Лабораторная работа № 6. Система защиты информации «Secret Net»

Цели:

1) расширение представлений о программных способах решения задач информационной безопасности;
2) расширение представлений о комплексном подходе к обеспечению информационной безопасности;
3) освоение системы комплексной защиты информации «Secret Net»;
4) получение опыта работы с системами комплексной защиты информации.

Задачи:

1) ознакомьтесь с приведённой теорией и описанием СЗИ «Secret Net»;
2) в соответствии с приведёнными далее инструкциями выполните лабораторную работу;
3) продемонстрируйте и прокомментируйте полученные результаты работы;
4) подготовьте ответы на вопросы, приведённые в конце лабораторной работы;
5) ответьте на вопросы преподавателя по лабораторной работе.

Теория

Системы защиты информации реализуют комплексный подход к защите информационных и аппаратных ресурсов компьютеров и сетей. Они взаимодействуют со средствами защиты информации операционной системы и значительно расширяют их.

«Secret Net» в отличие от некоторых других систем, в том числе «Страж NT», обладает неплохим сетевым функционалом и может функционировать в двух режимах: сетевом (с иерархической клиент-серверной структурой с любым количеством уровней) и автономном (устанавливается и действует на одном компьютере). В ходе данной лабораторной работы вы познакомитесь именно с автономным режимом работы.

СЗИ, как правило, выделяют 3 основных группы ресурсов:

1) файловые ресурсы (файлы и каталоги на локальных и сетевых дисках);

2) программные ресурсы (различные программы и другие запускаемые файлы);

3) аппаратные ресурсы (устройства, подключённые или потенциально подключаемые к компьютеру).

Пользователям нужно не просто предоставить доступ к этим ресурсам, но и управлять им. При том более надёжно и гибко, чем это возможно сделать средствами ОС. СЗИ решают эту задачу: они не замещают ОС, а взаимодействуют с ней, расширяя возможности для управления доступом, повышения защищённости входа в систему, журнализации и решения ряда других задач. СЗИ предоставляет, как правило, более удобные инструменты, чем встроенные средства операционной системы, и расширяет список решаемых в системе задач обеспечения информационной безопасности.

Основные защитные функции, реализуемые системой Secret Net 6:

1) контроль входа пользователей в систему;

2) разграничение доступа пользователей к устройствам компьютера;

3) создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды — ЗПС);

4) разграничение доступа пользователей к конфиденциальным данным;

5) контроль потоков конфиденциальной информации;

6) контроль вывода конфиденциальных данных на печать;

7) контроль целостности защищаемых ресурсов;

8) контроль аппаратной конфигурации компьютера;

9) функциональный контроль ключевых компонентов СЗИ «Secret Net»;

10) уничтожение (безвозвратное удаление) содержимого файлов при их удалении;

11) регистрация событий безопасности в журнале СЗИ «Secret Net»;

12) мониторинг и оперативное управление защищаемыми компьютерами (только в сетевом режиме);

13) централизованный сбор и хранение журналов (только в сетевом режиме);

14) централизованное управление параметрами механизмов защиты (только в сетевом режиме);

15) защита доступа к Active Directory при сетевых обращениях компонентов системы «Secret Net» (только в сетевом режиме).

Все эти функции реализуются по средством специальных защитных механизмов данной СЗИ. В зависимости от назначения защитные механизмы можно разделить на следующие группы:

1. Механизмы защиты входа в систему:

1) средства идентификации и аутентификации пользователей;

2) функции блокировки компьютера;

3) аппаратные средства защиты от загрузки ОС со съемных носителей.

2. Механизмы разграничения доступа и защиты ресурсов:

1) механизм полномочного разграничения доступа к объектам файловой системы;

2) механизм замкнутой программной среды;

3) механизм разграничения доступа к устройствам компьютера;

4) механизм затирания информации, удаляемой с дисков компьютера.

3. Механизмы контроля и регистрации:

1) механизм функционального контроля подсистем;

2) механизм регистрации событий безопасности;

3) механизм контроля целостности;

4) механизм контроля аппаратной конфигурации компьютера;

5) механизм контроля печати.

Для обеспечения дополнительной защиты входа в СЗИ могут применяться аппаратные ключи, в роли которых могут выступать как специальные устройства (eToken, iKey, Rutoken или iButton), а также обычные флеш-накопители.

Функции блокировки компьютера предназначены для защиты компьютера от НСД и может быть включена при простое, по команде пользователя, при обнаружении СЗИ событий, нарушающих заданную политику безопасности, а также в ряде других случаев.

В качестве аппаратных средств защиты от загрузки ОС со съёмных носителей относятся ПАКи: специализированные программно-аппаратные комплексы. Речь о них пойдёт в следующих лабораторных работах.

В ходе лабораторной работы вы познакомитесь с этими механизмами более подробно. **Обратите внимание,** что при работе с СЗИ «Secret Net» большинство настроек вступают в силу только при следующем входе пользователя в систему. Поэтому, чтобы проверить действие сделанных изменений нужно в меню «Пуск» выбрать пункт «Выйти из системы». Выполнять перезагрузку виртуальной машины не нужно.

Инструкция

Сначала определим модель, которую вы будете реализовывать средствами СЗИ. Пусть стоит задача защитить ресурсы компьютера, находящегося в помещении исследовательского отдела. В отделе работают начальник и две исследовательские группы, каждая из которых включает рядовых сотрудников и главу группы. Соответственно должностям в системе должны существовать пользователи, приведённые в таблице 10. Пользователи входят в группы, представленные на рисунке 100.

Отдел занимается секретными исследованиями, поэтому исследователи, входящие в одну группу не должны иметь доступ к закрытым документам другой группы. Один из исследователей входит в обе исследовательские

группы, соответственно должен входить в обе группы пользователей. Распределение пользователей по группам представлено в таблице 11.

Таблица 10

Список пользователей СЗИ

Пользователь	**Должность**
Alpha	Начальник отдела.
Bettal, Betta2	Начальники рабочих групп.
Epselonl. Epselon2. Epselon3	Исследователи, входящие в рабочие группы.
Omega	Стажёр.

Рис. 100. **Группы пользователей и их иерархия**

Распределение пользователей по группам

Пользователь	Группы
Alpha	Inside
Bettal	AGroup + Inside
Betta2	BGroup + Inside
Epselonl	AGroup + BGroup + Inside
Epselon2	AGroup + Inside
Epselon3	BGroup + Inside
Omega	Inside

Сотрудники отдела Centavra работают с секретной информацией: глава отдела имеет доступ к сверх секретным документам, главы рабочих групп и исследователи — только к секретным. Но один из исследователей может работать со сверхсекретными документами. Стажёры — это неопытные сотрудники, пришедшие практиковаться в отдел. Они не имеют допуска к секретной информации. Соответствующие их уровни допуска пользователей представлены в таблице 12.

Таблица 12

Уровни допуска пользователей

Пользователь	Уровень доступа
Alpha	TS (совершенно секретно)
Bettal	S (секретно)
Betta2	s
Epselonl	TS
Epselon2	S
Epselon3	s
Omega	NS (не секретно)

В помещении отдела установлены принтеры: у каждой группы исследователей по одному «секретному» и одному «несекретному» принтерам. Секретным будем называть принтер, на котором разрешено печатать секретные документы.

Пусть на обычном компьютере, установленном в первой группе исследователей, могут работать пользователи: alpha, bettal, epselonl, epselon2 и omega.

Кроме того, существует общий файловый ресурс, разделяемый всеми пользователями, но доступ к элементам которого пользователи получают в соответствии с правилами перечисленным в таблице 13 и своим допуском к секретности.

Правила доступа пользователей к общему файловому ресурсу

Пользователь	Правила
Alpha	Имеет доступ ко всем файлам и каталогам ресурса
Bettal, Betta2	Имеет доступ ко всем файлам своей исследовательской группы
Epselonl-3	Имеет доступ ко всем файлам своей исследовательской группы
Omega	Имеет доступ ко всем файлам.

Установка СЗИ

Эксплуатация начинается с установки программного продукта. Установка СЗИ «Secret Net» в автономном режиме проста, но всё же есть некоторые детали, на которые стоит обратить внимание:

1) лучше устанавливать СЗИ на «чистые» ОС, то есть на недавно установленные, содержащие минимум ошибок и проблем, возникающих в ходе их эксплуатации;
2) компьютер не должен содержать вирусного или вредоносного ПО;
3) лучше установить необходимое ПО до установки СЗИ;
4) на компьютере обязательно должно быть установлено всё необходимое аппаратное обеспечение, так как эта конфигурация будет принята СЗИ в качестве эталонной и в дальнейшем отличия обнаруженной аппаратной конфигурации от эталонной система будет воспринимать как нарушения информационной безопасности.

Теперь можно непосредственно переходить к установке. Подключите установочный носитель с СЗИ «Secret Net» и запустите autorun.exe. Перед вами появится окно, представленное на рисунке 101.

Выберите пункт «Клиентское ПО» — это запустит установку программ СЗИ, предназначенных для работы на компьютере пользователя. В следующем окне выберите автономный режим работы (см. рис. 102). Нажмите «Далее» — начнётся установка выбранной версии ПО (см. рис. 103).

Рис. 101. **Программа автозапуска установочного комплекта СЗИ «Secret Net»**

Secret Net 6

Режим работы продукта

Выберите режим работы продукта

Сетевой режим

В данном режиме система позволяет осуществлять централизованное управление доменными пользователями, управление параметрами с помощью механизма групповых политик, оперативное управление системой.

? Автономный режим]

В данном режиме все настройки системы осуществляются локально.

Внимание! Выбор режима работы системы возможен только в процессе установки. Во время установки потребуется ввести серийный номер подходящего типа.

Далее > Отмена

Рис. 102. Окно выбора режима работы

Secret Net 6

Secret Net 6

система защиты информации

Platform: Win32

Вас приветствует программа установки Secret Net 6 версии 6.5.333.53 (автономный режим)

Программа выполнит установку Secret Net 6 версии 6.5.333.53 (автономный режим) на компьютер. Для продолжения нажмите кнопку "Далее".

ПРЕДУПРЕЖДЕНИЕ: Данная программа защищена законами об авторских правах и международными соглашениями.

1Далее > j Отмена

Рис. 103. **Окно мастера установки СЗИ «Secret Net»**

Следующим шагом мастер установки попросит ввести серийный номер (см. рис. 104). Серийные номера лицензионных версий поставляются вместе с установочными дисками, но в разделе «Демоверсии» на сайте разработчика http://www.securitycode.ru/ после регистрации можно найти бесплатные демонстрационные ключи, которые позволяют использовать полнофункциональную версию программы в течение 175 дней.

Рис. 104. **Окно ввода регистрационного ключа**

Подтвердите ввод ключа и выберите папку установки ПО (см. рис. 105). Затем программа попросит заполнить форму «Учётные данные компьютера», представленную на рисунке 106. Заполните поля в соответствии с предложенной моделью подразделения.

fj? Secret Net 6

Папка назначения

Нажмите кнопку "Далее", чтобы установить в эту папку, Нажмите кнопку "Изменить", чтобы выполнить установку в другую папку.

Установка Secret Net 6 в:

C:Program FilesSecret NetClient

Изменить...

< Назад

(Далее > j| Отмена

Рис. 105. **Окно выбора пути установки**

Рис. 106. **Окно ввода учётной информации**

На следующем шаге откроется окно, представленное на рисунке 107. При включении опции «Выполнить расстановку прав доступа на файлы...» выполняется замена прав доступа. Эта операция усиливает защищённость операционной системы, однако выполнять её рекомендуется только в тех случаях, когда после установки ОС администратор не осуществлял специальную расстановку прав доступа.

Рис. 107. **Окно настройки дополнительных параметров установки**

Следует отметить, что на каталог установки СЗИ автоматически устанавливаются особые права доступа, повышающие защищённость самой СЗИ. Включите эту опцию и нажмите кнопку «Далее». После выполнения действий по установке основных компонентов, мастер сообщит об успешном завершении установки программы и дополнительного ПО (см. рис. 108, 109).

Рис. 108. **Окно завершения установки основных компонентов программы**

Рис. 109. **Окно установки дополнительного ПО**

После этого появится окно «Управление Secret Net», представленное на рисунке НО. В нём можно просмотреть основные сведения о системе и сделать общие настройки. Просмотрите содержимое вкладок в этом окне. Менять что-либо на данном этапе не будем.

Рис. ПО. Окно управления СЗИ

Нажмите «ОК» и дождитесь завершения работы программы. Если перезагрузка не началась автоматически, выполните её самостоятельно. При загрузке компьютера вы увидите первые изменения (см. рис. 111). Войдите в систему под учётной записью администратора.

© Secret Net 6

Демо-версия [осталось 175 дней]

Операционная система Windows

Kefrrpapn

Нажмите Ctrl-Alt-Delete или предъявите персональный идентификатор.

Сочетание клавиш Ctrl-Alt-Del помогает сохранить ваш пароль в безопасности. Нажмите кнопку "Справка" для получения дополнительных сведений.

? Windows

Professional

?лравк.з

Рис. 111. **Модифицированное окно интерактивного входа в систему**

Создание пользователей и групп

Начнём с создания групп и пользователей. СЗИ предоставляет удобный доступ к инструментам управления компьютером через свою группу в меню «Пуск». Откройте инструмент «Управление компьютером», раздел «Локальные пользователи и группы». Перейдите в раздел «Пользователи» (см. рис. 112) и создайте необходимых пользователей в соответствии с моделью, описанной ранее.

Затем перейдите в раздел «Группы» и создайте 3 группы, отражающие описанную ранее модель подразделения. Добавьте пользователей в созданные группы в соответствии с описанием организационной структуры. Для поиска пользователей можно в окне «Выбор пользователей» использовать комбинацию поиск, в разделе «Дополнительно».

Свойства созданных групп после добавления в них пользователей примут вид, представленный на рисунке 113.

2 Управление компьютером

Рис. 112. **Окно «Управление компьютером», создание нового пользователя**

Рис. 113. **Свойства созданных групп после добавления пользователей**

Управление доступом к ресурсам осуществляется одновременно с применением двух подходов: полномочного, при котором сравниваются уровни допуска пользователя или процесса с грифом запрашиваемого объекта, и дискреционного, при котором пользователям и группам пользователей назначаются правила доступа к определённым объектам.

Дискреционный подход присутствует в самой ОС и реализуется её собственными средствами. А вот полномочный подход, как правило, реализуется дополнительными средствами, в данном случае — СЗИ.

Зададим пользователям уровни допуска, то есть определим максимальную степень секретности документов, к которым они могут получить доступ. Выполним установку уровня доверия для пользователя *alpha.*

Для присвоения уровня допуска пользователю, нужно открыть свойства соответствующего пользователя: «Управление компьютером — Локальные пользователи — Пользователи» и перейти на вкладку «Secret Net» (см. рис. 114).

На этой вкладке расположены инструменты управления идентификаторами, ключами и допуском текущего пользователя. Нажмите

кнопку «Доступ» в столбце слева — вкладка «Secret Net» примет вид, представленный на рисунке 115.

Рис. 114. **Свойства пользователя Alpha, вкладка «Secret Net»**

Рис. 115. **Свойства пользователя Alpha, вкладка «Secret Net», уровень доступа**

В начале лабораторной работы были определены уровни допуска пользователей. В соответствии с ними, пользователь *alpha* имеет наивысший допуск секретности. В выпадающем списке выберите подходящий уровень допуска (см. рис. 116).

При этом стали активны дополнительные опции:

1. «Печать конфиденциальных документов» — разрешить ли пользователю печатать документы с грифом секретности выше NS.
2. «Управление категориями конфиденциальности» — разрешить ли пользователю изменять гриф объектов в пределах своего уровня

допуска (то есть, если пользователь имеет достаточный уровень допуска для работы с документом и права на доступ к нему, то он может изменять гриф секретности объекта на гриф, не превышающий текущего уровня допуска пользователя).

3. «Вывод конфиденциальной информации» — разрешить ли пользователю копировать объекты с грифом выше NS на съёмные диски.

Дайте все эти привилегии пользователю *alpha* и настройте допуски других пользователей отдела. **И не забудьте указать уровень допуска и привилегии учётной записи администратора!**

Рис. 116. **Присвоение пользователю Alpha наивысшего уровня допуска**

Создание файловых ресурсов

Создайте на жёстком диске компьютера каталог «Centavra» — он будет корневым каталогом для общего файлового ресурса отдела. Затем воссоздайте структуру каталогов, предложенную на рисунке 117.

Гриф доступа к объекту задаётся на вкладке «Secret Net» в свойствах этого объекта (см. рис. 118).

Опция «Автоматически присваивать новым файлам» означает, что при копировании в данный каталог или создании в нём файлов, файлам будет присваиваться гриф секретности этого каталога.

Настройте права доступа и грифы секретности ресурсов в соответствии с предложенной ранее моделью. Добавьте ресурсы на своё усмотрение, чтобы можно было бы проверить работу СЗИ.

Group A

Group B

Рис. 117. **Структура каталогов общего файлового ресурса**

Рис. 118. **Присвоение грифа «Не секретно» папке «Отдел А»**

Работа с идентификаторами

Персональный идентификатор— устройство для хранения информации, необходимой при идентификации и аутентификации пользователя. В идентификаторе могут храниться криптографические ключи для усиленной аутентификации пользователя.

В качестве идентификаторов могут быть использованы флэшки, дискеты или специальные устройства, напоминающие обычные флэшки или ключи от домофонов. Различные СЗИ могут поддерживать различные типы идентификаторов — информацию об этом стоит смотреть в документации к ним.

Для работы с идентификаторами нужно открыть окно свойств пользователя, вкладку «Secret Net» — здесь же вы задавали уровень доступа пользователя. Нажмите кнопку «Идентификатор» на панели слева (см. рис. 119).

Рис. 119. **Окно «Свойства» пользователя Alpha, вкладка «Secret Net», работа с идентификаторами**

Присвоение идентификатора пользователю в общем случае состоит из двух этапов:

1. Инициализация — форматирование идентификатора.
2. Присвоение — запись в идентификатор данных, необходимых для его использования, и привязка идентификатора к выбранному пользователю.

Первый этап — инициализация. Подключите идентификатор к компьютеру и нажмите «Инициализация». Если вы используете в качестве идентификатора флэш-диск, в появившемся окне нажмите кнопку «Диск» (см. рис. 120). При этом произойдёт сканирование подключённых съёмных носителей и подходящие, по мнению программы, отобразятся в списке.

Выберите нужный идентификатор в таблице и нажмите ещё раз «Диск» — статус выбранного идентификатора изменится на «Обработан» (см. рис. 120). Это значит, что выбранное вами устройство готово для дальнейшей работы. Закройте это окно.

Рис. 120. **Окно со списком подключённых персональных идентификаторов**

Второй этап — присвоение. Обратите внимание, что каждому пользователю можно присвоить сколько угодно идентификаторов, но каждый идентификатор может быть привязан только к одному пользователю.

В окне свойств пользователя нажмите кнопку «Присвоить...» — откроется окно мастера присвоения идентификаторов, представленное на рисунке 121.

СЗИ предоставляет возможность хранения пароля учётной записи Windows на идентификаторе, что позволяет входить в систему без ручного ввода пароля: пароль автоматически будет считан при предъявлении идентификатора.

Опция «Записать в идентификатор закрытый ключ пользователя» означает, что в идентификаторе будет храниться ключ, используемый при усиленной аутентификации (режиме, при котором для входа в систему запрашивается не только пароль и идентификатор, но специальный криптографический ключ).

Присвоение персональных идентификаторов

Настройка режимов использования идентификаторов

Укажите операции, которые необходимо выполнить для настройки режимов использования персональных идентификаторов, присваиваемых пользователю.

J Включить режим хранения пароля

У Записать пароль в идентификатор

У ^писатьв„идентификатор^^ыт^клю^пользомтеля!

j Далее > j Отмена

Рис. 121. **Окно «Присвоение персональных идентификаторов»**

Продолжите работу с мастером и присвойте пользователю аппаратный идентификатор. После успешного присвоения, добавленный идентификатор появится в списке идентификаторов пользователя (см. рис. 122).

Может случиться так, что у вас окажется несколько идентификаторов и будет неизвестно, какому пользователю каждый из них принадлежит. Для подобных ситуаций «Secret Net» предоставляет функцию проверки принадлежности идентификатора пользователю. Чтобы воспользоваться этой функцией нажмите кнопку «Сервис» на панели слева (см. рис. 123).

Рис. 122. **Список персональных идентификаторов пользователя Alpha**

Рис. 123. **Окно «Свойства» пользователя Alpha, вкладка «Secret Net», раздел «Сервис»**

Подключите идентификатор к компьютеру и нажмите кнопку «Проверить» — появится сообщение с информацией об идентификаторе аналогичное представленному на рисунке 124.

Рис. 124. **Окно информации об идентификаторе**

Вернитесь на вкладку «Secret Net» и перейдите в раздел «Криптоключ» (см. рис. 125). Теперь в окне отображаются данные о ключе для усиленной аутентификации текущего пользователя. Смените действующий крипто ключ пользователя. В результате работы мастера вы должны увидеть окно, представленное на рисунке 126.

Свойства: alpha

Общие Членство в группах Профиль

СШД Secret Nel 6

Сведения о криптографическом ключе пользователя:

Создан: 11/03/2014

Годен до: 06/03/2015

Действителен еще: 359 дня(ей)

Чтобы сменить текущий криптографический ключ, нажмите кнопку “Сменить..

i= Сменить...

Чтобы скопировать криптографический ключ с одного электронного идентификатора на другой, нажмите кнопку "Копировать..."

Копировать.

Закрыть

Применить

Справка

Рис. 125. Окно «Свойства» пользователя Alpha, вкладка «Secret Net», раздел «Криптоключ»

Рис. 126. **Окно результатов смены криптографических ключей пользователя**

Срок действия ключей настраивается в «Локальной политике безопасности» ветке «Secret Net», раздел «Ключи пользователей». Задайте продолжительность действия ключа 2 месяца и соответственно измените другие параметры этого раздела.

Присвойте персональный идентификатор для учётной записи администратора. В ветке «Secret Net» включите режим идентификации и аутентификации пользователей по персональному идентификатору. Попробуйте теперь выполнить вход в систему и проверить работу механизма усиленной идентификации.

Настройка контроля программ и данных

СЗИ «Secret Net» содержит средства контроля изменений (механизм контроля целостности) объектов файловой системы и контроля используемого пользователями ПО (механизм замкнутой программной среды). Для их настройки разработчики «Secret Net» предлагают последовательность этапов, описанную ниже. Но, до её рассмотрения нужно пояснить несколько понятий.

Параметры, определяющие работу механизмов контроля целостности и замкнутой программной среды, объединены в рамках единой модели данных. Модель данных представляет собой иерархию объектов и описание связей между ними. В модели используются 5 категорий объектов:

1. Ресурс — описание файла или каталога, переменной реестра или ключа реестра. Однозначно определяет местонахождение контролируемого ресурса и его тип.
2. Группа ресурсов — объединяет несколько описаний ресурсов одного типа (файлы и каталоги или объекты системного реестра). Например, исполняемые файлы или ключи реестра, относящиеся к конкретному приложению.
3. Задача — это набор «групп ресурсов». Например, задача может одновременно включать группу системных файлов и группу объектов системного реестра Windows.
4. Задание — определяет параметры проведения контроля целостности. Например, при использовании замкнутой программной среды может объединять описания исполняемых файлов, разрешённых для запуска определённой группе пользователей.
5. Субъект управления — компьютер и группа, включающая пользователей и компьютеры (при локальном управлении — также и отдельные пользователи). Определяет компьютеры, на которых выполняется контроль целостности в соответствии с назначенными заданиями, и пользователей, которым разрешено запускать программы, указанные заданиями замкнутой программной среды.

Этап 1 — Подготовка к построению модели данных.

На этом этапе проводится анализ размещения ПО и данных на защищаемых компьютерах. Разрабатываются требования к настройке механизмов КЦ и ЗПС. Выполняется размещение необходимого ПО и данных на защищаемых компьютерах.

Этап 2 — Построение фрагмента модели данных по умолчанию.

Работа механизмов КЦ и ЗПС в СЗИ «Secret Net» основывается на специальной «модели данных», описывающей ресурсы компьютера, важные для нормальной работы контроля целостности и замкнутой программной среды.

Данный этап выполняется при формировании новой модели с нуля. При этом в модель данных автоматически добавляются описания ресурсов для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ.

Этап 3 — Добавление задач в модель данных.

В модель данных добавляются описания задач — прикладного и системного программного обеспечения, наборов файлов данных и других ресурсов, к которым должны применяться КЦ и ЗПС в соответствии с требованиями, разработанными на 1 этапе.

Важно отметить, что задачи и задания в модели данных СЗИ «Secret Net» могут относиться к одному из двух механизмов: к контролю целостности или к замкнутой программной среде.

Этап 4 — Создание заданий и включение в них задач.

В модель данных добавляются все необходимые задания, то есть задаётся информация о том, как применять КЦ и ЗПС к задачам, включённым в каждое отдельное задание.

Этап 5 — Назначение субъектам заданий ЗПС и подготовка ресурсов ЗПС.

На данном этапе каждый пользователь связывается со своим набором заданий — правилами, применяемыми механизмом ЗПС в отношении этого конкретного пользователя.

Для того чтобы исполняемые файлы контролировались механизмом ЗПС, им должен быть присвоен признак «выполняемый». В противном случае, замкнутая программная среда просто не позволит их запускать ещё до проверки каких-либо привилегий пользователя. Процедура «Подготовка ресурсов для ЗПС» как раз выполняется на текущем этапе: она производит сканирование компьютера на наличие исполняемых файлов и присваивает им соответствующий признак.

Этап 6 — Расчёт эталонов.

Для всех заданий рассчитываются эталоны ресурсов. Эталон в данном случае означает некоторый набор значений признаков контролируемого

объекта, с помощью которых можно обнаружить изменения, произошедшие с объектом. В качестве признака объекта может выступать контрольная сумма, его имя, размер, путь, дата и время его создания или изменения.

Этап 7 — Включение ЗПС в «жёстком» режиме.

В «жёстком» режиме разрешается запуск только разрешённых программ, библиотек и сценариев**.** Запуск других ресурсов блокируется, а в журнале СЗИ «Secret Net» регистрируются события НСД.

Этап 8 — Включение механизма КЦ.

Устанавливаются связи заданий контроля целостности с субъектами «компьютер» или «группа компьютеров». С этого момента механизм КЦ начинает действовать в штатном режиме.

Этап 9 — Проверка заданий.

Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности настроек заданий. Проверка заключается в немедленном выполнении задания независимо от установленного расписания.

Выполним поэтапно настройку механизмов КЦ и ЗПС. Этап 1 — подготовка к построению модели данных. По плану, на этом этапе разрабатываются требования к настройке КЦ и ЗПС, включающие в себя: сведения о защищаемых компьютерах (установленное ПО, пользователи и их функциональные обязанности, задачи, решаемые пользователями по служебной необходимости); перечень ресурсов, подлежащих контролю целостности; перечень программ, с которыми разрешено работать разным группам пользователей; задачи (список задач и их краткое описание).

Пусть пользователи смогут работать с ПО так, как указано в таблице 14. В реальных условиях подготовка к использованию СЗИ потребует гораздо более детальных разработки требований и проектирования модели безопасности, но в рамках лабораторной работы остановимся на таком описании.

Перечень доступного пользователям программного обеспечения

Таблица 14

Пользователь	ПО
Alpha	FreeCommander, LibreOffice, Paint.Net, Mozilla Thunderbird. ICQ
Bettal, 2	FreeCommander, LibreOffice, Paint.Net. Mozilla Thunderbird
Epselonl, 2, 3	FreeCommander, LibreOffice, Paint.Net
Omega	FreeCommander, LibreOffice, Paint.Net

Переходим к этапу 2. Построение модели данных по умолчанию. В меню «Пуск» в группе СЗИ выберите пункт «Контроль программ и данных». Перед вами появится главное окно программы и окно настройки по умолчанию, представленные на рисунке 127. В последующем будет возможно создать модель заново. Для этого достаточно выбрать в меню «Файл» пункт «Новая модель данных».

Подтвердите предложенные параметры и дождитесь окончания настройки. Сохраните произведённые настройки («Файл — Сохранить» или кнопка с изображением «Дискеты» на панели инструментов). Вы произвели минимальную необходимую настройку механизмов замкнутой программной среды и контроля целостности.

На момент формирования модели на компьютере уже должны быть установлены необходимые программы. Для их добавления в ЗПС можно при создании модели данных выбрать пункт «Добавить другие задачи из списка» и указать соответствующие задачи (см. рис. 128).

Создайте новую модель данных, включив опцию «Предварительная очистка данных». И включите в создаваемую модель все программы, к которым у пользователей должен быть доступ кроме *Paint.Net.*

Рис. 127. **Главное окно программы «Контроль программ и данных» и окно настройки контроля по умолчанию**

Выбор дополнительных задач для ЗПС

Список доступных задач:

Pivot Animator - Pivot Animator

Pivot Animator - Uninstall Pivot

Secret Net - Журналы

Secret Net - Контроль программ и данных

Secret Net - Локальная политика безопасности

Secret Net - Настройка подсистемы полномочного управления доступом

Secret Net - Справка

Secret Net - Управление компьютером

Total Commander - SamLab.ws - New Soft

Total Commander - Total Commander Rus Total Commander - Информация о версии

Total Commander - Информация о сборке Total Commander - Настройка командера Total Commander - Открытие паролей ftp Total Commander - Справка к программе I Total Commander - Удаление командера

WinRAR - WinRAR

OK Отмена

Рис. 128. Окно «Выбор дополнительных задач для ЗПС»

Этап 3. В существующую модель данных можно добавлять элементы без её пересоздания. Установите *Paint.Net,* если этот программный продукт ещё не был установлен. Для его добавления, то есть добавления

соответствующей задачи в ЗПС, нужно запустить генератор задач: «Сервис — Генератор задач». При этом откроется окно, представленное на рисунке 129.

Генератор задач по установленным программам

Выберите программы для создания новых задач:

? Выделить все

Поиск по: ярлыкам из меню "Пуск" (ЗПС)

Полезные утилиты - Записывание CD&DVD Полезные утилиты - Извлечение флешки Полезные утилиты - Копия плохих файлов Полезные утилиты - Показ звезд-паролей Полезные утилиты - Проигрыватель аудио Полезные утилиты - Раздел автозагрузки Полезные утилиты - Раздел деинсталляции Полезные утилиты - Чистка жестких дисков Полезные утилиты - Чистка реестра системы Программы - Paint.NET Программы - Pidgin Развлечения - Громкость Развлечения - Звукозапись Связь - HyperTerminal

Связь - Мастер беспроводной сети Связь - Мастер настройки сети Связь - Мастер новых подключений

Дополнительно:

Р Игнорировать объекты р

Менять пути на переменные

Р Добавля7

Г*/ Помечать выполняемые (для ЗПС) Расширения выполняемых:

1Ы6 мс

I .exe; .dll; .epi; .drv; ,sys; .ocx; .vbs; .scr; .

ОК

Отмена

Рис. 129. Окно «Генератор задач по установленным программам»

Информацию об установленных программах генератор может брать из ярлыков меню «Пуск», как это показано на рисунке 129, или по данным MS Installer. Эти списки могут различаться, например программа может быть не обнаружена в меню «Пуск», но будет присутствовать в списке MS Installer и наоборот.

Выберите необходимые программы в одном из списков, проверьте флажки «Помечать выполняемые ...» (эта опция сообщает программе генератору задач, что найденным файлам нужно присвоить отметку «выполняемый») и «Добавлять зависимые модули» (эта опция сообщает генератору задач, что нужно добавлять в задачу различные утилиты, библиотеки и другие файлы, которые используют выбранные программы). Запустите процесс создания задачи. Если в выбранном источнике вы нашли не все нужные программы, повторно запустите генератор и обратитесь к другому источнику.

Таким образом, мы добавили задачи, необходимые для корректной работы программ. Главное окно программы «Контроль программ и данных» примет вид, представленный на рисунке 130.

& Контроль программ и данных

Файл Правка Вид Paint.NET *3.5.11 Файлы Сервис Справка

Категории

Субъекты управления

Задания

Задачи

Группы ресурсов

Ресурсы

Структура X	Имя	Изменен	
X ?1	[5? Effects	13.03.2014	06:40:44
П Задачи 3 ? FT Операционная система MS Windows >]- ? Q Secret Net 6 3 ? FT Microsoft .NET Framework 3.0 Service P Э- ? Q Microsoft .NET Framework 3.5 SP1	(3 FileTypes	13.03.2014	06:40:44
	J) ICSharpCode.SharpZipt... Interop.WIA.dll	13.03.2014 13.03.2014	06:40:44 06:40:44
	fpkicense.txt	13.03.2014	06:40:44
	§3 PantDot Net. Native. x64	13.03.2014	06:40:44

	x64...		
3 ? F~~ Microsoft .NET Framework 2.0 Service P	<§9 PaintDot Net. Native. x86...	13.03.2014	06:40:44
E9- ? Q Microsoft .NET Framework 1.1	§3 PantDotNet.Base.dll	13.03.2014	06:40:44
S ? FT Total Commander • SamLab.ws • New Sc	PantDotNet.Base.pdb	13.03.2014	06:40:44
S- ? FT Total Commander - Total Commander Rc	PantOotNet.Core.dll	13.03.2014	06:40:44
3 ? FT Total Commander • Реформация о вере S- ? FT Total Commander - реформация о сбор	PantDotNet.Core.pdb	13.03.2014	06:40:44
	5-I PaintDotNet.Data.dll	13.03.2014	06:40:44
3 ? FT Total Commander - Настройка команде	Jpl PaintOotNet.Data.pdb	13.03.2014	06:40:44
3 *J* FT Total			

Commander - Открытие паролей 3 ? ? Total Commander ? Справка к програні 3 ? FT Total Commander - Удаление команде^ б *4* Q Paint.NET v3.5.11 v (Q Paint.NET v3.5.1l Файлы	PantDotNet.Effects.dll PaintDotNet.Effects.pdb	13.03.2014 13.03.2014	06:40:44 06:40:44
	«		
	Зависимости		
	% Ресурсы Группы ресурсов |F| Задачи Задания (gfc		
	Объект		
	(QPant.NET V3.5.U Файлы		
	QPant.NET v3.5. И		
* i_____>J			

000000 ИЗ 000002 [0000001 06:43:25

Готов

Рис. 130. Главное окно программы «Контроль программ и данных» после добавления новых задач

Но это ещё не всё: добавленные задачи не привязаны к компонентам модели более высоких уровней, то есть существуют сами по себе и не влияют на работу' механизмов защиты.

Обратите внимание, что на вкладках под списком ресурсов задачи можно посмотреть, с какими объектами более высокого уровня иерархии связан конкретный ресурс.

Этап 4. Добавление заданий. Теперь в базе данных СЗИ есть сведения о программе в виде ресурсов, объединённых в задачу. Но эта задача ни к чему пока не привязана и функционально бессмысленна. Существующую задачу или задачи нужно связать с заданием.

Для этого сначала создайте задание: перейдите в категорию «Задания» и выберите в меню «Задания — Создать задание». На экране появится диалог выбора типа задания, представленный на рисунке 131.

Рис. 131. **Диалог создания нового задания**

Поставьте отметку «Замкнутая программная среда...» и нажмите «ОК». Введите название и описание задания. Теперь созданное задание отображается в главном окне в дереве элементов слева и в него можно добавлять задачи.

Вызовите контекстное меню узла, соответствующего созданному заданию, и выберите пункт «Добавить задачигруппы — Существующие». В открывшемся списке выберите созданную вами задачу и добавьте её в задание (см. рис. 132).

Главное окно программы «Контроль программ и данных» должно принять вид, аналогичный представленному на рисунке 133. В задании появился подпункт — задача, но само задание ни к чему не привязано и помечено краснобелым кругом.

Добавление подчиненных объектов к выбранному

X

Выберите объекты для добавления:

Объект	Принадле... *
И JPaint.NET v35.11	...0.....J =
Microsoft .NET Framework 3.0 Service Pac...	1
L_i Microsoft NET Framework 3.5 SP1	1
L_] Microsoft NET Framework 2.0 Service Pac...	1
F' I Microsoft NET Framework 1.1	1
i.JJ Total Commander - SamLab.ws • New Soft	1
ГТ Total Commander - Total Commander Rus	1
О Total Commander ? Информация о версии	1
Г'~1 Total Commander - Информация о сборке	1

Г Выделить все

ОК Отмена

Рис. 132. **Окно «Добавление подчинённых объектов к выбранному»**

Рис. 133. **Главное окно программы «Контроль программ и данных», раздел «Задания»**

Этап 5. Теперь нужно связать задания с субъектами. Для начала добавьте в список субъектов группу *inside* и всех необходимых пользователей. Теперь через контекстное меню свяжите группу и задание, которое вы создали для *Paint.Net* (см. рис. 134).

Рис. 134. **Главное окно программы «Контроль программ и данных», раздел «Субъекты управления»**

Теперь механизм замкнутой программной среды сможет отслеживать запуск ресурсов, указанных в задании. Самостоятельно настройте замкнутую программную среду для остальных пользователей компьютера.

Повторим этапы 4-5 для механизма контроля целостности. Перейдите к списку заданий и создайте новое задание на контроль целостности. Дайте заданию имя и выставьте метод проверки «Существование» (см. рис. 135).

Подробная информация о различных методах контроля целостности представлена в таблице 15.

Важно отметить, что к разным ресурсам можно применять различные наборы методов контроля. Более подробная информация об этом представлена в таблице 16.

Таблица 15

Описание методов контроля целостности СЗИ «Secret Net»

Метод контроля	**Что проверяется**
Содержимое	Целостность содержимого ресурсов
Права доступа	Категории конфиденциальности и атрибуты доступа Windows (дескриптор безопасности), установленные для ресурсов
Атрибуты	Стандартные атрибуты, установленные для ресурсов
Существование	Наличие ресурсов по заданному пути

Типы ресурсов и применимые к ним методы КЦ

	Содержимое объекта	Атрибуты объекта	Права доступа	Существовани объекта
Значение реестра	да	нет	нет	да
Ключ реестра	да	нет	да	да
Файл	да	да	да	да
Каталог	нет	да	да	да

При необходимости, измените параметры регистрации событий. Затем перейдите на вкладку «Расписание». На этой вкладке задаётся расписание проведения проверки: по календарю и по событию (см. рис. 135).

Рис. 135. **Окно «Создание нового задания на КЦ»**

Есть два режима планирования: «Основной», связанный с загрузкой ОС (проверку лучше выполнять после входа в систему, чтобы не замедлять загрузку компьютера), и «Календарный план», связанный непосредственно со временем. Оба эти режима могут использоваться параллельно друг другу.

Включите основной режим работы так, как показано на рисунке 135 и настройте календарный режим по своему усмотрению. Сохраните созданное задание и свяжите его с задачей *PaintNet.*

Создайте самостоятельно ещё одно задание на контроль целостности программы *PaintNet* и выберите методом контроля «Содержимое».

Таким образом, вы разрешили запуск и работу в программе *Paint.Net,* а также защитили его от несанкционированных изменений. По крайней мере, СЗИ «Secret Net» будет за этим следить.

Теперь привяжите созданные задания к компьютеру. Обратите внимание, что задания на контроль целостности могут быть привязаны только к машине, в то время как задания замкнутой программной среды — и к компьютеру, и к группе или пользователю. Другими словами КЦ работает для машины и не важно, кто за ней сидит, а ЗПС может работать как с параметрами для всего компьютера, так и с параметрами для отдельных пользователей и групп.

Этап 6. Теперь, когда все задания созданы и привязаны к субъектам, выполните подготовку ресурсов для ЗПС («Сервис — Ресурсы ЗПС»), а также расчёт эталонов для объектов контроля целостности («Сервис — Эталоны — Расчёт»).

Следующим шагом будет включение действия ЗПС и КЦ. Но для работы некоторых пользователей, например администраторов, бывает целесообразно отключить механизм замкнутой программной среды. Для этого перейдите в «Локальную политику безопасности» — «Secret Net» — «Привилегии» и откройте значение параметра «Замкнутая программная среда: не действует» (см. рис. 136). При необходимости отредактируйте список пользователей, для которых не должен действовать механизм замкнутой программной среды.

Этап 7. Включение ЗПС. В списке субъектов управления в контекстном меню узла, соответствующего данному компьютеру выберите пункт «Свойства» (см. рис. 137).

Перейдите на вкладку «Режимы» и поставьте флажок «Режим ЗПС включён». При желании можете включить дополнительные опции — их значения описаны в таблице 17. Сохраните сделанные изменения.

Рис. 136. **Окно настройки параметра СЗИ «Secret Net» «Замкнутая программная среда: Не действует»**

Рис. 137. **Свойства субъекта управления**

Таблица 17

Параметры режима ЗПС в отношении субъекта управления

Параметр	Пояснение
Проверять целостность модулей перед запуском	При запуске программ, входящих в список разрешённых, проверяется их целостность
Проверять заголовки модулей перед запуском	В процессе контроля включается дополнительный механизм, повышающий надёжность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке
Контролировать исполняемые скрипты	Блокируется выполнение сценариев (скриптов), не входящих в перечень разрешённых для запуска и не зарегистрированных в базе данных системы Secret Net

Этап 8. Механизмы контроля целостности начинают работать на компьютере при появлении первого задания на КЦ, связанное с субъектом управления, в соответствии с заданными параметрами. В нашем случае первые проверки целостности произойдут при следующей загрузке ОС.

Этап 9. Правильность настроек можно проверить, запустив задание «вручную»: «Сервис — Запуск заданий». При этом откроется окно, представленное на рисунке 138. Выберите задание для проверки и нажмите «ОК». Если ошибок не обнаружено, вы увидите сообщение, представленное на рисунке 139.

Выполните проверку созданных вами заданий на ЗПС и КЦ. В случае обнаружения ошибок, установите их причину и отредактируйте параметры заданий, при выполнении которых произошли эти ошибки.

Запуск задания КЦ

X

Рис. 138. **Окно ручного запуска заданий на контроль целостности**

Рис. 139. **Окно результатов ручного выполнения задания**

СЗИ «Secret Net» также позволяет экспортировать и импортировать настройки КЦ и ЗПС в файл, а также восстановить модель из базы данных по средствам соответствующих пунктов меню «Файл».

Программа «Контроль программ и данных» имеет функцию создания отчётов: паспорта ПО и ресурсов компьютера, доступных через соответствующие пункты меню «Сервис — Отчёты — ...». Запустите создание отчёта о ПО имеющемся на компьютере. При этом появится окно,

представленное на рисунке 140. Введите в поля предложенной формы информацию о себе и продолжите создание отчёта.

Рис. 140. **Окно мастера создания отчёта «Паспорт ПО»**

Проверьте, информация обо всём ли существующем на компьютере программном обеспечении включена в отчёт? Сформируйте максимально полный отчёт о ресурсах и настройках рабочей станции. Обратите внимание на то, какие данные можно в него включить.

После завершения формирования отчёта о ресурсах и настройках примет вид, аналогичный представленному на рисунке 142. Просмотрите полученный отчёт. Проверьте, соответствует ли его структура и содержание пунктам, выбранным вами в окне «Отчёт — Ресурсы рабочей станции», представленном на рисунке 141.

Рис. 141. Окно настройки формирования отчёта о ресурсах и настройках рабочей станции fi re?26 - WordPad

Файл Правка Вид Вставка Формат Справка

ОЙЙ ей Й IS

Arial ? 14 ? Кириллический ? Ж *К* Ч $) ? [S] Я ЕЕ

7- ? • 1 и • 2 • ' • 3 • • • 4 • • • 5 • i • 6 • ' • 7 • > • 8 • • • 9 • <' • 10- • • 11 • • -12• • -13-i -14• д15* ' *16- • -17- ? •

Настройки подсистем

Параметр	**Значение**
Вход в систему: Запрет вторичного входа в систему	отключена

Вход в систему: Количество неудачных попыток аутентификации	не ограничено
Вход в систему: Максимальный период неактивности до блокировки экрана	10 минут
Вход в систему: Режим аутентификации пользователя	стандартная аутентификация
Вход в систему: Режим входа пользователя	смешанный
Журнал: Максимальный размер журнала системы защиты	2048 кВ
Журнал: Политика перезаписи событий	затирать по необходимости
Запрет использования сетевых интерфейсов	отключено
Затирание данных: Количество циклов затирания конфиденциальной информации	отключено
Контроль устройств: Режим работы	мягкий
Полномочное управление доступом: Гриф конфиденциальности для Microsoft Excel	задан

Полномочное управление доступом: Гриф конфиденциальности для Microsoft Word	задан
Полномочное управление доступом: Названия уровней конфиденциальности	Неконфиденциально, Конфиденциально, Строго конфиденциально
Полномочное управление доступом: Режим контроля печати конфиденциальных документов	отключен
Полномочное управление доступом: Режим работы	контроль потоков отключен
Разграничение доступа к устройствам: Режим работы	мягкий

Для вывода справки нажмите NUM

Рис. 142. Фрагмент отчёта о ресурсах и настройках рабочей станции

Настройка механизмов контроля потоков информации

Теперь можно включить механизмы контроля потоков информации. Для этого в меню «Пуск» в группе программ «Код безопасности» выберите пункт «Локальная политика безопасности». Откроется окно управления локальными параметрами безопасности, представленное на рисунке 143.

Рис. 143. **Окно «Локальные параметры безопасности»**

Выберите узел «Параметры Secret Net» в дереве элементов слева — здесь находится большое количество опций СЗИ. Перейдите в ветку «Настройки

подсистем» и выберите параметр «Полномочное управление доступом». Включите контроль потоков информации (см. рис. 144). Аналогичным образом включите контроль печати конфиденциальных документов (см. рис. 145).

Свойства: Полномочное управление доступом: Режим работы

Параметр

Полномочное управление доступом: Режим работы

контроль потоков отключен

• контроль потоков включен

?расширенньїйконтроль вывода инфорглаций

Параметр устанавливает режим работы для механизма полномочного * управления доступом: _

- "контроль потоков отключен" • доступ пользователей к конфиденциальным Файлам разграничивается на основе уровня допуска пользователей, контроль потоков конфиденциальной информации в системе не осуществляется;

Отмена Применить

Рис. 144. **Окно «Свойства: Полномочное управление доступом: Режим работы»**

Рис. 145. **Окно «Свойства: Полномочное управление доступом: Режим контроля печати конфиденциальных документов»**

В разных организациях названия уровней доступа (грифов) могут различаться. Поэтому СЗИ «Secret Net» предоставляет возможность настроить их названия. Для этого откройте свойства параметра «Полномочное управление доступом: Названия уровней конфиденциальности» (см. рис. 146).

Рис. 146. **Окно «Свойства: Полномочное управление доступом: Название уровней конфиденциальности»**

Задайте названия грифов секретности для отдела Centavra по своему усмотрению. Теперь при загрузке ОС будет отображаться сообщение с выбором уровня допуска сессии, соответственно настройкам названий этих уровней (см. рис. 147).

Secret Net 6		
?© 1985-2001 МЛрссофт	Microsoft' / J Windows! Professional	***Microsoft***

Выберите уровень конфиденциальности для текущего сеанса:

[a] ®

Г з

г SS

ок

Рис. 147. **Окно выбора уровня конфиденциальности при входе в систему**

Обратите внимание, что самый высокий уровень секретности сессии — не всегда хорошо. К примеру, при включённом механизме контроля потоков информации, невозможно удалить никакой файл или каталог в корзину, если текущая сессия имеет наивысший уровень допуска, но можно удалять мимо корзины (по умолчанию комбинация клавиш *«Shift + Del»).* Также, некоторые инструменты настройки «Secret Net» будут недоступны. Более подробная информация об ограничениях возможностей пользователей при различных условиях конфиденциальности сессии приведена в документации к СЗИ.

Перейдём к настройке режима полномочного разграничения доступом. Настройка осуществляется с помощью программы «Настройки подсистемы полномочного управления доступом», представленной на рисунке 148. Обратите внимание, что для её запуска ваша учётная запись должна иметь наивысший уровень допуска и права администратора, а изменения учётных записей вступают в силу только после перезагрузки системы.

Для первичной настройки или восстановления стандартных параметров, нужно выполнить автоматическую настройку в режиме «По умолчанию». Выполните первичную настройку подсистемы.

Теперь, можно более тонко настроить работу механизмов СЗИ. Для этого перейдите в ветку «Вручную» в дереве в левой части окна. В этой ветке расположены параметры, которые можно настраивать самостоятельно. Но, чтобы сделанные настройки вступили в силу, нужно выполнить автоматическую настройку с «Текущими значениями» параметров (см. рис. 148).

По умолчанию

Текущие значения

Сообщения

{•••? События Перенаправление

*•••• Печать

i Пользователи

л Программы Microsoft Office

- Dr.Web AutoCAD FineReader 10 Photoshop CS5.1

		x
Г"" Настройки подсистемы полномочного управления доступом		
	С	й

Автоматически

J Вручную

л Общие

Автоматическая настройка системы с использованием значений по умолчанию.

Текущие значения будут сброшены и будет проведена настройка печати, перенаправления, пользователей и программ в соответствии со значениями по умолчанию.

Выполнить

Автоматическая настройка системы с использованием текущих значений.

Для проведения настройки печати, перенаправления, пользователей и программ будут использованы текущие значения. При необходимости к текущим значениям можно добавить значения по умолчанию.

Q Добавить значения по умолчанию Выполнить

Закрыть Справка

Рис. 148. **Программа «Настройки подсистемы полномочного управления доступом**

Разберём некоторые из параметров, доступных в ветке ручной настройки. Узел «Сообщения» позволяет отключить вывод некоторых информационных сообщений. Узел «События» позволяет управлять записью в журнал СЗИ события доступа к файлам по их расширению.

Узел «Перенаправление». Механизм полномочного управления доступом и контроля печати выполняет проверку соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталога или файла). Однако в ряде приложений, например MS Word, происходят обращения к служебным файлам, которые хранятся в специальных каталогах этих программ. При этом отсутствуют возможности изменять категории конфиденциальности этих файлов в зависимости от уровня допуска пользователя. При использовании механизма полномочного управления доступом при включённом режиме контроля потоков такие особенности пользовательского ПО приводят к конфликтным ситуациям и невозможности корректной работы этих приложений.

Для решения данной проблемы в системе реализована функция перенаправления вывода общих служебных файлов. Функция действует при работе пользователя в конфиденциальной или строго конфиденциальной сессии. Чтобы обеспечить работу приложения в сессиях с различными

уровнями конфиденциальности, создаются отдельные каталоги по количеству уровней, в которые копируются общие служебные файлы и этим копиям назначаются соответствующие категории конфиденциальности. Если приложение в конфиденциальной сессии осуществляет попытку обращения к общему файлу, система перенаправляет это обращение к копии общего файла, находящейся в отдельном каталоге и имеющей подходящий гриф секретности. Результат настройки этого механизма — несколько папок временных фалов «temp», представлен на рисунке 149.

Рис. 149. **Несколько системных папок «temp» для разных сессий разных уровней**

При настройке параметров перенаправления вывода файлов формируется список путей к каталогам с общими файлами, для которых должны быть созданы дополнительные каталоги различной категории конфиденциальности. В этих каталогах будут храниться файлы, используемые в сессиях соответствующего уровня конфиденциальности. Например, для обслуживания обращений приложения MS Word русской версии в списке должна присутствовать запись <> (см. рис. 150). Добавьте аналогичное правило для MS PowerPoint.

Рис. 150. **Окно программы «Настройки подсистемы полномочного управления доступом», узел «Перенаправление»**

Узел «Пользователи». Для работы пользователя в режиме контроля потоков в конфиденциальной или строго конфиденциальной сессиях должна быть выполнена настройка параметров, относящихся к профилю этого пользователя. Настройка заключается в создании структуры каталогов перенаправления вывода файлов для временных каталогов пользователя и установке соответствующих категорий конфиденциальности для этих каталогов. Настройка выполняется для тех пользователей, от имени которых хотя бы раз был выполнен вход в систему на данном компьютере. То есть для тех, у кого создан системный профиль на данном компьютере.

Настройка всех профилей пользователей в необходимом объёме осуществляется при общей автоматической настройке. При добавлении в систему нового пользователя или при переименовании существующего необходимо выполнить настройку профиля этого пользователя самостоятельно. Запуск процесса настройки профилей можно выполнить вручную. Сделать это можно просто выполнив настройку с «Текущими значениями».

Стоит отметить, что настройку с «Текущими значениями» нужно выполнять при появлении в системе нового пользователя, программы или принтера, то есть нужно настроить работу системы с новыми объектами, в соответствии с действующими на данный момент настройками СЗИ.

Узел «Программы» содержит список программ, о которых системе «известно», что они требуют особой настройки параметров. Добавить программу в этот список самостоятельно нельзя, нужен специальный xml-файл, содержащий инструкции по настройке данной программы для СЗИ. Но программы можно удалять из этого списка, а также включать и выключать их автоматическое конфигурирование. Просмотреть параметры конкретной программы можно из дочерних узлов.

Теперь добавьте в систему принтер, для этого установите специальную программу класса виртуальный принтер или драйвер реального принтера. Зайдите в систему под учётной записью одного из пользователей, созданных вами. Теперь можно посмотреть на изменения в программе настройки: снова зайдите в систему под учётной записью администратора, откройте программу «Настройки подсистемы полномочного управления доступом» и просмотрите узлы «Пользователи» и «Печать» (см. рис. 151).

Рис. 151. **Окно «Настройки подсистемы полномочного управления доступом», узел «Печать»**

Обратите внимание, что настроить можно как параметры конкретного пользователя, так и все объекты, которые требуют перенастройки. Выполните автоматическую настройку системы в режиме «Текущих параметров». После завершения проверки снова зайдите и просмотрите узлы «Пользователи» и «Печать».

Режимы входа

Система почти настроена и готова к запуску, теперь нужно настроить параметры входа пользователей. Раньше делать это не целесообразно: по ходу настройки может понадобиться часто перезагружаться или заходить в систему под разными пользователями, а при усиленной идентификации и аутентификации эти действия могут заметно замедлить процесс настройки.

Откройте «Локальные политики безопасности», перейдите в ветку СЗИ «Secret Net» в раздел «Настройка подсистем» (см. рис. 152). В данном разделе есть параметры, влияющие на поведение системы при выполнении процедуры идентификации-аутентификации. Рассмотрим смысл некоторых из этих параметров.

В" Локальные параметры безопасности

Консоль Действие Вид Справка

Параметры безопасности

I Политики учетных запис |_9 Локальные политики Р1 Политики открытого клг ГЛ Политики ограниченногс Политики безопасностиI л О Параметры Secret Net г Настройки подсистег Ключи пользователя Привилегии Регистрация событий ⋮ Устройства

Политика Параметр безопасности

ЭД Вход в систему: Запрет вторичного входа в систему отключена

[ЭДВход в систему: Количество неудачных попыток аутентификации не ограничено

ЭДВход в систему: Максимальный период неактивности до блокировки экрана 1Р. МИНУТ ЭДВход в систему: Режим аутентификации пользователя [ЭДвход в систему: Режим входа пользователя

стандартная аутентифи... смешанный

2048 кБ

затирать по необходимо...

отключено

отключено

отключено

отключено

мягкий

задан

задан

Неконфиденциалык^ Ко...

отключен

контроль потоков откл... мягкий

[ЭД Журна л: Максимальный размер журнала системы защиты [ЭДЖурнал: Политика перезаписи событий ^Запрет использования сетевых интерфейсов

[ЭД Затирание данных: Количество циклов затирания конфиденциальной информации ЭДЗатирание данных: Количество циклов затирания на локальных дисках ЭДЗатирание данных: Количество циклов затирания на сменных носителях [ЭД Контроль устройств: Режим работы ^Полномочное управление доступом: Гриф конфиденциальности для Microsoft Excel [ЭД Полномочное управление доступом: Гриф конфиденциальности для Microsoft

Word [ЭД Полномочное управление доступом: Названия уровней конфиденциальности [ЭД Полномочное управление доступом: Режим контроля печати конфиденциальных... ЭДПолномочное управление доступом: Режим работы ЭДРазграничение доступа к устройствам: Режим работы

Рис. 152. Окно «Локальные политики безопасности», ветка «Параметры Secret Net», раздел «Настройки подсистем»

Вход в систему: Запрет вторичного входа в систему — Если режим включён, блокируется возможность запуска команд и сетевых подключений с вводом учётных данных пользователя, который не выполнил интерактивный вход в систему. Для компьютеров под управлением ОС Windows XP и выше после включения режима дополнительно рекомендуется исключить возможность использования ранее сохранённых учётных данных. Для этого раскройте узел «Локальные политики — Параметры безопасности» и включите действие стандартного параметра безопасности ОС Windows «Сетевой доступ: не разрешать хранение паролей или учётных данных для сетевой проверки подлинности».

Вход в систему: Количество неудачных попыток аутентификации — устанавливает ограничение на количество неудачных попыток аутентификации пользователя по ключевой информации при входе в систему. При достижении ограничения компьютер блокируется и вход разрешается только для администратора. Если параметру присвоено значение «О», ограничение не действует.

Вход в систему: Максимальный период нсактивности до блокировки экрана — устанавливает максимальное значение интервала неактивности. Автоматическая блокировка компьютера, включаемая в том случае, если в течение определённого времени не использовались клавиатура и мышь, настраивается каждым пользователем индивидуально. Но пользователь не сможет установить интервал неактивности, превышающий значение, заданное данным параметром.

Вход в систему: Разрешить интерактивный вход только доменным пользователям — если режим включён, интерактивно в систему могут войти только пользователи, зарегистрированные в домене. Интерактивный вход в

систему локальных пользователей, включая локальных администраторов, запрещён.

Вход в систему: Режим аутентификации пользователя — *«Стандартная аутентификация»* выполняется по паролю пользователя. *«Усиленная аутентификация по ключу»* кроме пароля проверяется подлинность и актуальность (срок действия) ключевой информации пользователя. Для загрузки ключевой информации пользователь должен предъявить идентификатор. Вход в систему разрешается при подтверждении подлинности и актуальности ключа. Если подлинность ключа не подтверждается, вход запрещается и регистрируется значение ключа (если включён параметр «Регистрировать неверный ключ»). Если срок действия ключа истёк, пользователю предлагается выполнить смену ключей для усиленной аутентификации. При включённом режиме усиленной аутентификации вход в систему без предъявления ключа возможен только в административном режиме в обход механизмов СЗИ. Для этого нужно нажимать или удерживать ESC во время отображения сообщения о загрузке служб и модулей СЗИ при включении компьютера, предваряющего окно с запросом нажатия комбинации Ctrl+Alt+Del.

Вход в систему: Режим входа пользователя — *«Стандартный»* для входа в систему пользователь должен ввести свои учётные данные, используя только стандартные средства ОС Windows. *«Смешанный»* для входа в систему пользователь может предъявить идентификатор, активированный средствами СЗИ «Secret Net», или ввести свои учётные данные, используя стандартные средства ОС Windows. *«Только по идентификатору»* для входа в систему пользователь должен предъявить идентификатор, активированный средствами СЗИ. Пользователи, не имеющие персонального идентификатора, войти в систему не смогут.

Настройте и проверьте защиту входа в систему со своими или с предложенными значениями параметров:

1) запрет вторичного входа в систему включён;

2) максимальное количество неудачных попыток аутентификации — 5;

3) максимальный период неактивности — 5 минут;

4) аутентификация по ключу с регистрацией неверного ключа;

5) вход только по ключу.

Удаление

Удаление СЗИ «Secret Net» происходит так же, как и удаление любой другой программы на компьютере под управлением ОС Windows: «Панель управления — Установка и удаление программ — Secret Net» (см. рис. 153). Выберите в списке пункт «Secret Net» и нажмите кнопку «Изменить» — откроется знакомое вам окно мастера установки, представленное на рисунке 154.

***•' Установка и удаление программ**

5	**Установленью прогревы: Q Покатать обновленн**	**ісртировка: имя**	**-**
Изменение или			*****
удаление	**i rtcrosoft -NET Framework3.0 Service Pack 2**	**Размер**	**169,00МБ**
программ			
	jgJ hterosoft .NET Framework 3.5 SP1	**Размер**	**28,03МБ**
	? kfcrosoft Visual C++ 2008 PedisfrtutaWe ? x86 9.0.30729.17	**Размер**	**10,28МБ**

установка	**i M5XML 4.0 5P2 (KB954430)**	**Размер**	**2,67МБ**
программ			
	v* Oracle VM VirtualBox Guest Additions 4.3.6	**Размер**	**4,06МБ**
0^|	**§ Paint.NET V3.5.11**	**Размер**	**14,63МБ**
Установка	**? Pivot Animator version 4.1.10**	**Размер**	**2,46МБ**
компонентов			
Windows	**? Priovl.9.7**		
	Radmin Viewer 3.5	**Размер**	**8,46МБ**
	Secret Net 6	**Размер**	77.93МБ _
Вы5ор	Чтобы полудіть сведения о поддержке, щелкните здесь.	**Используется**	редко
программ			

по умолчанио	**Чтобы изменить эту программу, щелкните "Изменить".**		**Изменить**
	У Total Commander 7.04 PowerPack	**Размер**	**28,59МБ**
	A, Unlocker 1.8.7	**Размер**	**0,20МБ**
	XL **VistaDrive 3.1**	**Размер**	**1,07МБ**
	У} Архиватор VrtnRAR (только удаление)	**Размер**	**3,65МБ L**
	-0 Дополіяітельньїе апплеты	**Размер**	**14,37МБ**

Рис. 153. **Окно «Установка и удаление программ»**

Рис. 154. **Окно мастера установки СЗИ «Secret Net», шаг 1**

Выполните удаление СЗИ — по завершении процесса мастер сообщит о результатах удаления (см. рис. 155). Перезагрузите компьютер. Отметьте, какие изменения произошли в процессе загрузки и работы ОС после удаления СЗИ «Secret Net».

Рис. 155. **Окно мастера установки СЗИ «Secret Net», результат работы мастера**

Вопросы

1. Каков главный принцип обеспечения информационной безопасности?
2. Что такое СЗИ?
3. Каковы основные подсистемы СЗИ «Secret Net»?
4. Какие функции защиты информации выполняет СЗИ «Secret Net»?
5. Как связаны между собой гриф секретности и уровень допуска?
6. Какова роль журнализации?
7. Что такое «замкнутая программная среда»?
8. Для чего нужна ЗПС?
9. Что собой представляет механизм контроля потоков информации?
10. Что такое контроль целостности?

11. Есть ли связь между механизмом КЦ и ЗПС? Если есть, то какая? Если связи нет, то почему?

12. Есть ли необходимость в антивирусном программном обеспечении на компьютере, на котором действует ЗПС в жёстком режиме? Почему?

13. Что такое «персональный идентификатор»?

14. Какую роль играет персональный идентификатор в обеспечении информационной безопасности?

15. Каковы достоинства и недостатки использования персональных идентификаторов?

16. Каковы основные сходства СЗИ «Secret Net» и СЗИ «Страж NT»?

17. Какие различия существуют между ними?

ЛАБОРАТОРНАЯ РАБОТА № 7