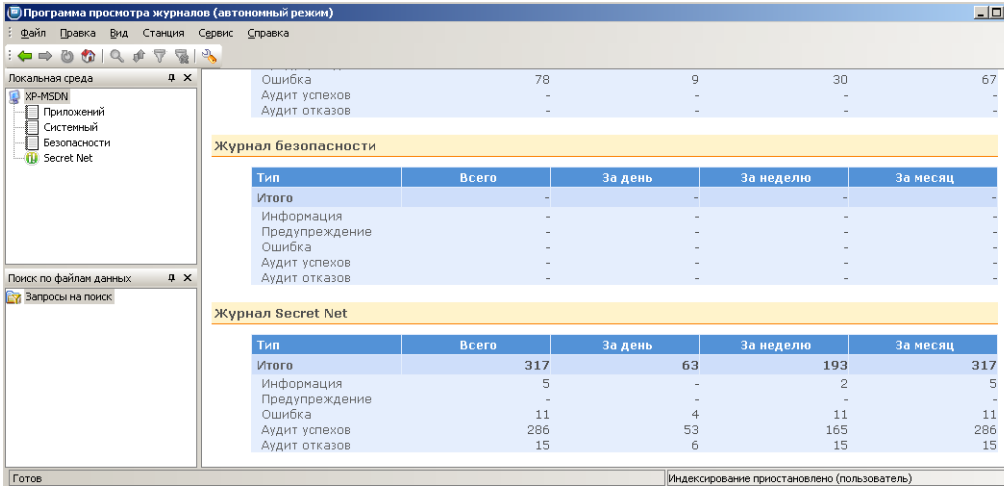
–Информация. Обозначает события, информирующие об успешном выполнении операций;

–Предупреждение. Обозначает события, предупреждающие об изменении состояния объектов или о создавшихся угрозах для безопасности системы;

–Ошибка. Обозначает события, предупреждающие о возникших неполадках при выполнении действий;

–Аудит успехов. Обозначает события, информирующие об успешном доступе;

–Аудит отказов. Обозначает события,



информирующие об отказе в доступе.

Рисунок 5 – Статистика по зафиксированным событиям

Откройте журнал Secret Net (XP-MSDN\Secret Net). В данном журнале фиксируются события системы Secret Net, произошедшие в ходе работы пользователей в операционной системе (рис. 6). Для данных событий фиксируются такие параметры, как:

–Тип события

–Дата и время создания события

–Источник события

–Категория события

–Код события

–Описание события

–Пользователь

–Компьютер, на котором произошло событие

–Дополнительная информация, раскрывающая подробности события

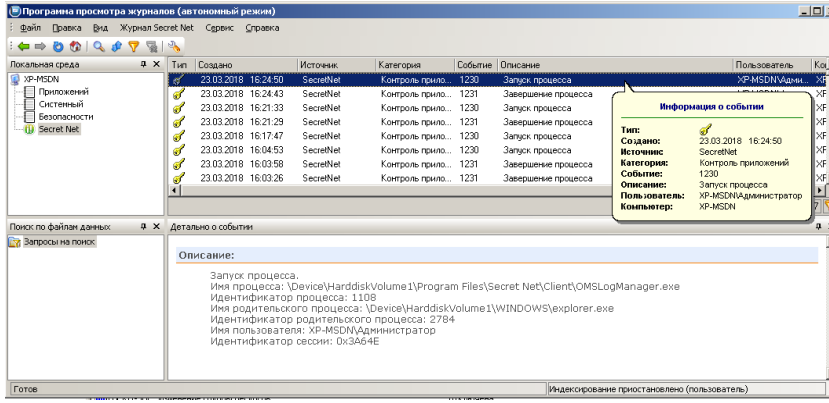


Рисунок 6 – Окно событий в журнале Secret Net

После выполнения ходы работы необходимо в соответствии с заданием, найти соответствующие события в журнале.

5.1. Настройка теневого копирования

Функцию теневого копирования можно включить для всех устройств следующих типов:

–устройства, подключаемые к системе в качестве дисков;

–принтеры.

Для общего управления функцией теневого копирования:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net».

2. Выберите папку «Настройки подсистем». В правой части окна появится список параметров.

3. Вызовите контекстное меню для параметра «Контроль устройств: Теневое копирование» и выберите в нем команду «Свойства». На экране появится диалог настройки параметра. Включите теневое копирование, настроив параметры в соответствии с рисунком (рис.7).

4. Настройте действие параметра и нажмите кнопку «OK».

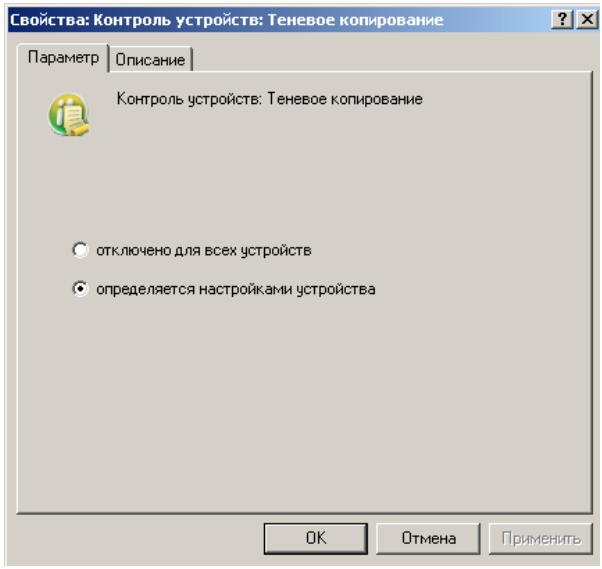


Рисунок 7 – Контроль устройств: Теневое копирование

Включим теневое копирование для съемного диска. Для выполнения данного задания необходимо подключить к компьютеру, а затем к виртуальной машине USB - носитель (необходимо проверить меню VMware Player или Virtual Box на наличие проброса USB-устройства к виртуальной машине).

Для управления режимом сохранения копий в списке устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net»
2. Выберите папку «Устройства». В правой части окна появится список устройств.
3. Выберите в списке объект (предварительно подключив флэшку к виртуальной машине), вызовите контекстное меню и выберите команду «Свойства». На экране появится диалог для настройки параметров объекта.
4. Перейдите к группе параметров «Настройки» (рис. 8).
5. Удалите отметку из поля «Наследовать настройки контроля от родительского объекта». После этого станут доступны параметры контроля устройства.
6. Отметьте режим контроля «Подключение устройства разрешено».
7. Установите отметку «Сохранять копию информации, записываемой на устройство».

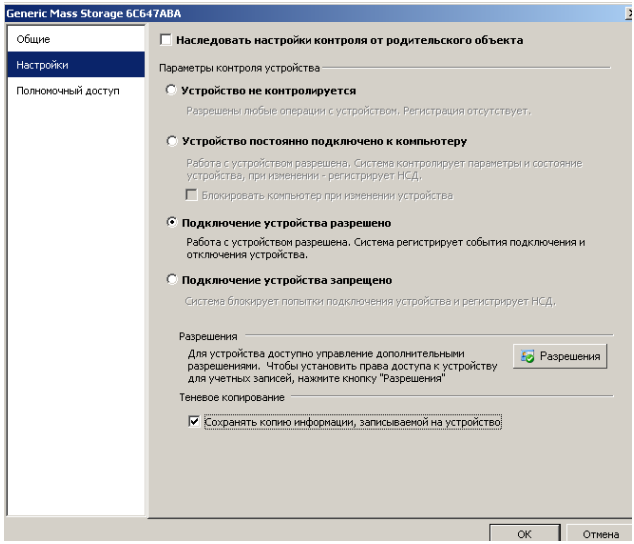


Рисунок 8 – Группа параметров «Настройка»

5.2. Изменение параметров хранилища теневого копирования

При настройке параметров можно изменить ограничение максимального объема хранилища, а также включить или отключить возможность перезаписи. Для настройки параметров хранилища:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net»
2. Выберите папку «Настройки подсистем». В правой части окна появится список параметров.
3. В списке параметров выберите элемент «Теневое копирование: Размер хранилища» и вызовите диалог настройки параметра.
4. Укажите размер 15% от дискового пространства (рис. 9).

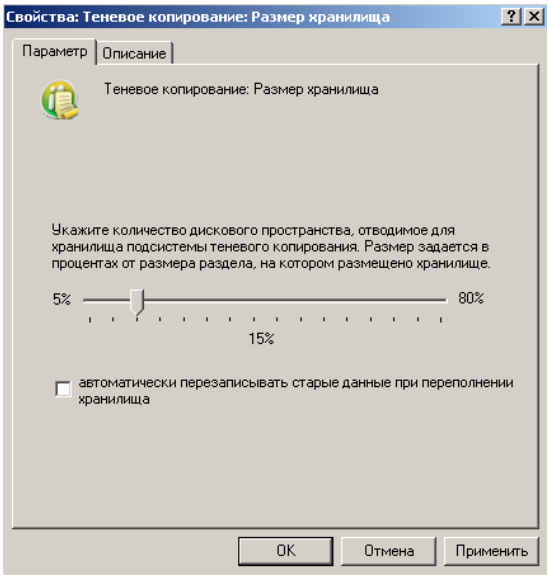


Рисунок 9 – Выбор размера теневого хранилища

Подключите устройство хранения к виртуальной машине и запишите на него несколько текстовых документов, находящихся на диске «D:\». После записи будет зарегистрировано событие, относящееся к категории «Теневое копирование» (рис. 10), а копия документа будет храниться в теневом хранилище (рис. 11). Хранилище располагается по адресу “C:\System Volume Information\SNCloneVault\”. Данный каталог можно открыть либо вставив в проводнике полный адрес данного каталога, либо перейдя по ссылке в журнале событий.

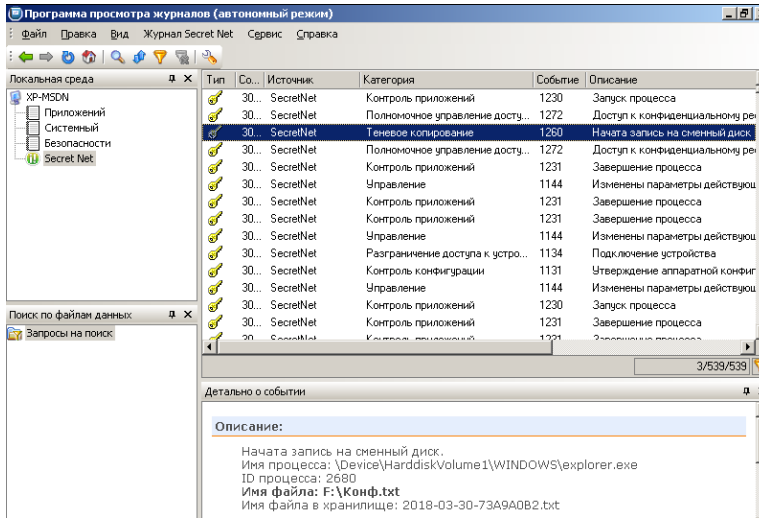


Рисунок 10 – Регистрация события теневого копирования

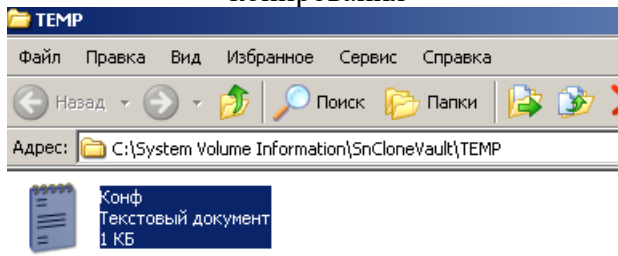


Рисунок 11 – Хранилище теневого копирования

6. Задание на лабораторную работу

При выполнении задания необходимо использовать учетную запись, созданную в ходе выполнения лабораторной работы № 1 (включающую в себя ФИО студента). Некоторые из событий уже могут находиться в журнале, для некоторых событий необходимо воссоздать ситуацию для их фиксации в журнале. Для каждого заданий в отчете к лабораторной работе должны быть предоставлены

скриншоты события с его описанием. Убедитесь, что на скриншотах с зафиксированными событиями отображается ваша учетная запись.

1. В групповой политике (параметры Secret Net - Настройки подсистем) включить режим «Стандартная аутентификация» для параметра «Вход в систему: Режим аутентификации пользователя», выполнить попытки входа пользователя в систему с вводом неверного пароля и с вводом правильного имени и пароля пользователя. Проверить, имеется ли зарегистрированное событие (аудит отказов) в программе просмотра журналов.

2. Запустить приложение, которое разрешено для запуска (входит в задание ЗПС). Зафиксировать регистрацию события в программе просмотра журналов (тип «Аудит успехов). ЗПС можно включить в мягком режиме.

3. Запустить приложение, которое запрещено для запуска (не входит в ЗПС). Зафиксировать регистрацию события в программе просмотра журналов (тип «Аудит отказов). ЗПС можно включить в мягком режиме.

4. Войти в систему под своей учетной записью и подключить устройство, для которого разрешено подключение к системе. Зафиксировать регистрацию события в программе просмотра журналов (тип «Аудит успехов).

5. Войти в систему под своей учетной записью и подключить устройство, для которого запрещено подключение к системе. Зафиксировать регистрацию события в программе просмотра журналов (тип «Аудит отказов).

6. При включенном теневом копировании, скопировать на съемный носитель текстовый файл,

затем найти соответствующее событие и файл в хранилище теневого копирования.

7. Контрольные вопросы

1. Для чего нужен журнал событий?
2. Какой формат данных используется в журнале Secret Net?
3. Приведите несколько категорий регистрации событий.
4. Какая информация фиксируется для каждого события?
5. Кто может работать с журналом?
6. Для чего нужно теневое копирование?
7. Для каких устройств может осуществляться теневое копирование?

Лабораторная работа №4
«Secret Net. Программа оперативного управления. Удаленное управление защищаемым компьютером»

1. Цель работы

Целью данной работы является изучение основного функционала средств оперативного управления системы Secret Net, получение навыков работы с программой оперативного управления Secret Net, навыков настройки, удаленного управления и мониторинга защитных подсистем автоматизированных систем.

2. Краткие теоретические сведения

В сетевом режиме функционирования системы Secret Net для централизованного управления защищаемыми компьютерами может использоваться компонент "Secret Net 7 – Программа управления". Данный компонент (далее – программа оперативного управления) предоставляет следующие основные возможности:

−конфигурирование сетевой структуры системы Secret Net;

−мониторинг и оперативное управление защищаемыми компьютерами;

−работа с централизованными журналами.

Программа оперативного управления может функционировать в различных режимах:

−режим конфигурирования;

−режим мониторинга и централизованного аудита;

−автономный режим без подключения к серверу безопасности.

Выбор нужного режима работы программы осуществляется при ее запуске. При установке компонентов системы Secret Net формируется начальная конфигурация структуры оперативного управления (ОУ). Как правило, начальная конфигурация достаточна для функционирования компонентов и выполнения администратором безопасности своих функций. Однако в процессе эксплуатации может возникнуть необходимость в изменении конфигурации с целью создания более удобных условий управления или для актуализации сетевой структуры.

При конфигурировании осуществляется:

−редактирование структуры оперативного управления;

−настройка параметров, применяемых на серверах безопасности (СБ);

−настройка параметров, применяемых на компьютерах с установленным клиентским ПО системы Secret Net в сетевом режиме функционирования (далее – защищаемые компьютеры или агенты).

3. Объекты конфигурирования

При конфигурировании структуры ОУ выполняются операции со следующими объектами:

−серверы безопасности – представляют компьютеры, на которых установлено программное обеспечение "Secret Net 7 – Сервер безопасности";

−агенты – представляют компьютеры, на которых установлено программное обеспечение "Secret Net 7" в сетевом режиме функционирования.

Из объектов формируется структура оперативного управления. Между объектами устанавливаются зависимости, определяющие подчиненность агентов серверам безопасности, а также подчиненность серверов безопасности между собой. Чтобы использовать возможности оперативного управления агентом, необходимо подчинить агент серверу безопасности.

4. Типовые задачи при конфигурировании

Одним из важных вопросов обеспечения защищенности рабочих станций является этап первоначальной и последующей настройки компонентов системы защиты Secret Net. К типовым задачам администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования, относятся:

– изменение подчиненности объектов в структуре ОУ;

– настройка почтовой рассылки уведомлений о событиях НСД;

– настройка параметров сетевых соединений;

– настройка параметров сбора локальных журналов;

– настройка параметров архивирования журналов в базе данных сервера безопасности;

– управление лицензиями на использование компонентов;

– управление привилегиями для работы с программой.

5. Мониторинг и оперативное управление

Под мониторингом системы защиты подразумевается контролирование состояния агентов. Контроль осуществляется в режиме реального времени. Оперативное управление заключается в незамедлительном воздействии на защищаемые компьютеры посредством передачи агентам соответствующих команд.

Основными задачами мониторинга и оперативного управления являются:

−контролирование и оповещение о произошедших событиях несанкционированного доступа;

−контролирование текущего состояния защищаемых компьютеров (какие компьютеры являются активными, какие пользователи работают на компьютерах и пр.);

−выполнение действий с защищаемыми компьютерами при возникновении угроз для безопасности системы.

В дополнение к перечисленным задачам, в программе реализована возможность управления параметрами групповых политик для агентов на компьютерах под управлением ОС Windows. Параметры могут быть настроены как для агентов (в локальных политиках безопасности), так и для других объектов: серверов безопасности, доменов и организационных подразделений.

6. Централизованный аудит

Под аудитом системы защиты понимается анализ информации о событиях, происходивших в системе в течение некоторого промежутка времени. Информация о событиях накапливается в журналах регистрации

событий. Для работы с централизованными журналами используется программа оперативного управления.

Основными задачами централизованного аудита являются:

−контролирование состояния защищенности системы;

−выявление причин произошедших изменений;

−определение обстоятельств, которые привели к изменению состояния защищенности системы или к НСД;

−установление времени изменений.

Для выполнения перечисленных и сопутствующих задач в программе реализованы различные возможности поиска, фильтрации и представления информации.

7. Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player, VMware Workstation или Virtual Box, а также скачать архив с виртуальной машиной «Secret Net Client» и «Secret Net Server». Скачанные архивы необходимо разархивировать. Рекомендуется использовать ту же виртуальную машину («Secret Net Client»), что и была использована в ходе выполнения предыдущей лабораторной работы. В противном случае, скачанный архив необходимо разархивировать.

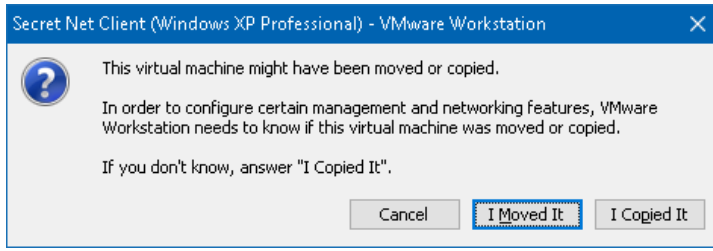
Убедитесь, что вы запускаете виртуальную машину на системе виртуализации, соответствующей названию скачанных архивов.

Желательно убедиться, что в настройках виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only») в случае, если используется система виртуализации VMware. При

наличии на хосте оперативной памяти достаточного объема, можно увеличить выделяемый виртуальным машинам объем ОЗУ (по умолчанию установлен 256 МБ).

8. Ход работы

Запустите клиентскую и серверную виртуальные машины. Для настройки конфигурации виртуальных машин VMware задаст вопрос о том были ли они скопированы или перемещены (рис. 1), выберите вариант «I Moved It» для обеспечения стабильности



работы виртуальной машины (виртуальная машина перемещена). Войдите под учетной записью **Администратор** в домен SAM на сервере (рис. 2).

Рисунок 1 – Запрос конфигурации при запуске виртуальной машины

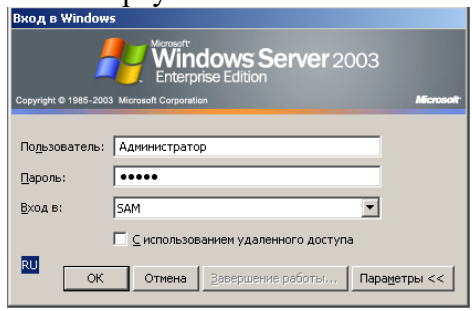


Рисунок 2 – Вход в систему под доменной учетной записью «Администратор»

Для запуска программы оперативного управления:

Выберите в главном меню Windows команду «Пуск | Все программы | Код безопасности | Secret Net | Программа управления». На экране появится стартовый диалог программы для выбора режима работы (рис. 3).

В поле «Сервер безопасности» введите или выберите имя сервера безопасности, с которым будет установлено соединение. Для получения списка всех

зарегистрированных серверов безопасности нажмите кнопку справа от поля (выполнение операции может занять некоторое время).

Рисунок 3 – Стартовое окно программы управления Secret Net

8.1. Режим «Мониторинг и управление»

Начните работу с программой в режиме «Мониторинг и управление». После выполнения подключения к серверу отобразиться диаграмма (рис. 4). На ней слева изображена доменная структура, а справа - сервер безопасности Secret Net и подчиненный ему компьютер. В этом режиме можно изменять подчиненность рабочих станций серверам безопасности. В данном случае имеется только один сервер безопасности, которому подчинена одна рабочая станция.

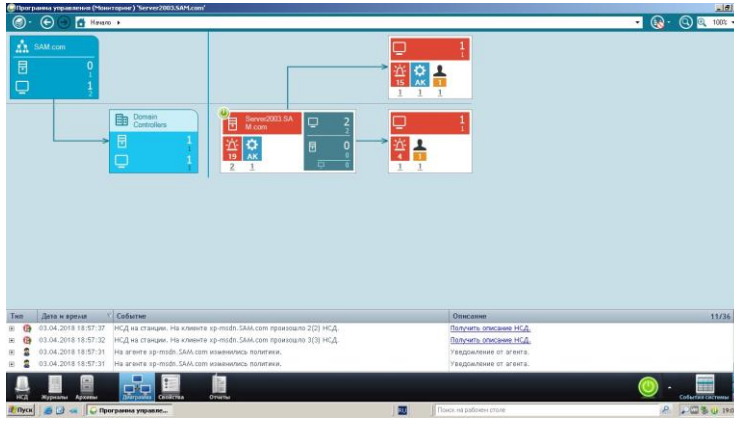
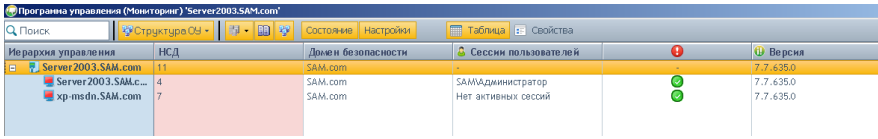


Рисунок 4 – Окно программы управления Secret Net в режиме «Мониторинг и управление»

Нажмите на кнопку «Свойства» в нижней панели для того, чтобы открыть окно с настройками Secret Net (рис. 5). Тип и количество настроек меняется в зависимости от выбранного элемента. В режиме «Мониторинг и управление» для редактирования



доступны политики Secret Net. Данные настройки доступны для всех типов элементов - «Домен», «Контроллер домена», «Сервер безопасности», «Рабочая станция», и применяются ко всем подчиненным компьютерам.

Рисунок 5 – Окно свойств в программе оперативного управления Secret Net

В данном окне можно выполнить настройки как для отдельных защищаемых компьютеров, так и для иерархии управления. В данном случае, красными мониторами обозначены отдельные защищаемые компьютеры, с установленной клиентской частью системы защиты Secret Net (в том числе она установлена на серверной виртуальной машине), а зеленым системным блоком обозначен сервер безопасности. Выберите в списке слева сервер безопасности «Server2003.SAM.com» и перейдите в режим изменения настроек сервера, нажав кнопку «Свойства». Откройте вкладку «Политики Secret Net» (рис. 6).

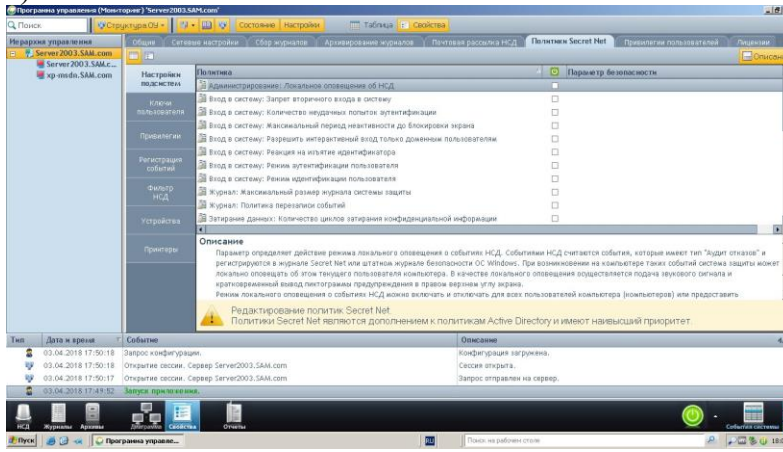


Рисунок 6 – Окно «Политики Secret Net»

Вкладка содержит списки параметров, соответствующих содержимому раздела «Параметры Secret Net» в стандартных оснастках управления групповыми политиками. На вкладке «Локальные политики» представлены параметры локальной политики безопасности выбранного агента. Вкладка «Политики Secret Net» содержит списки параметров, которые могут применяться на компьютерах, относящихся к домену, к организационному подразделению или к серверу безопасности – в зависимости от того, какой объект выбран в иерархии управления.

Параметры групповых политик применяются на компьютерах в следующей последовательности:

1. Параметры локальной политики безопасности.
2. Параметры политик, заданные в стандартных оснастках управления – в соответствии с действием механизма групповых политик Windows, сначала применяются параметры доменных политик и затем параметры политик для организационных подразделений.
3. Параметры политик, заданные в программе оперативного управления – сначала применяются параметры домена, затем параметры организационных подразделений и в конце параметры сервера безопасности.

Таким образом, параметры политик, заданные для сервера безопасности, имеют наивысший приоритет.

Во вкладке «Настройки подсистем» отредактируйте параметры (рис. 7). Данные параметры необходимо предварительно включить, поставив в соответствующей колонке галочку:

–«Вход в систему: Количество неудачных попыток аутентификации» = 3

–«Вход в систему: Разрешить интерактивный вход только доменным пользователям» = включено.

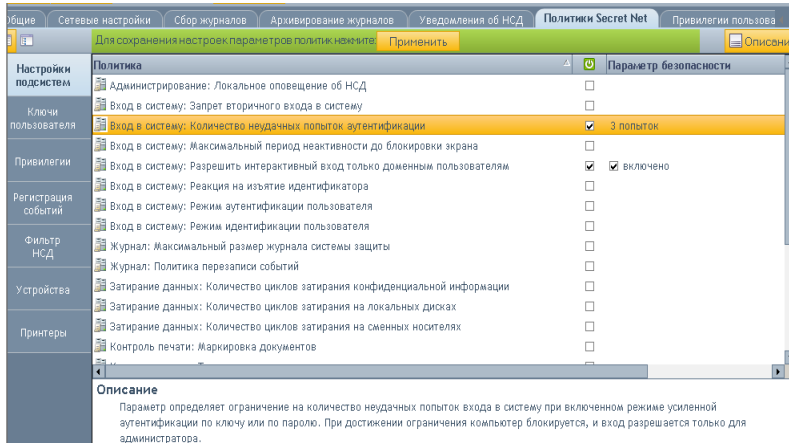


Рисунок 7 – Настройка политик защитных подсистем Secret Net

Во вкладке «Устройства» задайте политику устройств, которая будет использоваться в текущей иерархии управления (рис. 8). Нажмите кнопку «Задать политику устройств» и отредактируйте параметры:

–«Сменные диски», «Оптические диски» – подключение запрещено (необходимо также поставить галочку для включения политики).

–«Устройства хранения» – отключить наследование и запретить подключение устройства.

–«Сеть» - запретить подключение устройств. Отключить наследование и разрешить подключение устройств для соединения Ethernet.

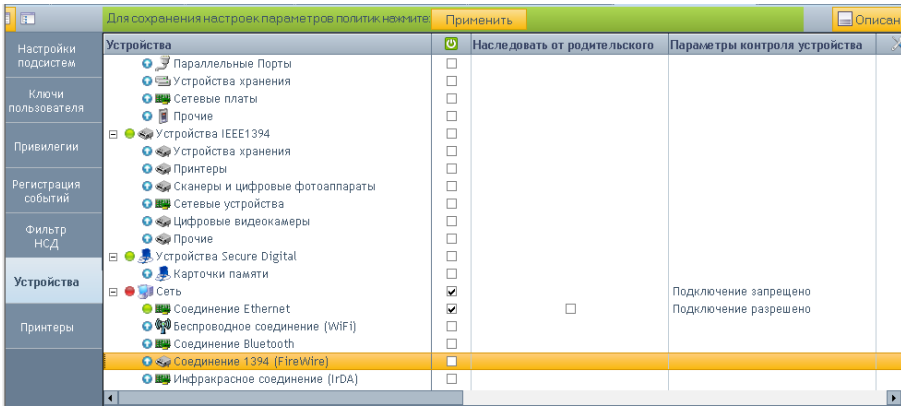


Рисунок 8 – Политики устройств Secret Net

Нажмите кнопку «Применить» для сохранения изменений в политиках. Просмотрите доступные настройки в остальных вкладках политик Secret Net.

Перейдите к диаграмме (иконка слева снизу). Дважды щелкнув по иконке сервера безопасности (Server2003.SAM.com) будет открыт вид программы управления с отображением защищаемых компьютеров (рис. 9). На данной диаграмме выберите рабочую станцию «XP-MSDN» и правой кнопкой мыши выберите действие – «Команды -> Применить групповые политики». С помощью данной команды параметры Secret Net, которые хранятся в групповых политиках, будут принудительно применены на защищаемом компьютере.

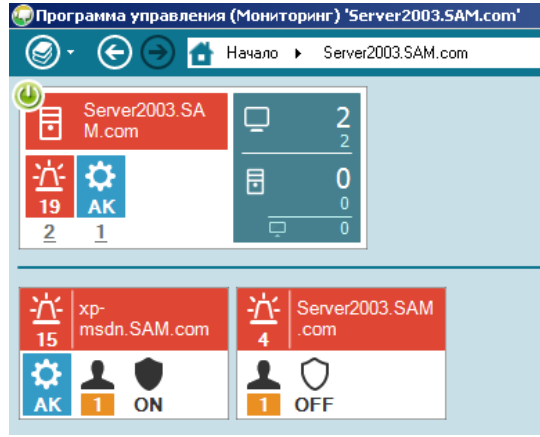


Рисунок 9 – Окно программы управления с отображением защищаемых компьютеров

Войдите под доменной учетной записью **«Администратор»** на клиентской виртуальной машине. Попробуйте подключить съемный USB-накопитель (флэшку) к клиентской виртуальной машине. Если данное устройство ранее не подключалось то оно будет заблокировано в соответствии с действующей политикой Secret Net. При этом CD и Floppy дисководы остаются работающими, потому что были определены в системе как разрешенные до применения политики. Соответственно данная политика применяется только ко вновь подключенным устройствам. Проверьте, открыв локальную политику безопасности на клиенте (рис. 10). Если USB-устройство разрешено к подключению в локальной политике, запретите его.

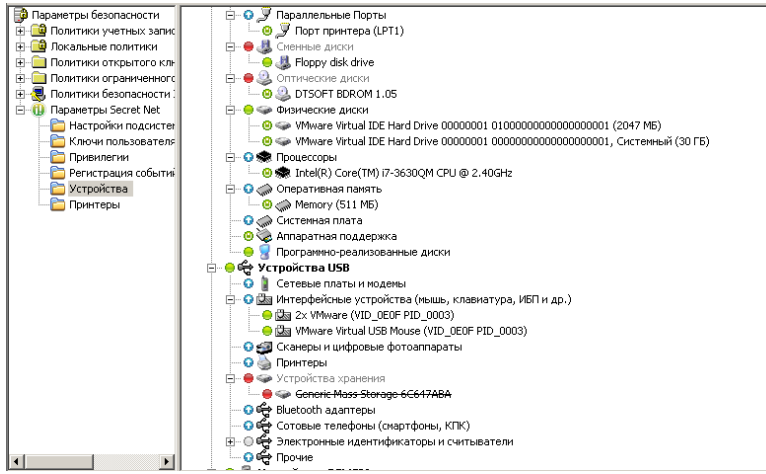


Рисунок 10 – Политика устройств в локальной политике Secret Net на клиентском компьютере

Откройте настройки клиентской машины «XP-MSDN» в программе оперативного управления, выберите вкладку «Локальные политики», а в ней вкладку «Устройства». Запретите подключенные CD и Floppy дисководы (рис. 11). Нажмите кнопку «Применить». Проверьте, что данные устройства были запрещены на клиентской машине.

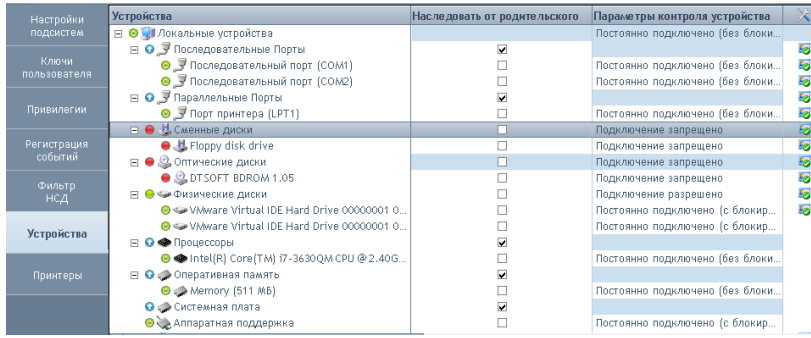


Рисунок 11 – Запрет устройств Floppy drive и CD-ROM в политике устройств Secret Net

При подключении запрещенного съемного устройства должно возникнуть событие несанкционированного доступа (НСД), которое отображается на диаграмме управления Secret Net значком сирены. При этом событие НСД отображается как на сервере, так и на клиенте в программе управления.

На диаграмме управления выберите сервер безопасности «Server2003.SAM.com», вызовите контекстное меню, в котором выберите «Запросы -> Журнал НСД -> Все (Неквитированные НСД)». В нижней части появится сообщение о том, что журнал получен (Если события не отображаются, нажмите на кнопку «События системы» в нижнем правом углу). Откройте данный журнал (рис. 12).

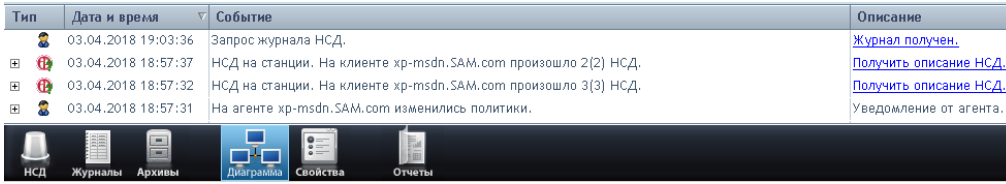


Рисунок 12 – Запрос журнала НСД с защищаемых компьютеров

Откроется журнал событий НСД (рис. 13). В данном журнале отображается тип событий НСД, компьютер на котором оно произошло и детальное описание события НСД.

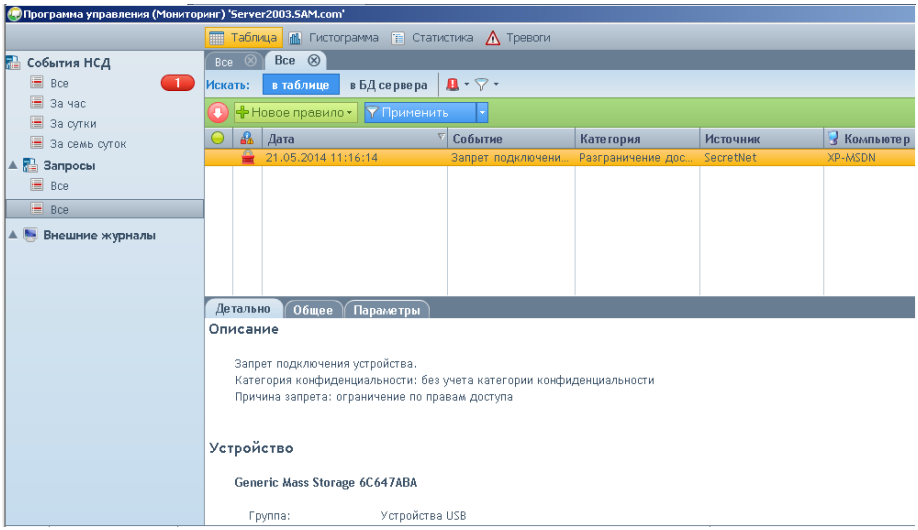


Рисунок 13 – Журнал событий НСД Secret Net

Выберите одно из событий и в контекстном меню нажмите «Квитировать НСД». Администратор при квитировании должен оставить комментарий о том, какие действия он предпринял после возникновения данного события или какую-либо другую

информацию, связанную с его действиями при данном событии НСД. Можно одновременно квитировать несколько событий НСД, выделив их с помощью клавиши «Shift». Квитируйте все НСД. Если вернуться на диаграмму (рис. 14), изображения компьютеров станут зеленого цвета, т.к. все события НСД были квитированы. Изображение может быть синего цвета, если осталось неутвержденное изменение аппаратной конфигурации.

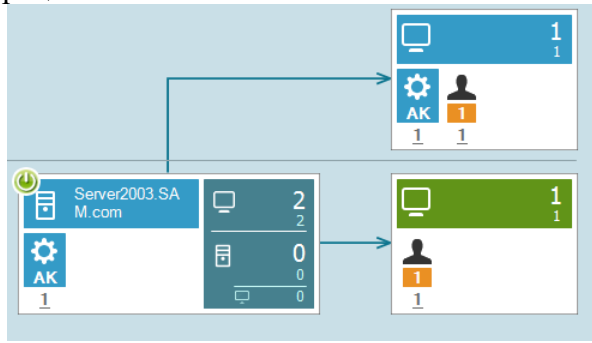
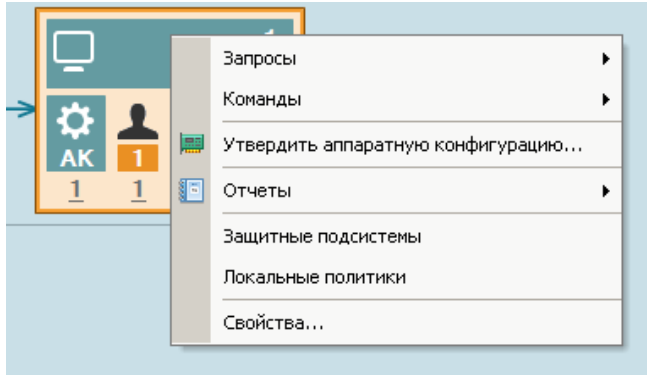


Рисунок 14 – Диаграмма защищаемых компьютеров Secret Net после квитирования НСД

В случае изменения аппаратной конфигурации компьютера, на диаграмме появится изображение шестеренки с подписью АК. Если на вашей диаграмме нет данного значка, измените состав оборудования клиентской виртуальной машины следующим образом: выключите клиентскую виртуальную машину, откройте параметры данной виртуальной машины и измените количество доступной



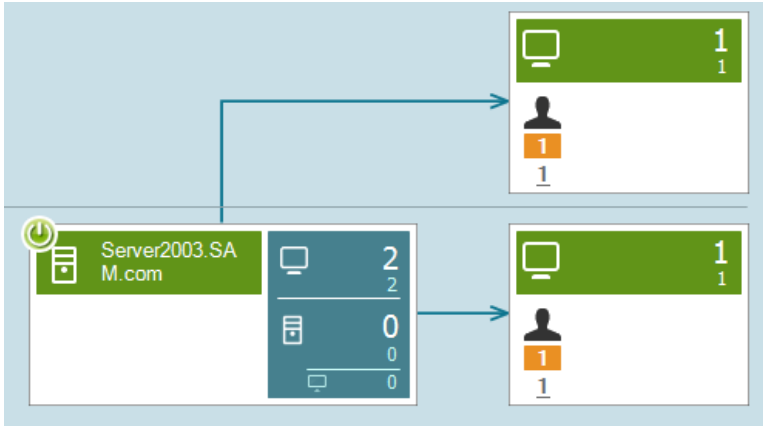
оперативной памяти, после чего запустите данную виртуальную машину. Secret Net должен обнаружить изменения в аппаратной конфигурации виртуальной машины. Вызвав контекстное меню на диаграмме, можно утвердить изменение аппаратной конфигурации (рис. 15).

Рисунок 15 – Запрос на утверждение аппаратной конфигурации

Далее будет отображены устройства, которые были извлечены, либо подключены с момента последнего утверждения конфигурации (рис. 16). В случае, если изменение аппаратного обеспечения было инициировано администратором или он был ознакомлен с действиями сотрудника, конфигурация утверждается. В ином случае администратор должен выяснить, по какой причине сотрудник на защищаемом компьютере изменяет состав подключенного оборудования.

Рисунок 16 – Окно утверждения аппаратной конфигурации

После этого, изображения компьютеров должны



стать зеленого цвета и диаграмма будет выглядеть следующим образом (рис. 17):

Рисунок 17 – Диаграмма защищаемых компьютеров Secret Net после утверждения аппаратной конфигурации

Просмотрите доступные команды удаленного управления рабочими станциями. Проверьте возможность блокирования, разблокирования и перезагрузки рабочей станции «XP-MSDN» (рис. 18).

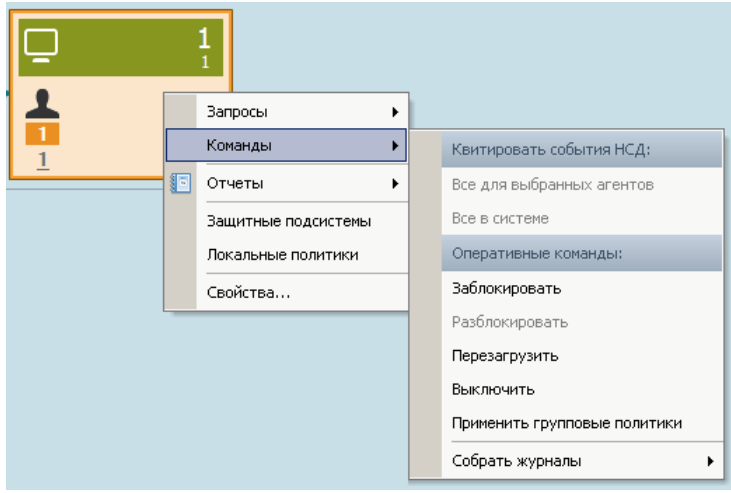


Рисунок 18 – Команды удаленного управления Secret Net

Выберите в контекстном меню рабочей станции «XP-MSDN» параметр «Защитные подсистемы». В данном окне можно включать и отключать различные защитные подсистемы на компьютерах (рис. 19). Отключите подсистему контроля устройств. Изменения в работе подсистем происходят только после перезагрузки. Перезагрузите клиентскую машину с сервера. Попробуйте подключить флэшку к клиентской виртуальной машине.

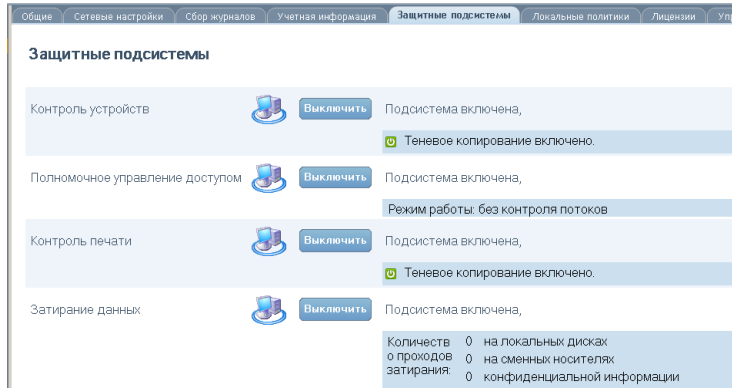


Рисунок 19 – Окно изменения состояния защитных подсистем Secret Net

Просмотрите и создайте доступные для рабочей станции отчеты (рис. 20).

Построение отчета «Паспорт ПО» может занять некоторое время (рис. 21, 22). Проверьте, какая информация фиксируется в отчетах.

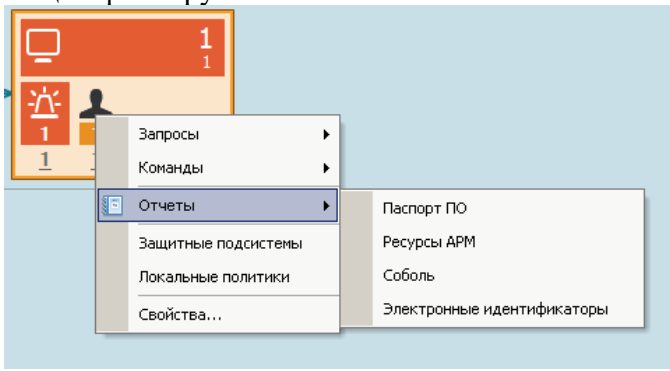
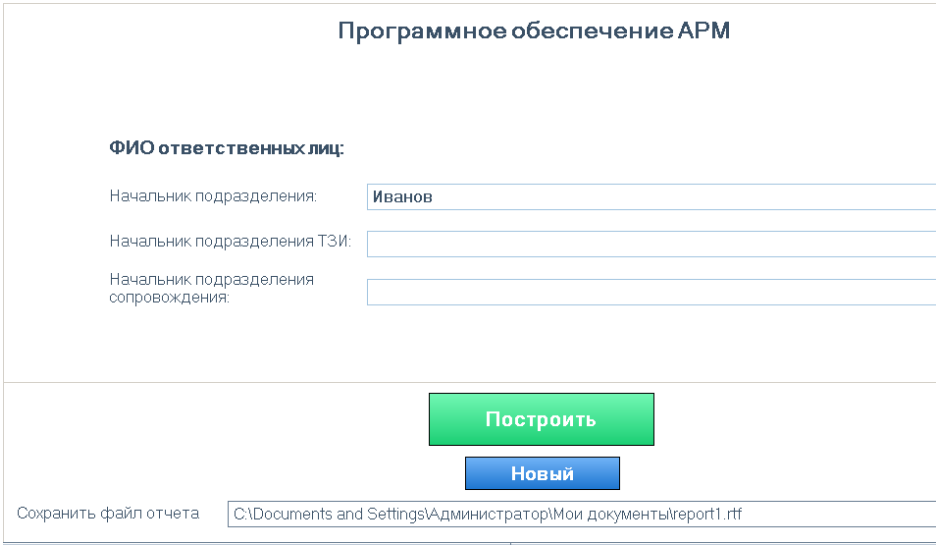


Рисунок 20 – Виды отчетов по защищаемому компьютеру

Рисунок 21 – Окно создания отчета «Паспорт ПО»



Паспорт ПО АРМ

АРМ:	XP-MSDN
Подразделение:	Course Unit
Наименование АС:	SN1
Операционная система:	Microsoft Windows XP Professional, 5.1.2600, Service Pack 3
Рабочее место:	Computer1
Номер системного блока:	1

Название ПО	Разработчик	Назначение	Объем (Кбайт)	Контрольная сумма	Примечание
VMware Tools	VMware, Inc.		10555021	B6F531C5	
Microsoft .NET Framework 3.0 Service Pack 2	Microsoft Corporation		79950314	45FD2195	
MSXML 4.0 SP3 Parser	Microsoft Corporation		1571905	67C22198	

Рисунок 22 – Содержание отчета «Паспорт ПО»

8.2. Режим конфигурирования

Откройте программу управления Secret Net в режиме конфигурирования. В данном режиме недоступны функции управления компьютерами,

просмотра отчетов, журналов событий и НСД (рис. 23).

Рисунок 23 – Панель с доступными функциями в режиме конфигурирования Secret Net.

Одной из основных функций в данном режиме является редактирование иерархии подчинения серверов безопасности Secret Net. Дважды щелкнув по серверу безопасности откройте диаграмму с отображением защищаемых компьютеров (рис. 24). В данной лабораторной работе имеется только два защищаемых компьютера, при этом свободные компьютеры, не подчиненные серверам безопасности отсутствуют.

Для того, чтобы появился неподчиненный компьютер, выведем из подчинения агента «XP-MSDN». Для этого правой кнопкой мыши для агента «xp-msdn.SAM.com» выберите команду «Вывести из подчинения». Данный агент исчезнет из диаграммы (рис. 25). Далее подчиним данный компьютер серверу безопасности, выбрав в контекстном меню команду «Подчинить объекты». В появившемся окне доступен список неподчиненных компьютеров (рис. 26). Выберите «xp-msdn.SAM.com» и нажмите кнопку «Применить». Данный агент вновь появится в списке подчиненных компьютеров.

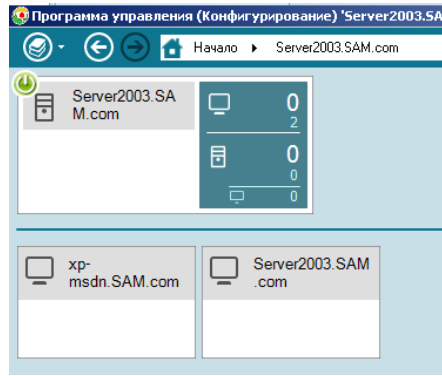


Рисунок 24 – Диаграмма подчинения в режиме «Конфигурирование» Secret Net

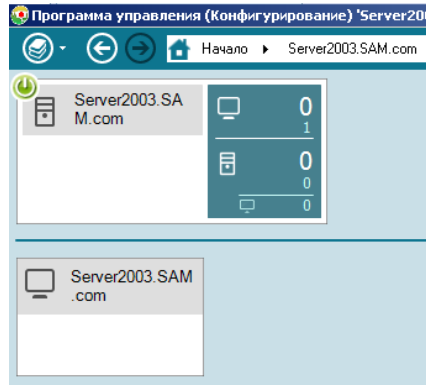


Рисунок 25 – Диаграмма подчинения после вывода агента «XP-MSDN»

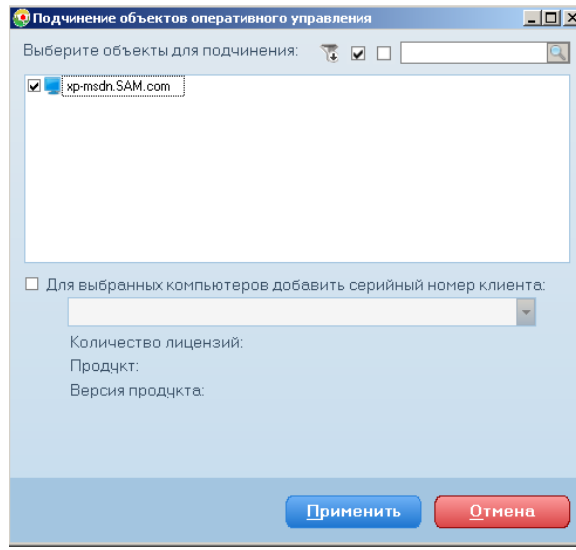


Рисунок 26 – Окно «Подчинение объектов оперативного управления»

Откройте свойства сервера безопасности. Выберите вкладку «Сетевые настройки» (рис. 27). Данные параметры используются при установке сетевого соединения объекта с сервером безопасности, которому подчинен данный объект. Если параметры сетевых соединений не заданы (имеют нулевые значения), связь объекта с родительским сервером не будет устанавливаться.

Сетевое взаимодействие компонентов системы Secret Net дает определенную нагрузку на каналы связи. Устойчивость сетевых соединений и затрачиваемое время на передачу данных зависят от пропускной способности сети. Если пропускная способность низкая (например, при использовании модемного соединения), могут проявляться

длительные задержки при установлении соединений и даже сбои при передаче данных.

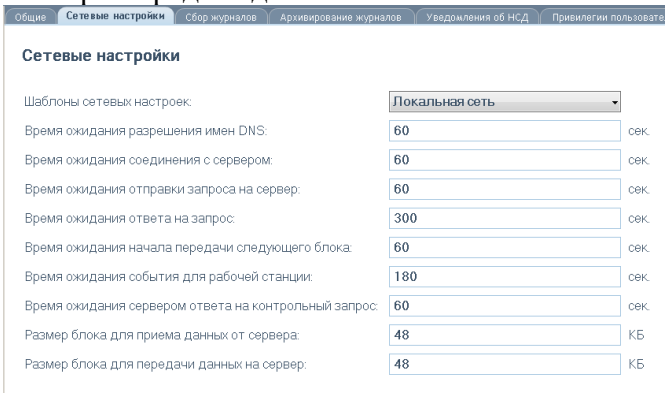


Рисунок 27 – Параметры сетевых соединений

Откройте вкладку «Сбор журналов». На данной вкладке можно настроить параметры передачи локальных журналов. Содержимое локальных журналов защищаемых компьютеров должно своевременно поступать в централизованные журналы в базе данных сервера безопасности. Длительные перерывы в отправке могут привести к переполнению локальных журналов или к чрезмерной нагрузке на сервер безопасности и каналы связи при получении больших объемов данных. Задайте ежедневный сбор журналов на сервер, в дополнение к этому включите параметры «Производить сбор журналов при подключении агента к серверу безопасности» и «Производить сбор журналов при заполнении на 80 % и более» (рис. 28).

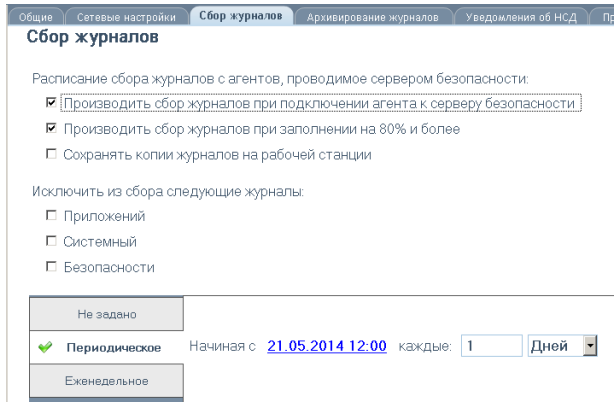


Рисунок 28 – Параметры сбора журналов

Откройте вкладку «Архивирование журналов». На данной вкладке можно настроить параметры архивирования централизованных журналов, в том числе задать расписание автоматического архивирования журналов. Архивирование применяется к записям журналов, которые поступили от подчиненных защищаемых компьютеров и хранятся в базе данных сервера безопасности. Задайте архивирование журналов по расписанию - «Еженедельное» архивирование (рис. 29).

С целью обеспечения сохранности информации следует проводить регулярное архивирование базы данных. Например, в некоторых версиях СУБД Oracle действуют ограничения на объем баз данных. Если размер базы превысит ограничение, поступление новой информации будет невозможно до очистки БД.

Наряду с обеспечением сохранности информации архивирование дает возможность вывести из базы данных неактуальные сведения, чтобы сократить время выполнения запросов к БД. При необходимости просмотра старых записей о событиях в программу

оперативного управления можно загрузить файлы архивных копий.

Рисунок 29 – Параметры архивирования журналов

Откройте вкладку «Привилегии пользователей» (рис. 30). Данная вкладка предназначена для просмотра и предоставления привилегий пользователям программы оперативного управления.

Пользователям и группам пользователей можно назначать следующие привилегии для управления сервером безопасности и его объектами:

–«Архивировать/восстанавливать журналы» – привилегия на архивирование и восстановление централизованных журналов;

–«Выполнять оперативные команды» – привилегия на выполнение команд оперативного управления;

–«Квитировать события НСД» – привилегия на выполнение команд квитирования событий НСД;

–«Управлять настройками Secret Net» – привилегия для удаленной настройки локальных параметров Secret Net на рабочих станциях;

–«Читать/просматривать данные» – привилегия для подключения к серверу безопасности и просмотра информации;

–«Редактировать конфигурацию и свойства объектов» – привилегия для внесения изменений при работе с программой в режиме конфигурирования (предоставляется только пользователям группы администраторов домена безопасности).

Добавьте пользователя Admin и разрешите ему выполнять оперативные команды.

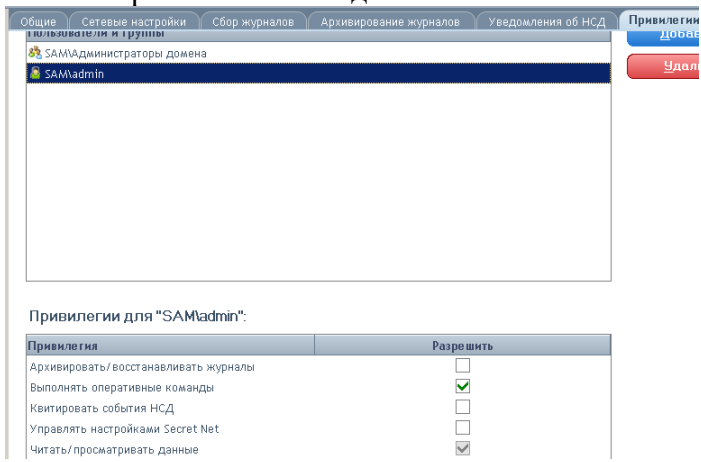
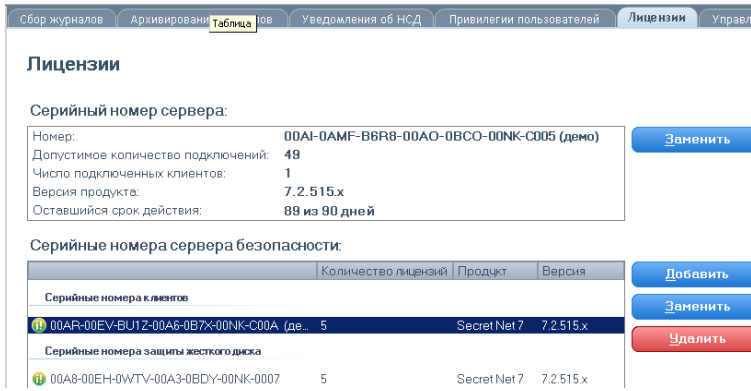


Рисунок 30 – Окно настроек привилегий пользователей программы управления Secret Net

Вкладка «Лицензии» позволяет управлять лицензиями на различные компоненты Secret Net (рис. 31). В данные момент все необходимые лицензии уже использованы, но в случае добавления новых защищаемых компьютеров будут использованы



доступные в системе лицензии. Помимо этого можно добавлять новые лицензии, заменять или удалять имеющиеся.

Рисунок 31 – Окно «Лицензии» Secret Net

Сохраните сделанные настройки, нажав кнопку «Применить иерархию и настройки» (рис. 32).

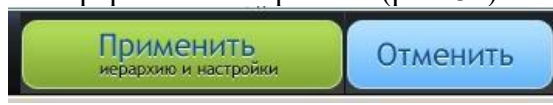


Рисунок 32 –Кнопки применения настроек в режиме конфигурирования

9. Задание на лабораторную работу

Настройте с помощью программы оперативного управления Secret Net клиентскую виртуальную машину в соответствии с вариантом.

Таблица 1

Варианты заданий работы с пользователями

Вариант	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Запретить использование устройств («+» означает запрет данной категории устройств):															
Сменные диски		+				+			+		+		+		
Оптические диски			+		+		+			+		+			+
Беспроводное соединение (Wi-fi)	+			+				+			+		+	+	
Соединение Bluetooth	+	+					+		+	+		+			
Устройства SD			+		+	+		+		+			+		
Принтеры	+			+		+	+							+	+
Параллельные порты		+						+	+			+		+	
Последовательные порты			+	+	+						+				+
Защитные подсистемы:															
Включить затирание данных	+		+		+		+		+		+		+		+
Включить ЗПС		+		+		+		+		+		+		+	

Продолжение таблицы 1

Настройки подсистем:																
Запрет вторичного входа в систему	+	-	+	+	-	-	+	-	+	+	-	-	+	-	+
Количество неудачных попыток аутентификации	5	10	2	5	8	4	6	9	7	6	8	4	6	9	5
Максимальный период неактивности до блокировки экрана	15	20	30	25	5	8	12	19	8	16	21	24	13	18	25
Разрешить интерактивный вход только доменным пользователям	-	+	-	-	+	+	-	+	-	-	+	+	-	+	-
Реакция на изъятие идентификатора	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3

10. Контрольные вопросы

1. Для чего предназначена программа оперативного управления Secret Net?

2. Какие режимы работы имеет программа оперативного управления Secret Net?

3. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования.

4. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.

5. В какой последовательности применяются параметры групповых политик?

6. Для чего необходимо квитирование событий НСД?

7. Какие виды отчетов можно построить с помощью программы ОУ?

8. В каких случаях необходимо изменение сетевых настроек?

9. Какие команды можно выполнять для удаленного управления защищаемыми компьютерами?

Лабораторная работа № 5
«Safenet Authentication Manager (SAM). Настройка и базовые возможности»

1. Цель работы

Целью данной работы является изучение основного функционала системы управления ключевыми носителями eToken – Safenet Authentication Manager (SAM), получение навыков работы с программой SAM, навыков настройки SAM и управления ключевыми носителями.

2. Краткие теоретические сведения

SafeNet Authentication Manager (SAM) - система, предназначенная для внедрения, управления и учета аппаратных и программных средств аутентификации пользователей в масштабах предприятия.

SAM обеспечивает:

–Централизованное управление средствами аутентификации в течение всего жизненного цикла (инициализация/выпуск сертификата, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование).

–Учет средств аутентификации, аудит их использования.

–Автоматизацию типовых операций и сценариев администрирования в соответствии с политиками безопасности, принятыми в организации.

–Быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

SafeNet Authentication Manager использует два хранилища:

–Хранилище пользователей – содержит учетные данные пользователей. Данное хранилище должно

быть установлено и настроено на сервере до установки SafeNet Authentication Manager. Также существует вариант установки автономного хранилища пользователей ADAM (AD LDS). В этом случае предварительная настройка не требуется.

–Хранилище служебной информации – содержит данные, касающиеся использования устройств eToken, и настраивается после установки компонента SAM Server.

3. Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player или VMware Workstation, а также скачать архив с виртуальной машиной «Safenet Authentication Manager (SAM)». Скачанные архивы необходимо разархивировать. Следует убедиться, что в настройках всех виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only»). При наличии на хосте оперативной памяти достаточного объема, можно увеличить выделяемый виртуальной машине объем ОЗУ (по умолчанию установлен 512 МБ).

Для выполнения данной лабораторной работы необходим eToken, не содержащий важных данных (содержимое токена будет удалено в ходе работы).

4. Ход работы

4.1. Настройка SAM

Шаг 1: Добавление ролей для доступа к порталам SAM:

Откройте менеджер настройки SAM: Пуск > Все программы > SafeNet > SafeNet authentication manager > Configuration Manager. С помощью данной

программы можно изменять общие настройки данной программы.

1. Из меню Action менеджера конфигурации Configuration Manager, выберите: Authorization Manager -> Edit Roles…

2. Можно увидеть 3 веб сайта SAM. Каждому из них можно назначать определенный набор ролей. Использование различных ролей позволяет назначать различный набор прав и разрешений на выполнение операций, как обычным пользователям, так и разного рода администраторам. Для сайтов Self Service Center и Rescue Center, по умолчанию имеется только одна роль – user. Для сайта Management Center имеется несколько стандартных ролей – Administrator, Helpdesk, Certificate Recovery, First tier approval, Second tier approval (рис. 1).

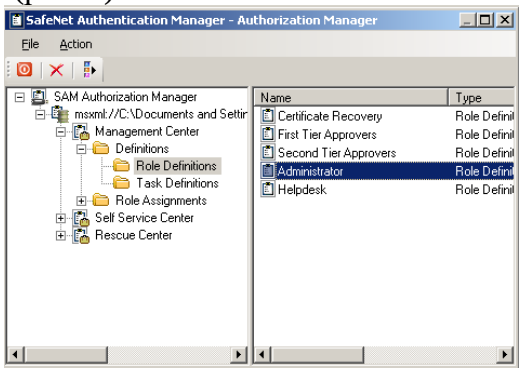


Рисунок 1 – Запрос конфигурации при запуске виртуальной машины

3. В дереве Management Center, перейдите к определению ролей (Definitions -> Roles Definitions). Дважды щелкните по роли администратора (Administrator). Во вкладке «Definitions» можно увидеть задачи и операции, доступные роли администратора.

4. Добавьте операцию «Web_Service_» «API_Access» роли администратора:

–Нажмите кнопку «Add» Откройте вкладку операции – «Operations».

–Выберите операцию: «op_web_service_api_access». Нажмите OK дважды, чтобы применить изменения.

–Закройте «Authorization Manager» (рис. 2).

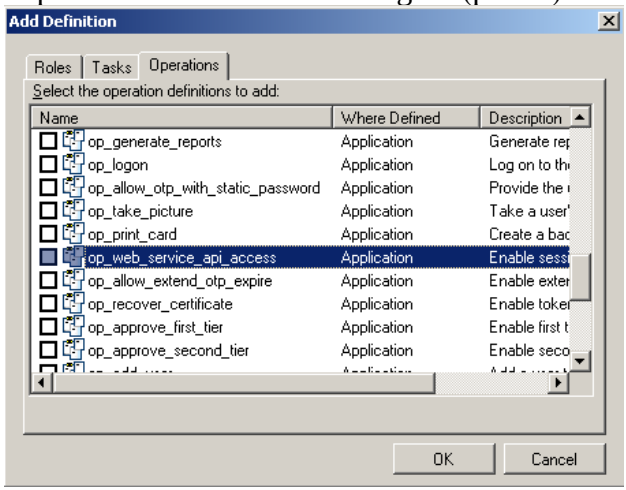


Рисунок 2 – Добавление операций

4.2. Базовая настройка выпуска токенов

Шаг 1: Открываем редактор политик токенов TPO Editor для настройки выпуска токенов SAM:

1. Из меню Пуск, откройте: Все программы > SafeNet > SafeNet Authentication Manager > Policy Management. Откроется утилита Active Directory Пользователи и компьютеры.

2. Откройте Token Policy Object (TPO) для редактирования:

a. Правой кнопкой мыши нажмите на домен в дереве (SAM.COM) и выберите свойства.

b. Откройте закладку Token Policy и нажмите кнопку Open.

c. Выберите «Default policy object» и нажмите Edit (рис. 3).

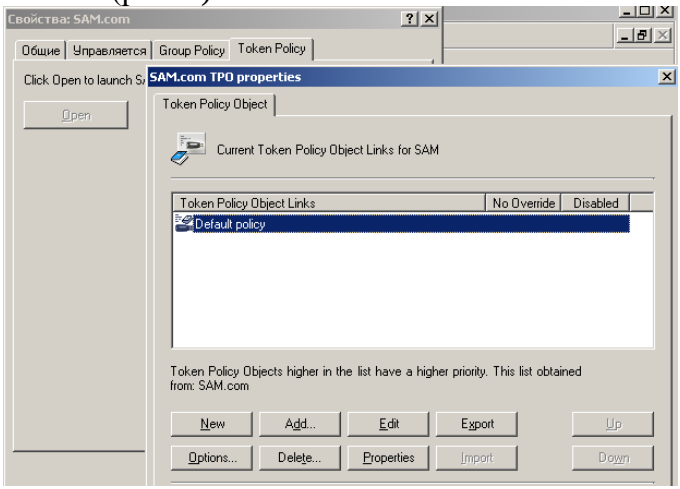


Рисунок 3 – Редактирование политики токенов

Шаг 2: Настройка параметров токенов и паролей:

1. Выберите настройки токена Token Settings. В политике шаблон имени токена при назначении пользователям (Token name template for assigned tokens), задайте значение $Account_name. Нажмите OK чтобы сохранить (рис. 4).

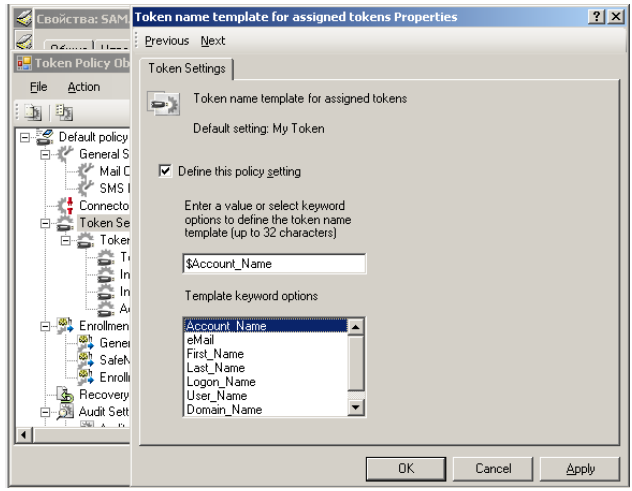


Рисунок 4 – Настройка параметров токенов и паролей

2. Включите настройку Enable token naming in the Self Service Center (пользователь сможет изменить имя токена при самостоятельном выпуске токена)

3. Выберите Token initialization (Инициализация токена). Ограничьте инициализацию токена, разрешив ее делать только через центр управления SAM Management Center:

• Задайте политику SAM Management Center behavior и выберите Delete token content and initialize.

• Задайте политику SAM Self Service Center behavior и выберите Delete token content only.

Для большей безопасности, эти значения заданы по умолчанию. Пользователи могут только удалять содержимое токенов, инициализация запрещена (так как ключ инициализации токена не должен передаваться по сети).

4. Выберите Token Password. Задайте значение по умолчанию 1234567890.

Шаг 3: Настройка параметров инициализации токенов:

1. Выберите Initialization Parameters – посмотрите значения по умолчанию.

2. Задайте максимальное число попыток подключений пользователя (Maximum number of user logon failures) = 4

3. Включите поддержку 2048-битных ключей RSA (2048-bit RSA key support)

4. Включите поддержку OTP токенов (OTP support).

5. Включите поддержку (RSM support)

6. Примените настройки (Apply) (Рис. 5).

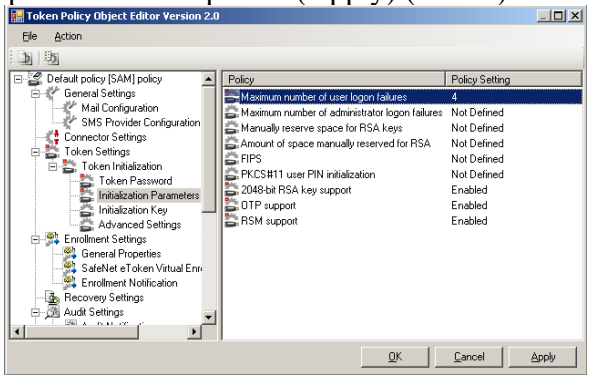


Рисунок 5 – Настройка параметров инициализации токенов

Шаг 4: Задайте следующие параметры выпуска токенов:

1. В Enrollment Settings, выберите General Properties.

2. Установите максимальное число активных токенов на пользователя = 6 (Maximum number of active tokens per user).

3. Не трогайте настройку “Initialize token on each enrollment”.

4. Задайте и включите настройку Инициализировать токен при первом выпуске (Initialize new token on first enrollment) - для задания пароля пользователя и администратора для разблокирования токена.

5. Следующие 4 настройки не трогайте.

6. Включите настройку Игнорировать несовместимость коннекторов во время выпуска токена (Ignore connector incompatibility during enrollment). Эта настройка позволяет завершить выпуск токена, даже если произойдет ошибка при инициализации коннектора.

7. Включите создание eToken Virtual (Enable SafeNet eToken Virtual creation).

8. Включите настройку «Требовать заполнение опросника для аутентификации через портал восстановления» (Require the user to complete the authentication questionnaire).

9. Остальные настройки оставьте неопределенными (ставятся значения по умолчанию).

10. Нажмите Apply (Рис. 6).

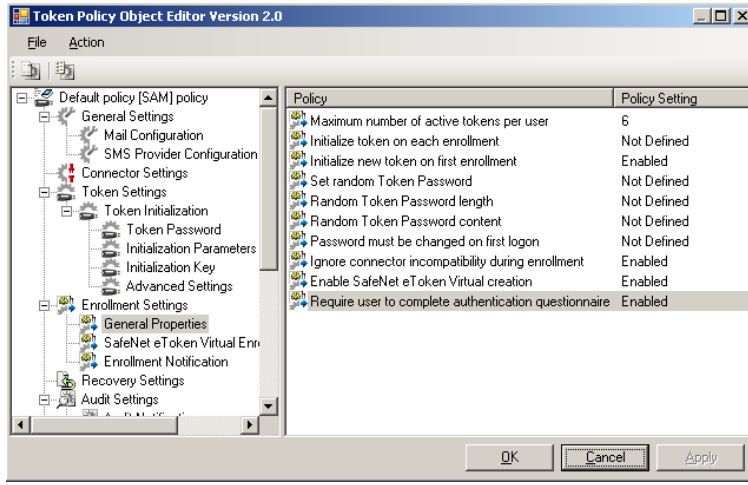


Рисунок 6 – Установление параметров выпуска токенов

4.3. Настройка параметров восстановления eToken

Выберите Recovery Settings (настройки восстановления) и включите следующие настройки:

a. Включите ”Enable token unlock”.

b. Выберите unlock password type (тип пароля разблокировки) = random password (случайный пароль).

c. Установите значение Maximum number of SafeNet eToken Virtual unlocks(Максимальное число разблокировок eToken Virtual) = 25.

d. Установите значение Enable SafeNet eToken Rescue (Включить восстановление eToken) = Enable.

e. Установите значение Maximum SafeNet eToken Rescue usage period (Максимальный срок действия eToken Rescue) = 8 дням.

f.Задайте значение SafeNet eToken Rescue download option = User manually initiates download.

g. Выберите User authentication questionnaire и добавьте 3 вопроса для аутентификации для использование Rescue Service Center (например, год рождения, любимый цвет и т.д.).

h. Пусть отображаются все вопросы - не включайте политику “Number of random questions asked”.

i. Установите максимальное число попыток аутентификации = 3 (maximum number of authentication retries).

j. Остальные политики оставьте без изменений. Просмотрите их значения по умолчанию.

k. Примените настройки (Apply) (Рис. 7).

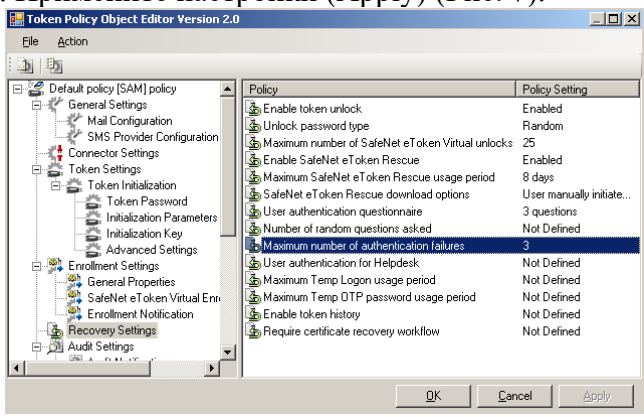


Рисунок 7 – Настройка параметров восстановления eToken

Часть II – Порталы SAM

4.4. Management Center

Перед выполнением следующей части работы инициализируйте eToken для очистки содержимого и сброса пароля к стандартному. Для этого в программе Safenet Authentication client (панель задач) выберите команду «Инструменты», далее откройте подробный вид, где для подключенного eToken задайте команду инициализации, запустив ее с параметрами по умолчанию (рис. 8).

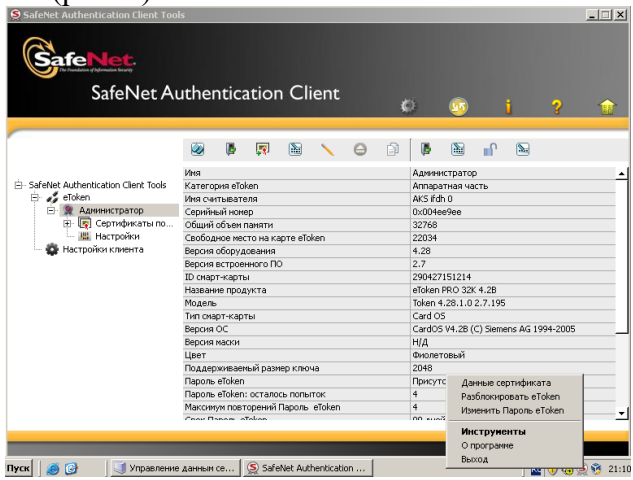


Рисунок 8 – Инициализация eToken

Запустите Internet Explorer. Перейдите по адресу http://127.0.0.1/sammanage. Введите логин и пароль администратора. Откроется центр управления токенами SAM Management Center. С помощью сайта SAM Management Center администраторы SafeNet Authentication Manager могут выпускать и закреплять за пользователями устройства eToken. Для работы с

устройствами eToken необходимо, чтобы на компьютере, с которого происходит обращение на сайт, было установлено ПО eToken PKI Client 5.1 SP1 / SafeNet Authentication Client 8.0 или выше и компонент SAM Client.

В левой панели располагаются ссылки на разделы сайта и формы для поиска. Для поиска администратор должен указать домен и выбрать соответствующие критерии (параметры поиска зависят от выбранного раздела). Всего имеется пять разделов:

– **Helpdesk (Поддержка).** Основные операции, производимые службой технической поддержки: разрешение временного доступа по паролю (без eToken), разблокирование учетной записи пользователя и другие.

– **Deployment (Распределение).** Выпуск и назначение устройств eToken пользователям.

– **Inventory (Учет).** Операции с выпущенными устройствами eToken, такие как повторный выпуск, удаление, инициализация.

– **Reports (Отчеты).** Просмотр доступных отчетов о событиях SAM и подключениях eToken.

– **Downloads (Загрузка).** Ссылки для загрузки файлов установки SAM Client для 32/64-битных платформ и ссылки на приложения, необходимые для работы MobilePASS.

Откройте вкладку Deployment (рис. 9). Данный раздел позволяет закреплять устройства eToken за пользователями и осуществлять выпуск устройств eToken. Страница раздела выглядит следующим образом:

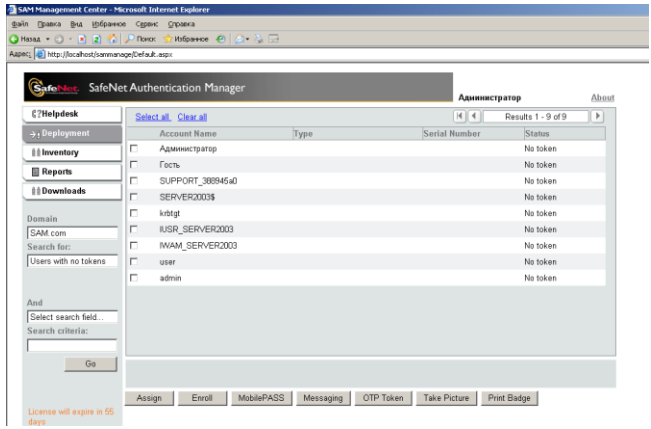


Рисунок 9 – Вкладка Deployment

В нижней части страницы расположены управляющие кнопки, значение которых приведено в таблице:

Таблица 1

Описание доступных кнопок на сайте SAM Management Center в разделе Deployment

Кнопка	Описание
Assign (Назначить)	Позволяет закрепить за пользователем устройство eToken
Enroll (Выпуск)	Позволяет выпустить на имя выбранного пользователя устройство eToken
MobilePASS (Выпуск MobilePASS)	Позволяет выпустить на имя выбранного пользователя MobilePASS
Messaging (Выпуск MobilePASS Messaging)	Позволяет выпустить на имя выбранного пользователя MobilePASS

	Messaging

Продолжение таблицы 1

OTP Token (Выпуск eToken PASS)	Позволяет выпустить на имя выбранного пользователя eToken PASS
Take Picture (Фото)	Позволяет выбрать/сохранить фотографию выбранного пользователя или пользователей для создания пропуска
Print Badge (Печать пропуска)	Позволяет распечатать пропуск пользователя

Отличие функции Assign от Enroll заключается в том, что функция Assign позволяет просто сделать запись о фиксации факта владения eToken в базе данных SAM, без необходимости подключения данного eToken, его инициализации и записи содержимого. Для функции Enroll наличие подключенного eToken является обязательным, так как в зависимости от настроек политик токенов TPO, может быть произведена инициализация токена, а также могут быть использованы коннекторы.

4.5. Назначение eToken пользователю

При назначении eToken устройство автоматически добавляется в хранилище SAM (если оно там отсутствует) и происходит (либо не происходит) инициализация eToken в соответствии с параметрами, установленными в редакторе TPO, после чего eToken закрепляется за выбранным пользователем.

Чтобы назначить eToken пользователю:

1. Воспользуйтесь формой поиска, чтобы выбрать пользователя или пользователей, за которыми нужно закрепить устройства eToken (например, выберите Users with no tokens – пользователи без токенов, в появившемся списке выберите пользователя **Администратор**).

2. Нажмите Assign (Назначить).

3. На отобразившейся странице предлагается выбрать один из двух вариантов:

–Assign a connected token (Назначить подключенный eToken).

–Assign a token by its serial number (Назначить eToken по серийному номеру) – в этом случае введите в отобразившемся поле серийный номер устройства eToken, которое нужно закрепить за пользователем.

Выберите Assign a connected token (перед этим необходимо подключить eToken к виртуальной машине)

4. Нажмите Run (Запуск).

5. Отобразится сообщение Tokens successfully assigned (eToken успешно назначен), либо возможно появление предупреждений или ошибок, в случае проблем с инициализацией.

4.6. Раздел Helpdesk (Поддержка)

Раздел Helpdesk (Поддержка) предоставляет администратору доступ к основным операциям по работе с устройствами eToken. Страница раздела выглядит следующим образом (рис. 10).

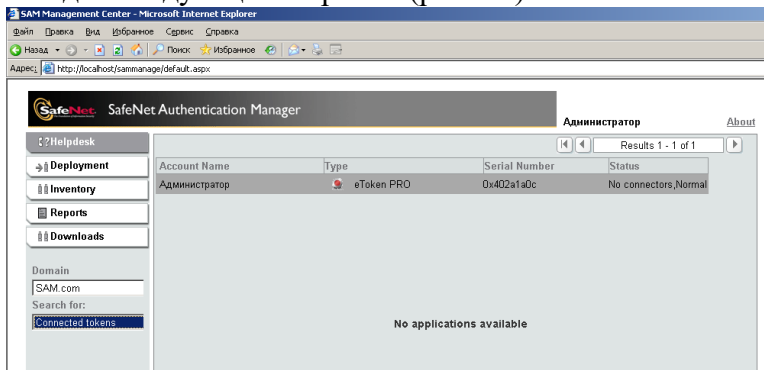


Рисунок 10 – Страница раздела Helpdesk

Выберите в окне поиска Connected tokens и нажмите кнопку Go для того, чтобы отобразить назначенный пользователю Администратор токен.

Внизу страницы располагаются управляющие кнопки. Доступны следующие действия:

– **Reset Pwd (Сбросить пароль).** Позволяет сбросить текущее значение пароля eToken и заменить его стандартным паролем

– **Revoke (Отозвать).** Позволяет аннулировать сертификаты в памяти eToken и сделать его недоступным для использования

– **Unassign (Открепить).** Позволяет открепить eToken от конкретного пользователя, за которым он закреплен

– **Unlock (Разблокировать).** Позволяет разблокировать eToken, если он был заблокирован в результате превышения допустимого числа неудачных попыток аутентификации

–**More Actions > Replace (Дополнительно > Заменить).** Позволяет отозвать существующий eToken и заменить его новым.

Открепите токен от пользователя Администратор (кнопка Unassign).

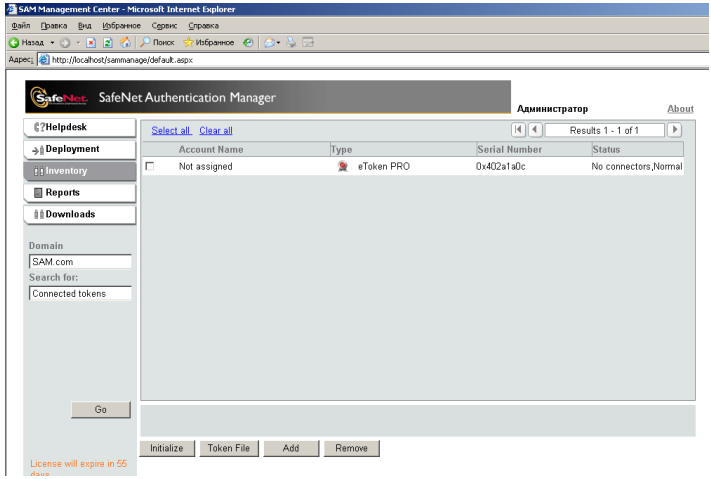
4.7. Раздел Inventory (Учет)

Данный раздел предоставляет администратору доступ ко всем используемым в системе устройствам eToken. Данный раздел предоставляет администратору доступ к следующим возможностям.

–Инициализация eToken

–Загрузка инвентарного файла в базу данных SAM

–Добавление и удаление eToken из базы данных SafeNet



Authentication Manager Выберите в строке поиска Conn ected tokens. Страница раздела выглядит следующим образом (Рис. 11):

Рисунок 11 – Страница раздела Inventory

Под результатами поиска располагаются кнопки, которые позволяет осуществлять следующие действия (рис. 12):

Кнопка	Описание
Initialize (Инициализировать)	Позволяет инициализировать подключенный eToken.
Token File (Файл eToken)	Позволяет загрузить инвентарный файл со списком eToken организации.
Add (Добавить)	Позволяет добавить подключенный eToken в базу данных SAM.
Remove (Удалить)	Позволяет удалить выбранный eToken из базы данных SAM.

Рисунок 12 – Описание действий

Инициализируйте подключенный eToken.

4.8. Раздел Reports (Отчеты)

Данный раздел позволяет просматривать различные отчеты, связанные с использованием eToken. Доступны следующие типы отчетов:

–**Token Inventory (Учет).** Список устройств eToken, находящихся в инвентаре SafeNet Authentication Manager

–**Token History (История).** Данные об устройствах eToken которые не назначены или удалены.

–**Token Expiration (Срок истечения действия).** Список eToken, которым назначена дата истечения срока действия.

–**Token Audit (Аудит).** Сведения аудита операций SafeNet Authentication Manager.

–**OTP Usage (Использование OTP).** События, связанные с аутентификацией по OTP, определенные в конфигурации веб-службы OTP.

–**Token Connections (Подключенные eToken).** Аппаратные eToken, подключенные с момента

последнего обновления (необходима настройка MS SQL).

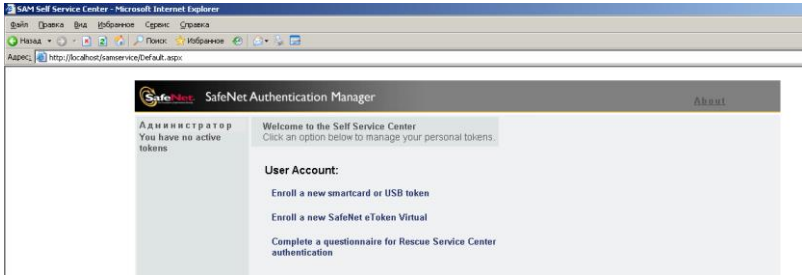
–**Hourly Distribution (Почасовое распределение).** Среднее число подключений аппаратных eToken в час (необходима настройка MS SQL).

Просмотрите доступные отчеты.

4.9. SAM Self Service Center (Центр самообслуживания SAM)

Сайт SAM Self Service Center доступен по адресу http://<имя сервера или домена>/SAMservice. (http://127.0.0.1/samservice).

При заходе на сайт главная страница выглядит



следующим образом (рис. 13).

Рисунок 13 – Сайт SAM Self Service Center

В левой панели отображается имя пользователя и принадлежащие ему устройства eToken. Ниже расположена ссылка Downloads (Загрузки), которая ведет на страницу загрузки ПО, необходимого для работы с eToken.

В центральной части страницы располагаются два списка.

–**Selected Token (Выбранный eToken)** – содержит ссылки на операции, которые доступны с

выбранным устройством eToken. В данный момент этого списка нет, так как за пользователем не закреплены токены.

–**User Account (Учетная запись пользователя)** - содержит ссылки, позволяющие выпустить новый eToken, а также заполнить аутентификационную анкету.

Для восстановления содержимого токена и разблокировки токена пользователю необходимо заполнить аутентификационную анкету (рис. 14). Заполните опросник **(Complete the Questionnaire for Rescue Service Center authentication).** Ответы необходимо запомнить. Вернитесь в главное меню.

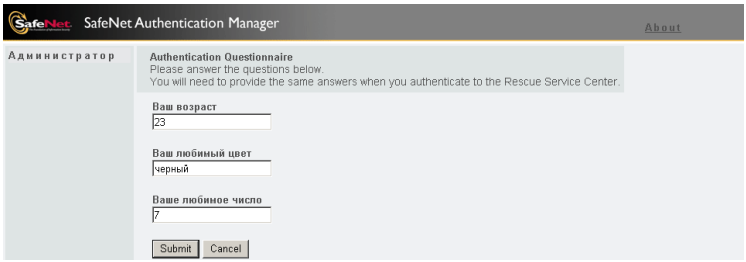


Рисунок 14 – Аутентификационная анкета

Щелкните по ссылке Enroll a new smartcard or USB token (Выпустить аппаратный eToken). Нажмите Start (Начать). Отобразится предупреждение о том, что eToken будет инициализирован. Чтобы продолжить, нажмите Yes. Continue with the enrollment (Да, продолжить выпуск). Отобразится следующая форма (Рис. 15).

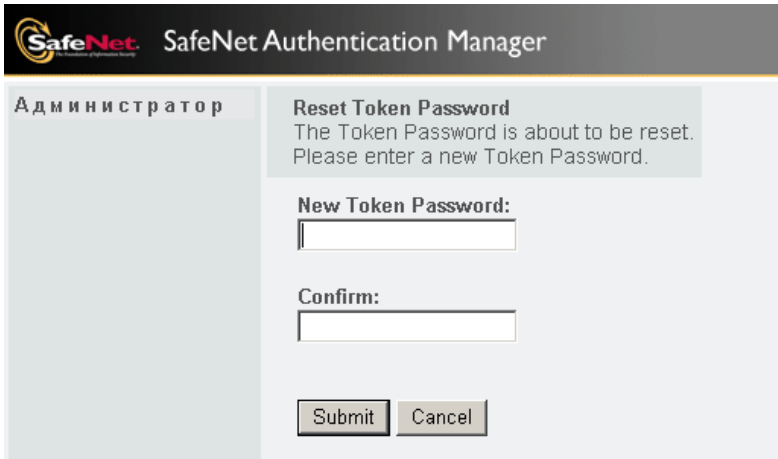


Рисунок 15 – Форма выпуска

Введите ПИН токена, а затем имя токена. Токен будет успешно инициализирован. Теперь в главном меню сайта появилось больше возможностей (рис. 16).

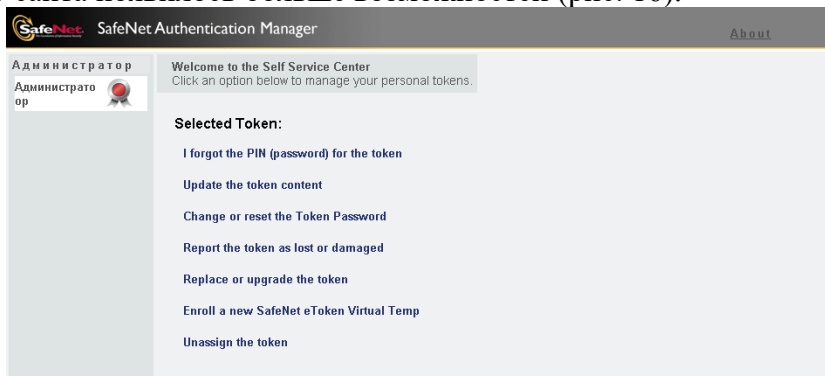


Рисунок 16 – Главное меню сайта

–I forgot the PIN (password) for the token – смена пароля, в случае, если пользователь его забыл

–Update the token content – обновление содержимого токена

–Change or reset the Token Password – смена или сброс ПИН токена

–Report the token as lost or damaged – сообщить о потере или повреждении токена

–Replace or upgrade the token – заменить или обновить токен

–Enroll a new SafeNet eToken Virtual Temp – выпустить новый eToken Virtual Temp

–Unassign the token – открепить токен

4.10. SAM Rescue Center (Центр удаленного доступа SAM)

Сайт SAM Rescue Center доступен по адресу http://<имя сервера или домена>/SAMrescue (http://sam.com/samrescue) и предназначен для пользователей eToken, которые находятся за пределами офис и не имеют доступа к сети организации. В случае возникновения проблем при использовании eToken, пользователи могут решить задачу самостоятельно с помощью данного сайта.

На данном сайте доступны операции, перечисленные в таблице 2: Наличие той или иной операции зависит от моделей eToken, зарегистрированных на пользователя.

Таблица 1

Описание доступных действий и соответствующих им моделей eToken на сайте SAM Rescue Center

Ссылка на раздел	Модели eToken

Отключение/включение возможности использования eToken	Все модели eToken
Разблокировка пароля пользователя eToken	Аппаратные eToken, а также eToken Virtual, eToken Virtual Temp и eToken Rescue
Изменение PIN–кода для OTP	Все модели eToken с поддержкой OTP
Синхронизация значений OTP	Все модели eToken с поддержкой OTP
Запрос временного OTP	Все модели eToken с поддержкой OTP
Активация eToken Rescue	Все модели eToken
Запрос нового пароля для eToken Rescue	eToken Rescue
Замена файла eToken Rescue	eToken Rescue
Отзыв eToken Rescue	eToken Rescue

4.11. Разблокировка токена с помощью кодов Запроса/Ответа в SAM

Пароль заблокированного токена можно сбросить, если токен был инициализирован с паролем администратора. Эта настройка доступна в разделе recovery settings TPO - “Enable token Unlock”.

SAM использует механизм запросов-ответов для аутентификации в заблокированном токене с целью сброса пользовательского пароля.

1. Откройте SAC Tools (рис. 17).

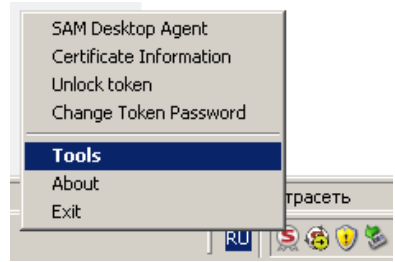


Рисунок 17 – SAC Tools

2. Заблокируйте токен, попытавшись несколько раз неправильно ввести пароль, использовав функцию Rename Token (Переименовать токен) (рис. 18).

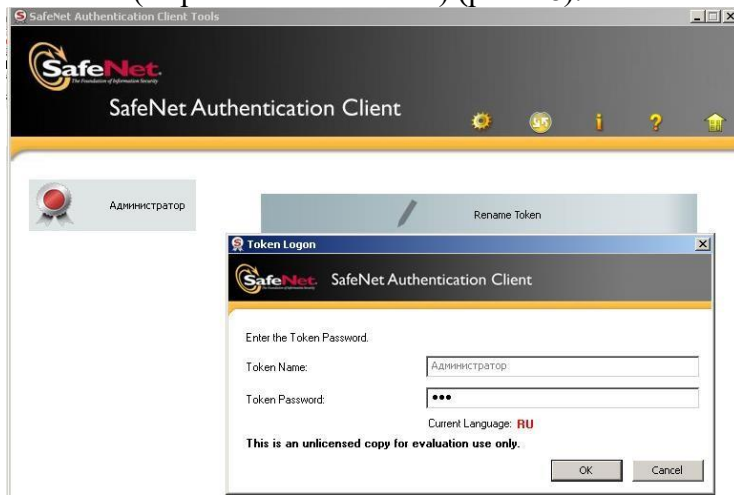


Рисунок 18 – Функция Rename Token

3. В SAC Tools выберите Unlock Token (Разблокировать eToken). Будет выдан код запроса для разблокирования токена (рис. 19).

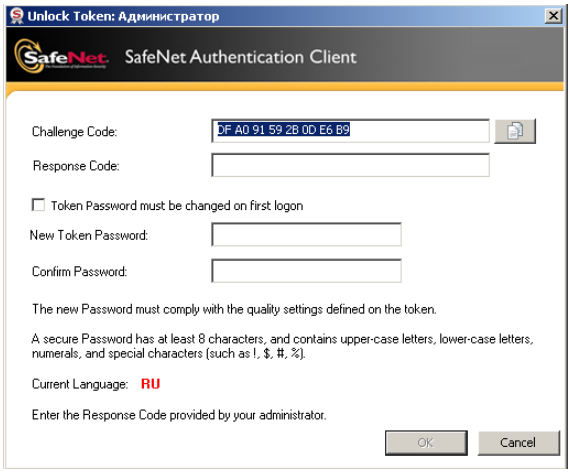


Рисунок 19 – Разблокирование токена в SAC Tools

4. Откройте сайт SAMRescue <http://sam.com/SAMRescue>. **Внимание!** Возможно понадобится добавить http://sam.com в список надежных узлов Internet Explorer (Сервис -> Свойства обозревателя -> Безопасность -> Надежные узлы -> Узлы…) Введите имя пользователя и заполните капчу (Рис. 20).

Рисунок 20 – Ввод имени пользователя

5. Пройдите аутентификацию, ответив на вопросы.

6. Выберите настройку “Unlock the token”

7. Введите код запроса eToken Challenge Code, который был выдан в SAC Tools (рис. 21).

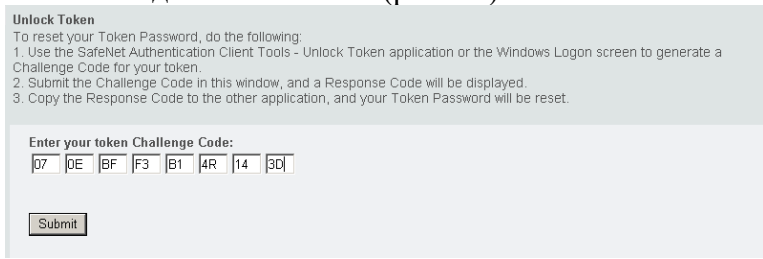


Рисунок 21 – Ввод кода запроса

8. Нажмите Submit – Будет предоставлен код отзыва (Рис. 22).

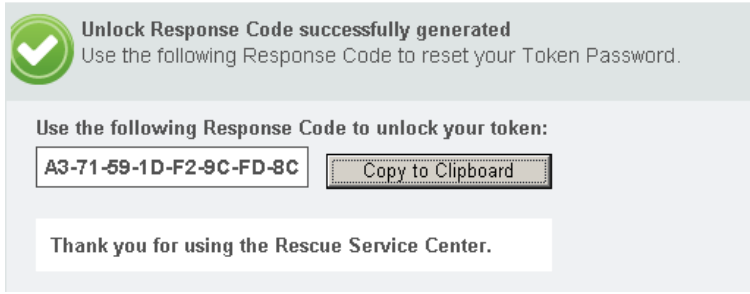


Рисунок 22 – Код отзыва

9. Скопируйте данный код в SAC Tools и задайте новый пароль (должен соответствовать требованиям сложности).

10. Нажмите OK. Токен успешно разблокирован.

4.12. Создание коннектора для записи сертификата вход со смарт-картой и проверка содержимого токена

Как создать сертификат:

1. Открыть оснастку certtmpl.msc

2. Создать копию шаблона вход со смарт-картой.

3. Установить срок действия 2 дня, период обновления – 1 день, галочку опубликовать сертификат в AD. Имя шаблона должно быть без кавычек.

4. Во вкладке безопасность добавить право “Заявка” для группы пользователей “Прошедшие проверку”.

5.Открыть центр сертификации из панели администрирование.

6. Открыть папку Шаблоны сертификатов и создать выдаваемый шаблон сертификата, выбрав созданный вами ранее шаблон из списка (Действие – Создать – Выдаваемый шаблон сертификата). Также добавьте шаблон Агент подачи заявок и Вход со смарт картой.

7. Открыть certmgr.msc и выдать личный сертификат Агента подачи заявок администратору.

8. Настройте коннектор MS CA:

–Откройте TPO (Policy Management – Sam.com – Свойства – Token Policy – Open - Edit), выберите Connector Settings, Connector for Microsoft CA.

–Включите политику и нажмите на кнопку Definitions.

–Добавьте новый запрос: введите имя запроса, тип сервера – standalone, версию windows – server 2003, цель использования – Smartcard Logon и шаблоны созданного вами сертификата.

–Нажмите Apply и закройте открытые окна.

9. Обновите содержимое токена на сайте SamService (Update the token content).

10. Проверьте наличие сертификата на токене. Для этого в контекстном меню программы Safenet Authentication Client (в панели задач) выберите команду «Данные сертификата».

11. Протестируйте возможность входа в систему с использованием eToken (возможно необходимо переподключить токен в настройках виртуальной машины).

5. Задание на лабораторную работу

Проделайте ход работы. Необходимо на занятии показать преподавателю вход в операционную систему с использованием eToken.

6. Контрольные вопросы

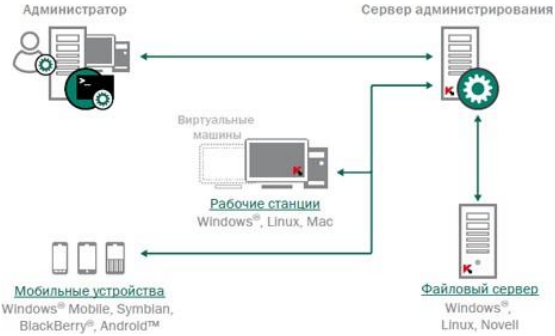
1. Для чего предназначена программа SAM?
2. Для чего предназначен сайт SAM Management Center?
3. Для чего предназначен сайт SAM Self Service Center?
4. Для чего предназначен сайт SAM Rescue Center?
5. Где находятся основные настройки SAM, связанные с токенами?
6. В чем отличие операций Assign и Enroll?
7. Для чего предназначена аутентификационная анкета?

Лабораторная работа №6
«Kaspersky Security Center»
1. Цель работы

Целью лабораторной работы является ознакомление с программным продуктом Kaspersky Security Center и изучение его основных функциональных возможностей.

2. Теоретические сведения

Основное назначение Kaspersky Security Center – предоставление администратору инструментов для настройки всех компонентов системы защиты и доступа к детальной информации об уровне безопасности корпоративной сети. Kaspersky Security Center является единым средством для централизованного управления большим набором средств защиты в организации, предоставляемым



«Лабораторией Касперского». Набор программных продуктов, которыми можно управлять при помощи Kaspersky Security Center, включает в себя решения для защиты рабочих станций, серверов и мобильных устройств (рисунок 1):

Рисунок 1 – Логика использования Kaspersky Security Center при защите сети организации.

Kaspersky Security Center является не отдельной программой, а комплексом программных средств, который включает в себя (рисунок 2):

−сервер администрирования – служба, отвечающая за управление безопасностью. Является основным модулем Kaspersky Security Center и хранит всю информацию об управляемых компьютерах в базе данных (MS SQL Server или MySQL). Помимо основного сервера администрирования можно организовать иерархическую структуру серверов администрирования для работы через них с удаленными частями локальной сети или локальной сетью обслуживаемой организации. Это особенно актуально для компаний, структура которых является распределенной. В этом случае локальные пользователи обращаются только к своему серверу.

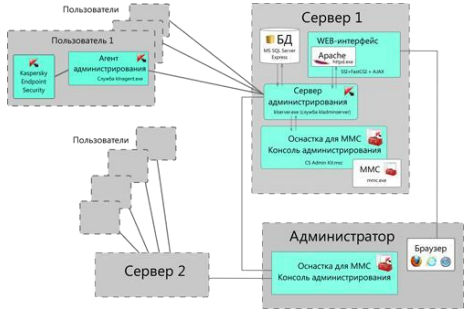
−консоль администрирования – модуль, реализованный в виде оснастки для Microsoft Management Console и предназначенный для управления сервером администрирования;

−веб-консоль – веб-приложение, имеющее аналогичное консоли администрирования предназначение. Различие заключается в том, что веб-консоль позволяет получать доступ к серверу администрирования через браузер, используя веб-интерфейс. Однако, по сравнению с той же консолью администрирования, имеет ограниченные возможности по управлению;

−агент администрирования Kaspersky Security Center – программа, предназначенная для взаимодействия между сервером администрирования и клиентскими компьютерами. Она устанавливается на клиентские системы и позволяет получать

информацию о текущем состоянии программ и о событиях, произошедших на клиентских компьютерах, отправлять и получать команды управления, а также обеспечивает функционирование агента обновлений.

–модули управления программами – модули, которые устанавливаются на рабочее место администратора. Предназначение – получение доступа



к программным продуктам «Лаборатории Касперского» в организации через консоль администрирования.

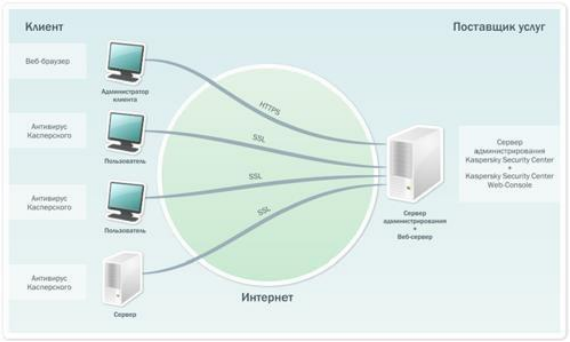
Рисунок 2 – Структурная схема взаимодействия компонентов Kaspersky Security Center.

Из схемы видно, что администратор имеет возможность работать посредством оснастки с несколькими серверами администрирования, являющимися, к примеру, серверами компании, расположенными в разных офисах. Кроме того, администратор имеет возможность получить доступ к серверу администрирования через интернет- браузер с любого компьютера без необходимости устанавливать на него какие-либо модули, что может быть полезно при необходимости мониторинга системы безопасности. Данный способ доступа также применяется при разворачивании защиты в

организации внешним поставщиком услуг, доступ к серверу администрирования которого из защищаемой сети как раз и можно получить при помощи веб-консоли (рисунок 3).

Рисунок 3 – Схема использования веб-консоли.

Kaspersky Security Center позволяет настраивать



и управлять компонентами и настройками на клиентских компьютерах. Для каждой группы пользователей или конкретного пользователя администратор может задавать различные настройки следующих компонентов (рисунок 4):

1. Компоненты защиты: файловый антивирус, почтовый антивирус, веб-антивирус, IM-антивирус, сетевой экран, защита от сетевых атак, мониторинг сети, мониторинг системы.

2. Компоненты контроля: контроль запуска программ, контроль активности программ, поиск уязвимостей, контроль устройств, веб-контроль.

Рисунок 4 – Схема компонентов, управляемых Kaspersky Security Center.

Kaspersky Security Center является развитием инструмента Kaspersky Administration Kit. По сравнению с ним в Kaspersky Security Center был добавлен набор новых функций. Появилась возможность создавать виртуальные серверы администрирования, добавлено управление работой компонентов «Контроль программ», «Контроль уязвимостей», «Веб-контроль» и «Контроль устройств» появилась веб-консоль для управления сервером администрирования через браузер, добавлены функции управления клиентами на виртуальных машинах, появилась возможность централизованно обнаруживать и устранять уязвимости на клиентских компьютерах. Существенно расширены функции инструментов для управления инсталляциями различных компонентов, получения дополнительной информации о контролируемых компьютерах, создания отчетов и работы с учетными записями.

4. Ход работы

Во время выполнения хода работы следует использовать имена задач, политик и других объектов

системы с именами, содержащих в себе **имя учетной записи в кафедральной сети** (либо ФИО).

Запустите серверную и клиентскую виртуальные машины. Войдите в домен под учетной записью Администратор. Запустите консоль Kaspersky Security Center.

Внешний вид консоли Kaspersky Security Center 10 представлен на рисунке 5. Инструменты для системного администрирования интегрированы в различные разделы консоли.

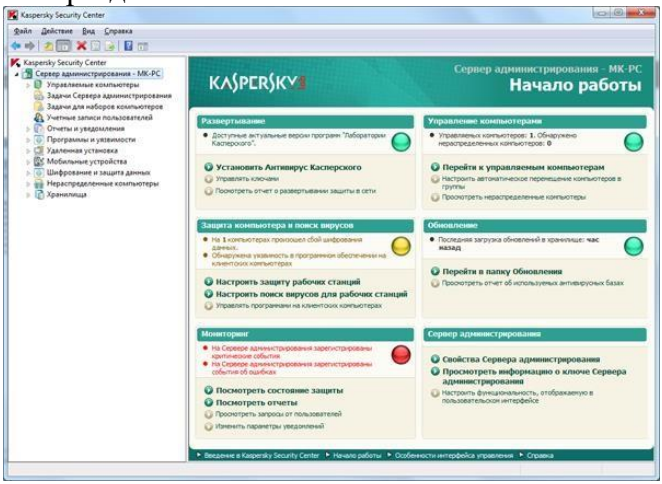


Рисунок 5 - Главное окно при работе с Kaspersky Security Center 10.

4.1. Средства системного администрирования

Добавьте клиентский компьютер в список управляемых компьютеров:

1. Выберите раздел “Управляемые компьютеры”;
2. Выберите вкладку Компьютеры и нажмите «Добавить компьютеры»;

3. Нажмите кнопку “Выбрать компьютеры, обнаруженные в сети сервером администрирования”;

4. Выберите клиентский компьютер из группы Нераспределенные компьютеры.

Одной из задач, решаемых администратором, является установка программного обеспечения на компьютеры в сети. Функции администрирования позволяют создавать инсталляционные пакеты операционных систем и приложений для их централизованной установки на устройства в сети. Работа с этими функциями производится в разделе «Удаленная установка» (рисунок 6).

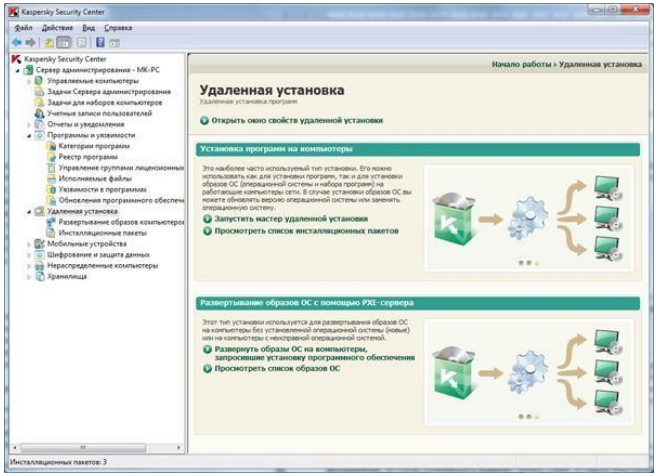


Рисунок 6 - Раздел «Удаленная установка».

Например, чтобы установить программу Kaspersky Endpoint Security на клиентскую машину необходимо:

1. Воспользоваться функцией «Удаленная установка» (Удаленная установка – Запустить мастер удаленной установки).
2. Выберите в списке Kaspersky Endpoint Security.
3. Выберете “Выбрать компьютеры для установки”.
4. Выберите в списке клиентский компьютер.
5. Поставьте галочку “Назначить установку агента администрирования в групповых политиках Active Directory” и нажмите «Далее».
6. Оставьте ключ без изменений.
7. Выберите “Перезагрузить компьютер”.
8. Нажмите «Далее» дважды.
9. Выберите учетную запись **Администратор** и введите пароль.
10. Запустите установку.

Далее начнется архивация установочного файла для отправки на клиентский компьютер. За ходом установки можно следить во вкладке “Задачи для наборов компьютеров”.

Для установки прикладных программ нужно создать инсталляционные пакеты. При создании нужно выбрать тип сборки – образ операционной системы, программы «Лаборатории Касперского» или произвольное приложение (Удаленная установка - Инсталляционные пакеты - Создать инсталляционный пакет) (рисунок 7).

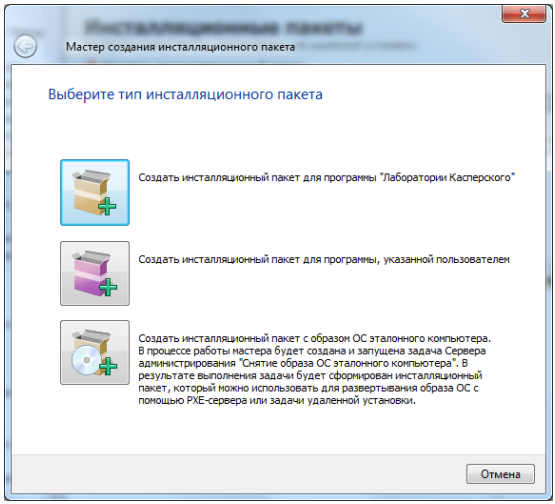


Рисунок 7 – Выбор типа инсталляционного пакета.

Помимо того, что при создании инсталляционного пакета мы можем выбрать любое приложение на компьютере, Kaspersky Security Center 10 предоставляет возможность создать инсталлятор из бесплатных приложений из своей базы данных (7Zip, Adobe Reader, WinZip и т.д., при этом необходимо подключение к Internet) (рисунок 8).

Создайте инсталляционный пакет для программы 7-zip:

1. Выберите создать инсталляционный пакет для программы, указанной пользователем (рис. 7).
2. Введите имя пакета.
3. Выберите файл 7-zip (на рабочем столе).
4. Закончите создание пакета.

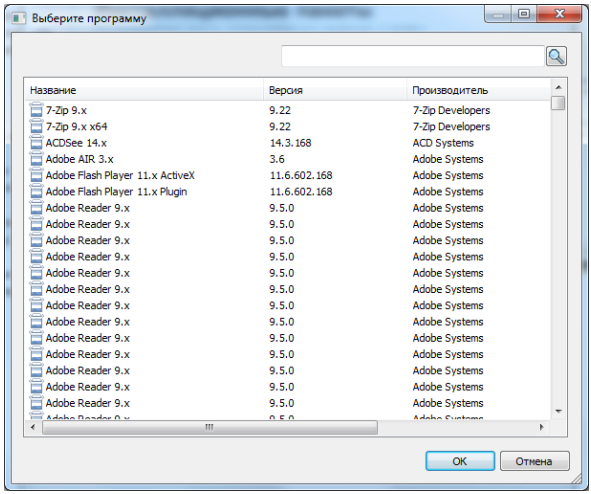
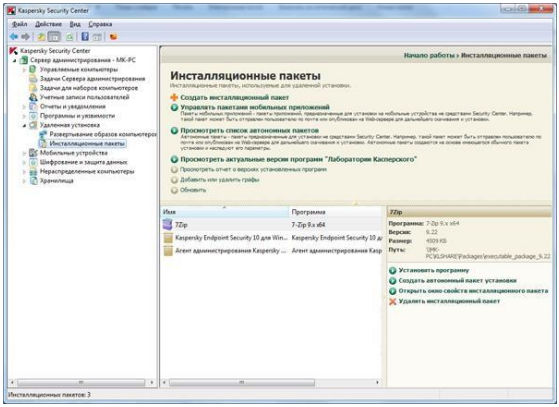


Рисунок 8 – Выбор программы из базы данных «Лаборатории Касперского».

После того, как инсталляционный пакет создан, он попадает в хранилище «Инсталляционные пакеты» (Удаленная установка – Инсталляционные пакеты), из которого он может быть установлен на любое количество компьютеров в сети (рисунок 9).



Установите пакет с архиватором 7-zip на клиентский компьютер.

Рисунок 9 – Хранилище «Инсталляционные пакеты»

KSC позволяет создавать и устанавливать на компьютеры образы ОС (Не выполняется в рамках данной работы, информация для ознакомления).

Для создания образа операционной системы необ ходим так называемый «эталонный» компьютер, с которого и будет «сниматься» образ для его дальнейшей установки на другие компьютеры. Чтобы начать работать с образами операционных систем, вначале нужно установить пакет Windows Automated Installation Kit (WAIK), предназначенный для их установки, настройки и разворачивания.

После этого необходимо создать и запустить задачу для сервера администрирования «Создание инсталляционного пакета на основе образа ОС эталонного компьютера» (Задачи сервера администрирования – Создание образа ОС) (рисунок 10).

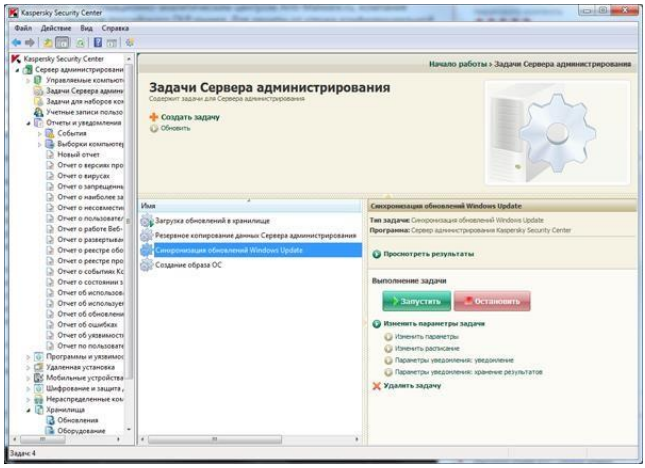


Рисунок 10 - Задача для создания образа операционной системы.

При ее создании нужно указать компьютер для снятия образа; программы Microsoft для включения в образ; категории программного обеспечения, которые нужно обновлять и т.д. (рисунок 11).

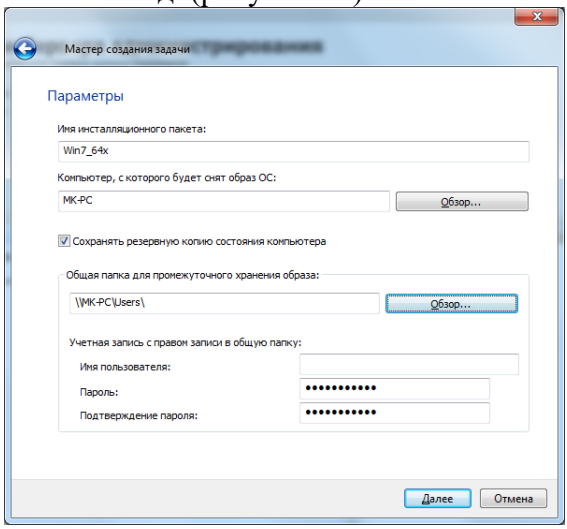


Рисунок 11 - Выбор эталонного компьютера для создания образа операционной системы.

После того как образ был создан, он помещается в хранилище с инсталляционными пакетами, из которого его всегда можно развернуть на выбранных компьютерах. В уже существующие образы администратор может добавлять необходимые для конкретных компьютеров драйвера. Установка образов на компьютеры осуществляется при помощи технологии Preboot eXecution Environment (PXE).

Установка приложений и операционных систем, также как и большинство других действий, производится путем создания необходимого набора задач, запускаемых вручную или по расписанию. Удобной возможностью является удаленное включение компьютеров (WAKE-ON-LINE), позволяющей проводить установку приложений и их обслуживание в нерабочее время, даже если компьютеры уже были выключены сотрудниками.

Примечание: WAKE-ON-LINE - технология, позволяющая удалённо включить компьютер посредством отправки через локальную сеть специальной последовательности байтов (пакета данных).

4.2. Инвентаризация

Одной из важных для администратора задач является учет и контроль различных ресурсов. Инструменты для системного администрирования позволяют работать с тремя видами ресурсов -

аппаратными устройствами, программным обеспечением и его лицензиями.

Kaspersky Security Center 10 автоматически обнаруживает и ведет учет всех компьютеров и внешних устройств в сети. Это позволяет администратору оперативно реагировать на появления новых устройств (Хранилища – Оборудование) (рисунок 12).

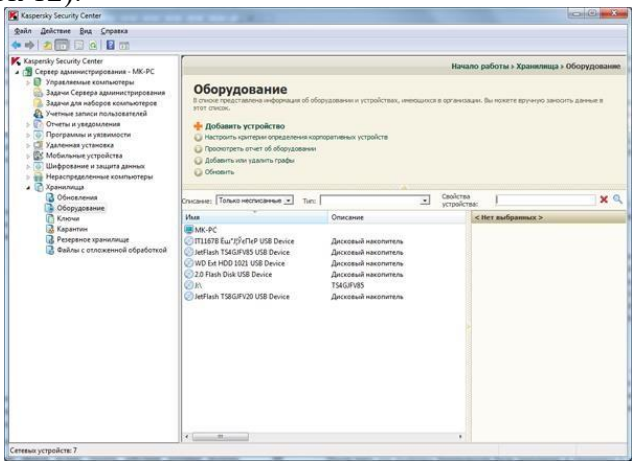


Рисунок 12 – Хранилище оборудования.

Для конкретного компьютера мы можем получить информацию обо всех аппаратных компонентах и подключенных устройствах (Управляемые компьютеры – XP-MSDN – Свойства – Информация о системе – Реестр оборудования). Это может быть полезно при выборе компьютеров, на которые можно устанавливать ресурсоемкие операционные системы или приложения (рисунок 13).

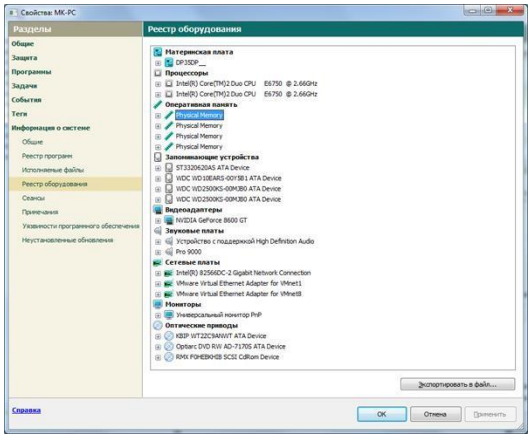


Рисунок 13 – Реестр оборудования

Для каждого конкретного устройства в его свойствах также можно посмотреть все установленные на нем приложения (Информация о системе – Реестр программ) (рисунок 14). Просмотрите оставшиеся разделы в окне свойств компьютера.

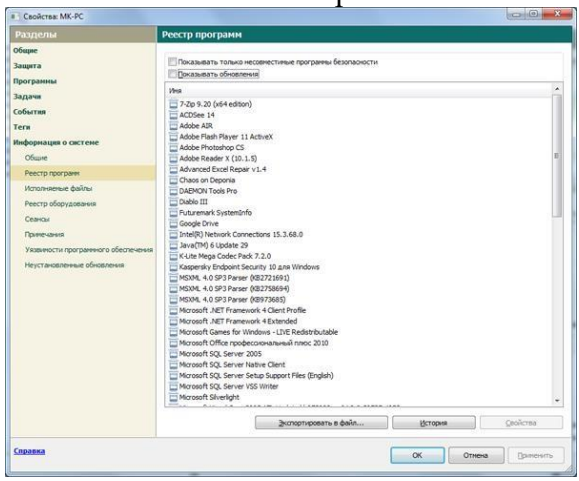


Рисунок 14 – Реестр программ для конкретного устройства

Реестр программ позволяет контролировать установленное на компьютерах программное обеспечение (Программы и уязвимости – Реестр программ). Данные этого реестра можно использовать для контроля нелицензионных приложений, а также для планирования установки новых лицензионных приложений на компьютеры сотрудников (рисунок 15).

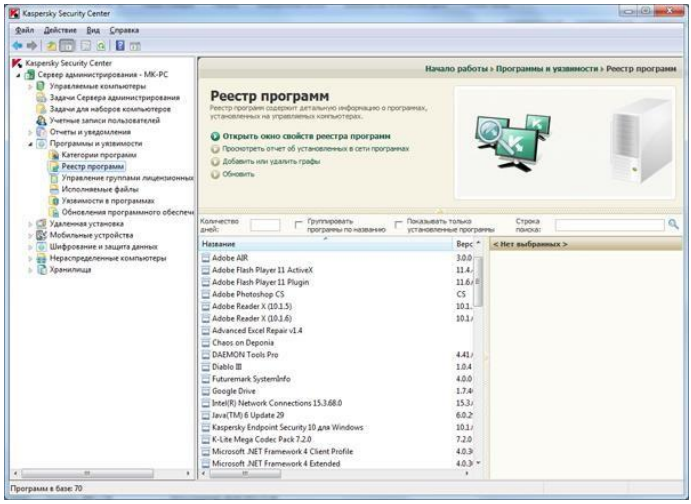


Рисунок 15 – Реестр программ для всех устройств.

4.3. Исправление уязвимостей и установка обновлений

Еще одной важной возможностью Kaspersky Security Center 10 является поиск и исправление уязвимостей, а также установка обновлений различных приложений (требуется подключение к Internet). Поиск уязвимости осуществляется при помощи задачи «Поиск уязвимостей и обновлений программ», а закрытие найденных уязвимостей – задачей

«Установка обновлений программ и закрытие уязвимостей» (Управляемые компьютеры – Задачи).

Механизм обнаружения и закрытия уязвимостей достаточно прост. Для внесенных в реестр программ проводится сравнение их текущих версий и установленных обновлений с обновлениями, предлагаемыми их разработчиками. Если для какого-либо приложения не установлены последнее обновление, то фиксируется его потенциальная уязвимость и предлагается установить последнее обновление. Закрывать уязвимости можно вручную, анализируя предлагаемые обновления, или можно настроить автоматическое закрытие уязвимостей и разгрузить администратора (рисунок 16).

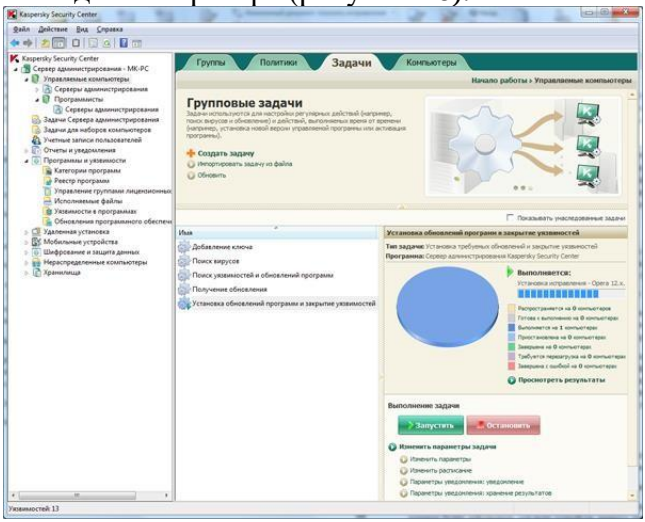


Рисунок 16 – Задача для поиска и закрытия уязвимостей.

После выполнения соответствующей задачи администратор получает список найденных уязвимостей с указанием их критичности и ссылками на их описание (Программы и уязвимости –

Уязвимости в программах) (рисунок 17). Чтобы получить более подробную информацию, можно сформировать отчет о выполненной задаче поиска уязвимости (Отчеты и уведомления – Отчет об уязвимостях) (рисунок 18).

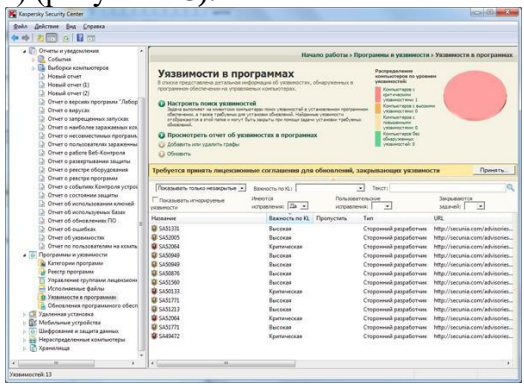


Рисунок 17 – Список найденных уязвимостей

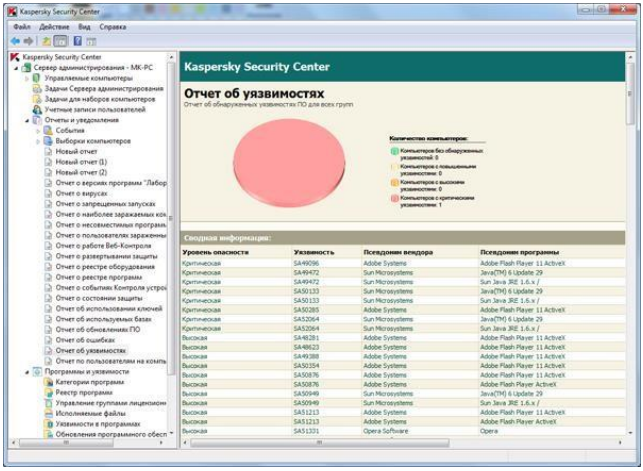


Рисунок 18 – Отчет о поиске уязвимостей.

Аналогично происходит работа с обновлениями программного обеспечения. Создаются и запускаются задачи «Получения обновлений» и «Синхронизация

обновлений Windows Update» (Управляемые компьютеры – Задачи). По результатам их работы формируется реестр необходимых обновлений ПО, которые могут быть загружены немедленно или быть отложены до более удобного случая (Программы и уязвимости – Обновления программного обеспечения) (рисунок 19).

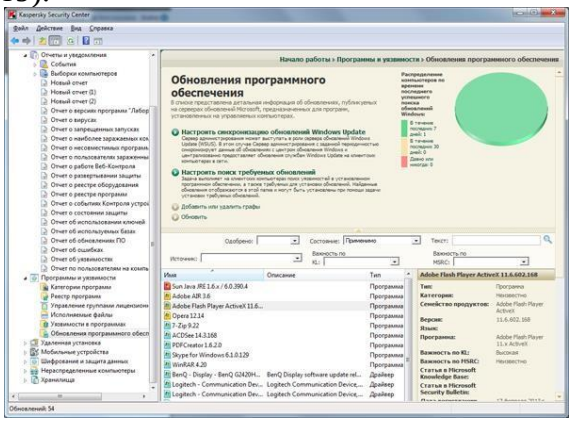


Рисунок 19 – Реестр обновлений программного обеспечения.

Еще одной простой, но в то же время полезной функцией является удаленный доступ к компьютерам в сети. Если у пользователей возникли проблемы или неполадки, администратор может получить управление их компьютерами и решить возникшие проблемы, не покидая своего рабочего места (Управляемые компьютеры – XP-MSDN – Подключиться к компьютеру – RDP).

4.4. Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии системы защиты. Отчеты формируются на основании информации, хранящейся

на Сервере администрирования. Можно создавать отчеты для следующих объектов:

−для выборки клиентских компьютеров;

−для компьютеров, входящих в определенную группу администрирования;

−для набора клиентских компьютеров из различных групп администрирования;

−для всех компьютеров в сети (доступно для отчета о развертывании).

В программе имеется набор стандартных шаблонов отчетов, предусмотрена также возможность создания пользовательских шаблонов отчетов. Отчеты отображаются в главном окне программы, в папке дерева консоли **Отчеты и уведомления**. Просмотрите доступные отчеты.

4.5. Управление компьютером

Kaspersky Security Center позволяет удаленно управлять клиентскими компьютерами: включать, выключать и перезагружать их. Создайте задачу управления клиентским компьютером:

1. Выберите Управляемые компьютеры – Задачи – Создать задачу.
2. Введите имя задачи.
3. Выберите узел Kaspersky Security Center, раскройте папку Дополнительно и выберите задачу Управление клиентским компьютером.
4. Выберите вариант перезагрузить компьютер.
5. Нажмите Далее, оставив ручной запуск.
6. Поставьте галочку Запустить задачу после завершения работы мастера.

4.6. Настройка политик антивируса

Kaspersky Security Center позволяет настраивать параметры работы антивируса через групповые политики. Создайте новую политику:

1. Выберите Управляемые компьютеры – Политики – Создать политику.
2. Введите имя политики.
3. Выберите KES 10 для Windows.
4. Не выбирайте конфигурационный файл.
5. Появится окно с основными подсистемами. Для изменения настроек подсистемы, выберите необходимую подсистему и нажмите Изменить. Отключите Сетевой экран. Выберите основные параметры защиты и поставьте галочку Применять технологию лечения активного заражения.
6. Нажмите далее.
7. Примите участие в программе Kaspersky Security Network.
8. Нажмите кнопку Настройка в группе Уведомления. Просмотрите доступные уведомления.
9. Включите защиту паролем.
10. Выберите Активная политика (Если уже существует аналогичная политика, она будет отключена, а активной станет только что созданная).

5. Контрольные вопросы

1. Что такое Kaspersky Security Center?
2. В каких режимах может работать Kaspersky Security Center?
3. Что включает в себя Kaspersky Security Center?
4. Какие основные функции в Kaspersky Security Center?
5. Что такое «Сервер администрирования»?
6. Что такое «Агент администрирования»?

7. Что такое «Инсталляционный пакет» и как его создать?

8. Что такое «Удаленная установка» и как ей пользоваться?

9. Как получить информацию о конкретном компьютере в сети?

10. Как осуществляется поиск и устранение уязвимостей?

Лабораторная работа №7
«Система сбора данных о программном и аппаратном обеспечении «Код Безопасности: Инвентаризация»

1. Цель работы

Изучить функциональные возможности системы сбора данных о программном и аппаратном обеспечении «Код Безопасности: Инвентаризация».

2. Краткие теоретические сведения

2.1. Назначение и основные функции системы

Система «Код Безопасности: Инвентаризация» — это программное средство, предназначенное для сбора сведений о программном и аппаратном обеспечении компьютеров в организации.

Система КБИ, разработанная компанией «Код Безопасности», обеспечивает:

−проведение плановых инспекций компьютеров в соответствии с заданным расписанием, а также внеплановых инспекций;

−поиск на локальных дисках компьютеров программных модулей и нежелательного контента (файлов mp3, avi, wmv и т. п.);

−учет и хранение информации о проведенных инспекциях;

−учет и хранение информации об установленном на компьютерах пользователей программном и аппаратном обеспечении;

−контроль установленного на компьютерах запрещенного и разрешенного к использованию программного обеспечения и оборудования;

−контроль и учет найденных на компьютерах программных модулей на основе входящей в состав системы библиотеки программного обеспечения;

−контроль подключения к компьютерам съемных носителей данных и некоторых других подобных устройств (USB, Wi-Fi, Bluetooth);

−генерацию отчетов по результатам, полученным в ходе инспекций;

−просмотр с удаленных компьютеров сведений, полученных в ходе проведения инспекций.

Информация об установленном на компьютерах программном и аппаратном обеспечении формируется на основании данных, полученных в результате инспектирования системных реестров ОС Windows и сканирования локальных дисков.

2.2. Компоненты системы

Система КБИ состоит из следующих программных компонентов:

−сервер — центральная часть, обеспечивающая взаимодействие всех компонентов, сбор и обработку данных;

−база данных (БД) — предназначена для хранения данных, полученных в ходе подготовки и проведения инспекций. В качестве сервера БД используется MS SQL Server 2005 (MS SQL Server 2005 Express Edition) или MS SQL Server 2008 (MS SQL Server 2008 Express);

−программа управления — предназначена для централизованного управления инспекциями и просмотра отчетов о результатах инспектирования;

−сервер отчетов — используется для формирования отчетов о событиях, происходящих при проведении инспекций, а также для отображения

полученных данных. В качестве сервера отчетов используется MS SQL Reporting Services;

–агент — этот компонент предназначен для сбора данных непосредственно на компьютерах доменной и одноранговой сети и на автономных компьютерах.

2.3. Интерфейс программы управления

Управление работой системы КБИ осуществляется с помощью специальной программы, основными функциями которой являются:

–управление заданиями на проведение инспекций;

–управление перечнем инспектируемых компьютеров;

–управление инспекциями;

–подготовка данных для работы с отчетами;

–работа с отчетами о результатах инспектирования.

Основное окно программы управления (рисунок 1) состоит из нескольких частей. В левой части основного окна — окне объектов — отображается список объектов управления, организованный в виде иерархического дерева.

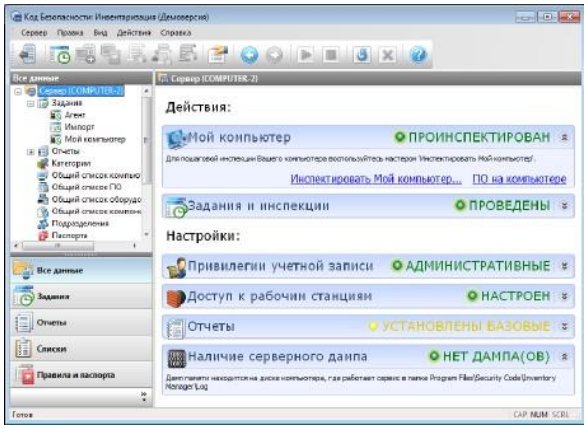


Рисунок 1 – Основное меню программы управления КБИ

В правой части основного окна — информационном окне — содержатся сведения и средства управления, относящиеся к выбранному объекту.

2.4. Инспекция компьютера

Инспекция компьютера может предоставить такую информацию о компьютере, как:

–сведения об установленной на компьютере ОС;

–сведения об установленном на компьютере ПО;

–список установленных на компьютере устройств;

–список всех съемных носителей данных и некоторых других подобных устройств, которые подключались к компьютеру по USB, Wi- Fi, Bluetooth (по информации из системного реестра);

–список учетных записей пользователей, работающих на данном компьютере (по информации из системного реестра об имеющихся локальных профилях);

−список компонентов программ, обнаруженных на локальных дисках компьютера;

−список файлов заданного типа, обнаруженных при сканировании локальных дисков компьютера.

Система КБИ позволяет проводить как плановые, так и внеплановые инспекции компьютеров, зарегистрированных в заданиях.

Плановые инспекции компьютеров проводятся автоматически в соответствии с расписанием, заданным в заданиях. Периодичность, дата и время проведения инспекций определяются параметрами заданий.

Средства системы КБИ позволяют учитывать и хранить информацию об инспекциях компьютеров.

Перечень проведенных инспекций и их результаты можно получить следующими способами:

−выполнить процедуру обзора инспекций компьютера;

−сформировать один из отчетов группы "Инспекции".

2.5. Паспорта компьютеров

Паспорт компьютера представляет собой объект системы КБИ, определяющий перечень программного обеспечения и оборудования, которое должно быть установлено на компьютере. Перечень программного обеспечения определяется набором правил из белого списка ПО, а оборудования — набором правил из белого списка оборудования.

3. Требования для выполнения работы

Работа выполняется на двух виртуальных машинах. Одна из них является сервером (Windows Server 2003 R2), а другая выполняет роль клиентской

машины (Windows XP Professional). В случае отсутствия подключения клиента к серверу – отключите брандмауэр на клиентской машине.

При выполнении работы используйте имена заданий и паспорта компьютера, соответствующего **имени учетной записи в кафедральной сети** (либо ФИО).

4. Ход работы

4.1. Инспектирование сервера

Сразу после загрузки сервера запустите Программу управления КБИ. Нажмите кнопку «Пуск» («Start») и активируйте в главном меню Windows команду «Все программы|Код Безопасности|Инвентаризация|Программа управления КБИ» или используйте ярлык программы на рабочем столе. При запуске произойдёт автоматическое соединение с сервером и на экране появится основное меню программы.

Сразу после запуска программы на экране появится стартовый диалог Мастера «Инспектировать Мой компьютер». Программа Мастер «Инспектировать Мой компьютер» предназначена для ознакомления с порядком подготовки и проведения инспекций.

Нажмите кнопку «Далее > ». На экране появится следующий диалог (рисунок 2).

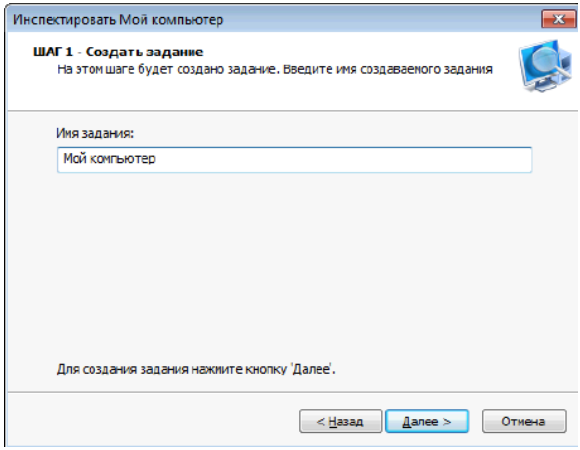


Рисунок 2 – Инспектирование локального компьютера

Укажите название создаваемого задания и нажмите кнопку «Далее > ». На экране появится диалог, в котором указано имя локального компьютера.

Для продолжения нажмите кнопку «Далее > ». На экране появится диалог, отражающий ход выполнения задания.

После успешного выполнения задания на экране появится диалог, предлагающий выбрать вариант просмотра результатов инспектирования (рисунок 3).

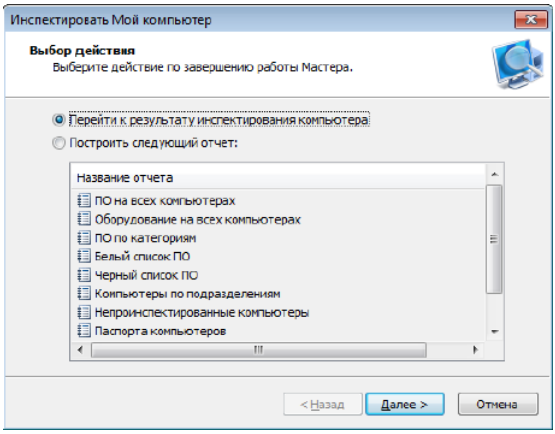


Рисунок 3 – Инспектирование локального компьютера

Отметьте поле «Перейти к результату...» и нажмите кнопку «Далее > ».

На экране появится заключительный диалог Мастера, содержащий информацию о действиях, выполненных на предыдущих шагах. Нажмите кнопку «Готово».

По аналогии с инспекцией локального компьютера проведите инспекцию клиентского компьютера, создав для этого отдельное задание.

4.2. Создание задания

Система КБИ позволяет создать одно или несколько заданий на проведение инспекций компьютеров домена.

Активируйте в меню команду «Действия|Создать|Задание».

При первом запуске мастера на экране появится стартовый диалог. Нажмите кнопку «Далее > ». На экране появится диалог для ввода названия задания.

Введите название задания и нажмите кнопку «Далее >».

На экране появится диалог для выбора способа выполнения задания (рисунок 4).

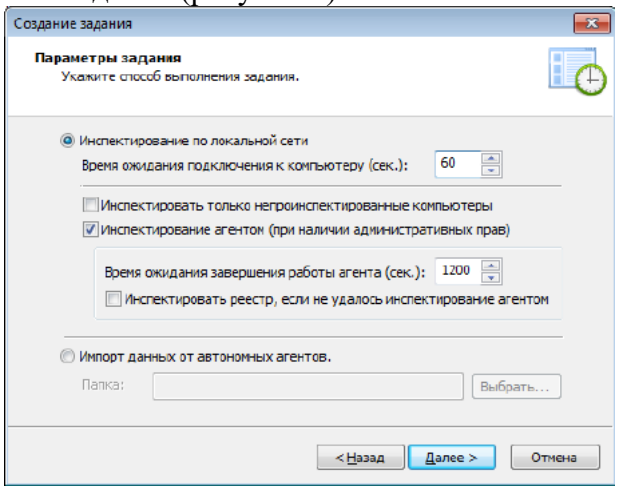


Рисунок 4 – Инспектирование локального компьютера

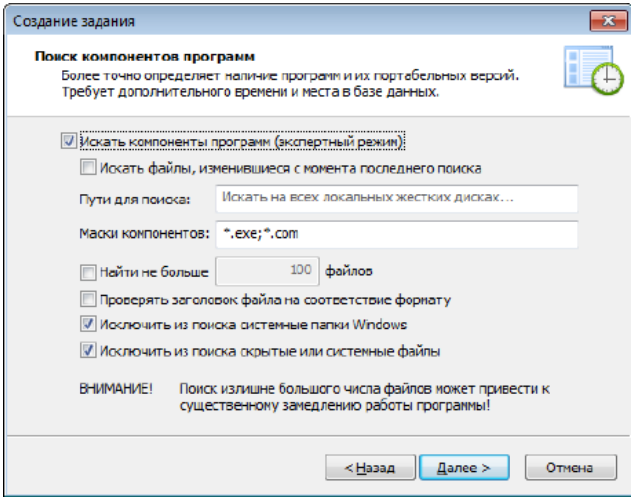
–Отметьте поле «Инспектирование по локальной сети»;

–в поле «Время ожидания подключения к компьютеру (сек.)» укажите период времени (от 10 до 999 сек.), в течение которого требуется предпринимать попытки подключения к каждому компьютеру, указанному в задании. По истечении заданного времени в случае отрицательного результата (например, если компьютер выключен) попытки подключения будут прекращены, а результат инспекции данного компьютера — признан неуспешным;

–отметьте поле «Инспектирование агентом...»;

–при инспектировании агентом в поле «Время ожидания завершения работы агента (сек.)» укажите период времени (от 30 до 1800 сек.), в течение которого сервер системы КБИ будет ожидать завершения работы агента на каждом инспектируемом компьютере. По истечении заданного времени сервер останавливает работу агента и сохраняет полученный результат в БД.

Нажмите кнопку «Далее > ». Если выбран способ инспектирования компьютеров по локальной сети с помощью агента, на экране появится диалог для



настройки параметров поиска компонентов программ (рисунок 5).

Рисунок 5 – Настройка параметров поиска компонентов программ

Отметьте те же поля, что и на рисунке 5 и нажмите кнопку «Далее > ». На экране появится диалог для настройки параметров поиска

нежелательного контента (файлов mp3, avi, wmv и т. п.) (рисунок 6).

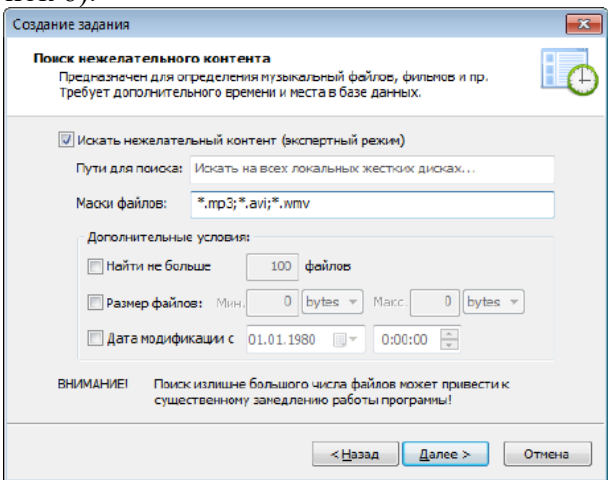


Рисунок 6 – Настройка параметров поиска компонентов и программ

–отметьте поле «Искать нежелательный контент»;

–В поле «Маски файлов» укажите расширения файлов «*.mp3;*.avi;*.wav»;

Нажмите кнопку «Далее > ». Поставьте галочку **Использовать специальную учетную запись.** Поставьте значения: Домен – SAM, Имя пользователя – Администратор, Пароль - 12345.

Нажмите кнопку «Далее > ». Если выбран способ инспектирования компьютеров по локальной сети, на экране появится диалог выбора способа добавления компьютеров в задание.

Установите отметку в поле «Добавлять компьютеры вручную» и нажмите кнопку «Далее > ».

Откажитесь от рассылки отчётов по электронной почте и установите запуск задания вручную. На экране появится заключительный диалог мастера. В поле

«Подробности» отобразится наименование создаваемого задания.

Чтобы приступить к формированию списка инспектируемых компьютеров, — отметьте поле «Добавить компьютеры в задание» и нажмите кнопку «Готово». Работа мастера создания задания будет завершена, а на экране появится стартовый диалог мастера добавления компьютеров в задание.

Просмотрите доступные способы добавления компьютеров и добавьте одним из них клиентский компьютер (XP-MSDN). Отключите брандмауэр на клиентской машине.

4.3. Просмотр списка заданий

Все созданные задания составляют список, который можно посмотреть как в окне объектов, так и в информационном окне. В информационном окне для каждого задания приводятся следующие сведения:

−тип инспектирования (способ выполнения задания);

−текущий статус (выполняется/не выполняется);

−расписание;

−дата и время выполнения последней и следующей инспекций.

Для просмотра списка заданий выберите в окне объектов элемент «Задания». В верхней части информационного окна отобразится список имеющихся заданий, содержащий перечисленные выше сведения.

В нижней части информационного окна содержится отчет (при его наличии) о выполнении задания, выбранного в верхней части.

Выберите ранее созданное Вами задание и запустите его на выполнение (с помощью

контекстного меню или кнопки на панели задач). Просмотрите отчёт о выполнении задания и проанализируйте его результаты.

4.4. Изменение параметров задания

Параметры, указанные при создании задания, можно изменить.

Для изменения параметров задания выберите в окне объектов задание, параметры которого требуется изменить, и активируйте в меню команду «Правка|Свойства».

На экране появится диалоговое окно для настройки параметров задания (рисунок 7).

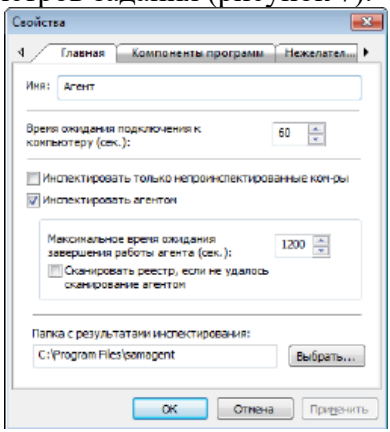


Рисунок 7 – Настройка параметров поиска компонентов и программ

Измените периодичность выполнения задания. Установите выполнение задания один раз через две - три минуты после текущего времени. Нажмите кнопку «ОК». Дождитесь окончания выполнения задания и просмотрите отчёт о проведении инспекции.

4.5. Создание паспорта компьютера

Для работы со списком паспортов выберите в окне объектов элемент «Правила и паспорта». Список паспортов компьютеров содержится в верхней части информационного окна, а в нижней части этого окна находятся перечни правил белого списка ПО и оборудования, относящиеся к выбранному в списке паспорту.

Выберите в окне объектов элемент «Правила и паспорта» и активируйте в главном меню команду «Действия|Создать|Паспорт». На экране появится стартовый диалог мастера создания паспорта.

Нажмите кнопку «Далее >». На экране появится следующий диалог (рисунок 8).

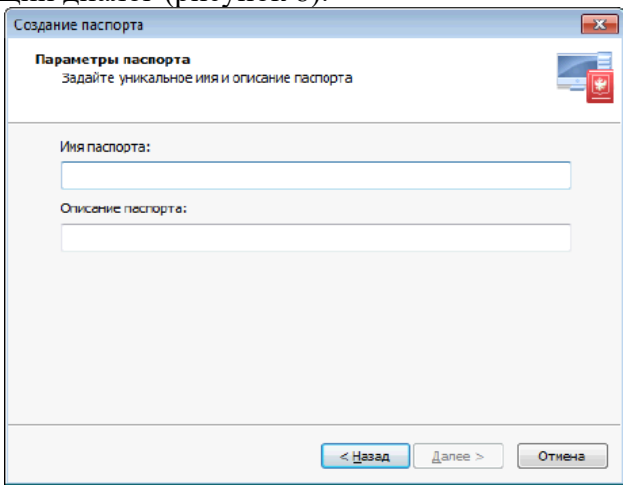


Рисунок 8 – Настройка параметров поиска компонентов и программ

В поле «Имя паспорта» введите название паспорта (это поле обязательно для заполнения), а в поле «Описание паспорта» — его словесное описание и нажмите кнопку «Далее > ».

На экране появится диалог для выбора варианта создания паспорта. Выберите вариант «**Заполнить**

паспорт результатами инспекции компьютера» — паспорт будет создан на основе перечня ПО и оборудования, полученного в результате инспектирования конкретного компьютера. Нажмите кнопку «Далее > ».

На экране появится диалог для выбора компьютера и инспекции (рисунок 9).

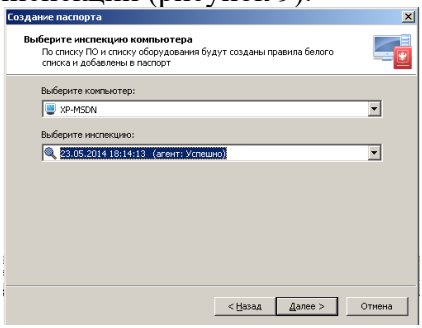


Рисунок 9 – Настройка параметров поиска компонентов и программ

В первом открывающемся списке выберите компьютер XP-MSDN, во втором — последнюю инспекцию этого компьютера и нажмите кнопку «Далее >». На экране появится диалог, содержащий перечень ПО, обнаруженного на данном компьютере в результате проведения выбранной инспекции.

Установите отметки слева от названий ПО, описание которого хотите добавить в паспорт, и нажмите кнопку «Далее >».

На экране появится диалог с перечнем оборудования, обнаруженного на данном компьютере в результате проведения выбранной инспекции. Нажмите «Выбрать всё» и нажмите кнопку «Далее >».

На экране появится заключительный диалог мастера. Нажмите кнопку «Готово». Выдайте только

что созданный паспорт компьютеру XP-MSDN. Для этого:

1) выберите в окне объектов элемент «Общий список компьютеров»;

2) вызовите контекстное меню для компьютера XP-MSDN и активируйте в нем команду: «Выдать паспорт компьютеру»;

3) поставьте отметку слева от созданного Вами паспорта и нажмите кнопку «Готово».

4.6. Добавление правила черного списка ПО

Для добавления правила выберите в окне объектов элемент «Правила черного списка ПО» и нажмите на панели инструментов кнопку «Создать правило черного списка ПО». На экране появится стартовый диалог мастера создания правила.

Нажмите кнопку «Далее > ». На экране появится диалог для ввода названия правила. В поле «Название» введите название правила (это поле обязательно для заполнения), а в поле «Описание» — его словесное описание и нажмите кнопку «Далее > ».

На экране появится диалог для выбора варианта продолжения процедуры. Выберите вариант «Общий список ПО» – правило будет создано на основе общего списка ПО, обнаруженного на компьютерах при проведении инспекций – и нажмите кнопку «Далее > ».

На экране появится диалог, содержащий общий список ПО. Выберите программу doPDF 7.2 Printer, найденную при инспекции клиентского компьютера, и нажмите кнопку «Далее > ».

На экране появится диалог для настройки параметров правила. В текстовых полях диалога введите или отредактируйте одноименные параметры, описывающие искомое ПО. Для обозначения любого,

произвольного набора символов используйте символ «*» (звездочка). Например, если ввести значение «*Microsoft*», заданное в поле «Производитель», то в отчет будут добавлены все продукты данного производителя (при условии совпадения значений остальных параметров), содержащие в любом месте названия производителя это слово. А значение «*», заданное в поле «Версия», укажет на то, что в отчет нужно добавить сведения обо всех без исключения найденных версиях данного ПО.

Введите в поле название «doPDF*». Поле «Производитель» оставьте пустым. Нажмите кнопку «Далее> ». На экране появится заключительный диалог мастера, содержащий описание созданного правила. Нажмите кнопку «Готово».

Установите на клиентском компьютере архиватор 7-zip. На сервере проведите инспекцию клиентской машины. Покажите найденный архиватор в результатах инспекции.

4.7. Работа с отчетами

Откройте вкладку «Отчеты». Просмотрите доступные виды отчетов. Создайте следующие отчеты:

−отчет «Компьютеры с ПО из черного списка», выбрав правило, содержащее принтер doPDF;

−отчет «Компьютеры без паспорта»;

−отчет «Несоответствующие паспорту компьютеры»;

−отчет «Изменения ПО на всех компьютерах»;

Экспортируйте один из отчетов в pdf файл.

5. Контрольные вопросы

1. Назначение системы КБИ.

2. Из каких программных компонентов состоит система КБИ?

3. Основные функции системы КБИ.

4. Что такое паспорт компьютера?

5. Для чего нужны отчёты о результатах инспектирования? Какие группы отчётов предлагаются системой КБИ?

6. Назовите все имеющиеся в системе КБИ варианты запуска задания.

Литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с.

2. Фомин, Д. В. Информационная безопасность и защита информации [Электронный ресурс]: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с.

3. Ермакова, А. Ю. Методы и средства защиты компьютерной информации [Электронный ресурс]: учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с.