Министерство образования и науки РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

А.А. Конев, А.Ю. Якимук

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

(Часть 2)

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность
телекоммуникационных систем»,
10.05.03 – «Информационная безопасность
автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

В-Спектр
Томск, 2017

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1

АУТЕНТИФИКАЦИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ ПРИ ПОМОЩИ ФИЗИЧЕСКОГО ОБЪЕКТА

В лабораторной работе рассмотрены утилиты и приложения, позволяющие производить аутентификацию в операционной системе (ОС) при помощи физического объекта – eToken. При этом пароль для входа в операционную систему хранится на физическом объекте, а для доступа к нему используется PIN-код на eToken. Для подключения eToken к компьютеру используется USB-порт.

Рассматриваемые утилиты и приложения:

– утилита управления eToken – позволяет устанавливать качество PIN-кода к нему;

– eToken Network Logon – позволяет использовать eToken для хранения аутентификационных данных для входа в ОС.

Ход работы

1. Базовые действия с eToken

Запустите виртуальную ОС и войдите под учётной записью «Администратор». Подключите eToken к USB-порту. Запустите утилиту «eToken Properties»: «Пуск – Программы – eToken – eToken Properties» (или через значок «eToken PKI Client» на панели уведомлений). Вид основного окна представлен на рис. 1.

Рисунок 1 – Вид основного окна утилиты «eToken Properties»

Смените PIN-код. Используемый по умолчанию PIN-код: «1234567890». При смене PIN-кода необходимо соблюдать требования, предъявляемые к его качеству. Достижение отметки 100% означает, что введённый PIN-код отвечает установленным требованиям (рис. 2).

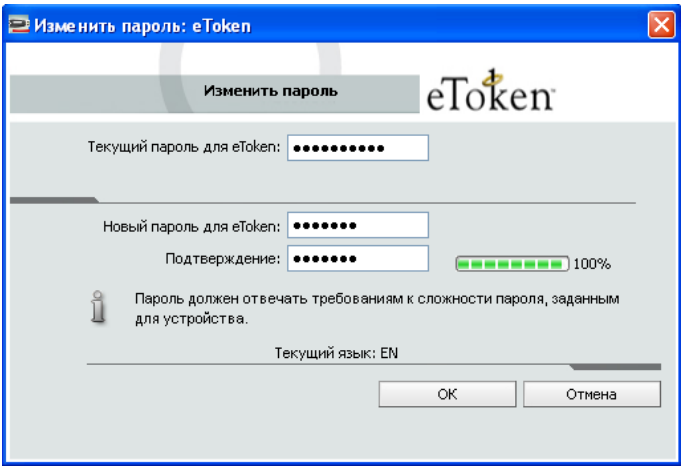

Рисунок 2 – Смена PIN-кода

Переименуйте eToken (рис. 3). Для возможности простого определения принадлежности eToken необходимо присвоить ему уникальный в системе идентификатор пользователя (login), которому выдаётся eToken. При первой операции с eToken необходимо ввести PIN-код.

Измените режим интерфейса на «Подробный вид» (значок на панели инструментов). В данном режиме предоставляется доступ к дополнительным настройкам и функциям по работе с подключенными eToken (рис. 4). В основном окне режима «Подробный вид» предоставляется информация о выбранном eToken.

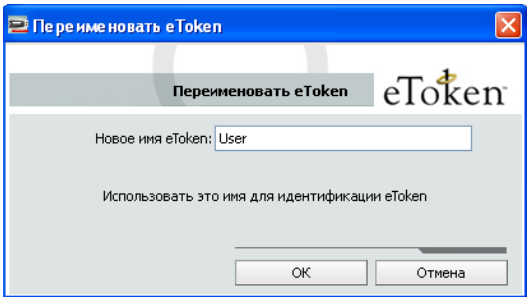

Рисунок 3 – Переименование eToken

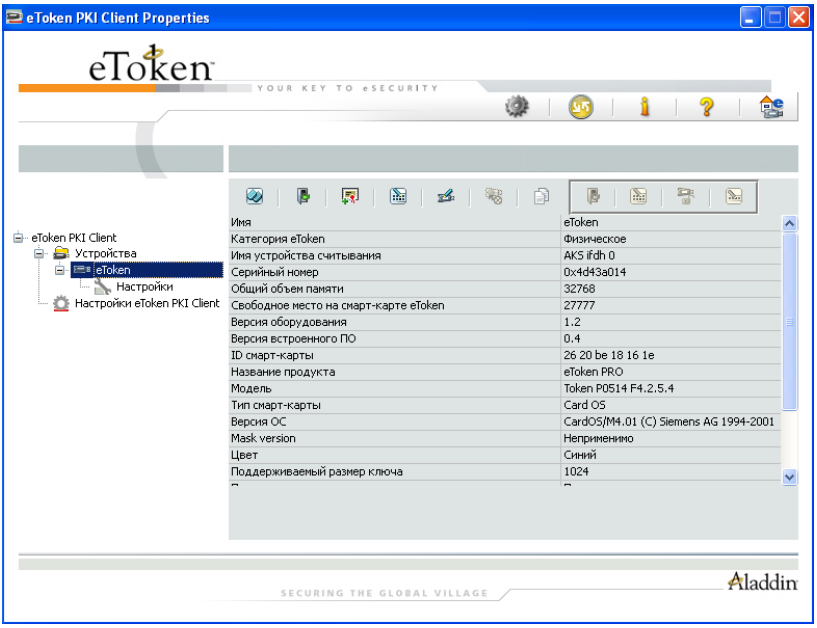

Рисунок 4 – Вид основного окна для eToken в режиме «Подробный вид»

2. Установка требований к качеству PIN-кода eToken

В разделе «Настройки eToken PKI Client» возможна установка требований к качеству PIN-кода eToken, которые будут записаны на него при форматировании (рис. 5). Просмотр требований, сохранённых на eToken, возможен в разделе «Настройки» выбранного eToken.

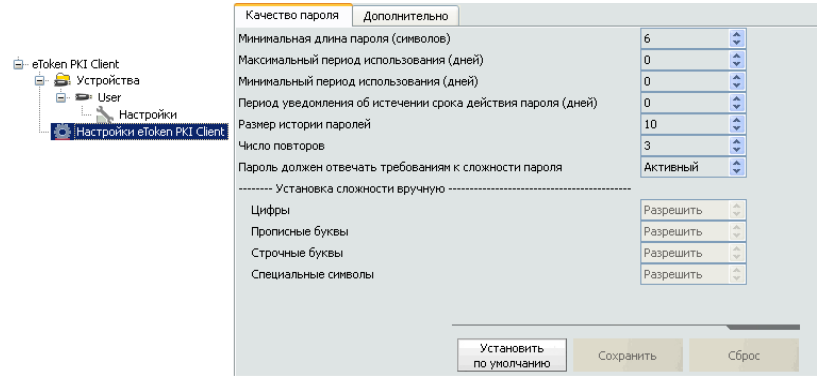

Рисунок 5 – Настройка параметров качества PIN-кода eToken

3. Администрирование eToken

В режиме «Подробный вид» выберите подключенный eToken и на панели инструментов выберите «Инициализировать eToken». В окне «Параметры инициализации eToken» (рис. 6) установите PIN-код eToken или требование к обязательной смене пароля при первом использовании (если оставите PIN-код по умолчанию), а также PIN-код администратора eToken. Также можно установить максимальное количество ошибок ввода соответствующих PIN-кодов и имя eToken. Отформатируйте eToken. **Внимание!** При форматировании есть возможность указать ключ форматирования («Дополнительно» – «Изменить ключ инициализации»). **Не изменяйте** настройки этой вкладки, так как при незнании ключа форматирования нельзя восстановить его в первоначальном состоянии, что приводит к неработоспособности eToken.

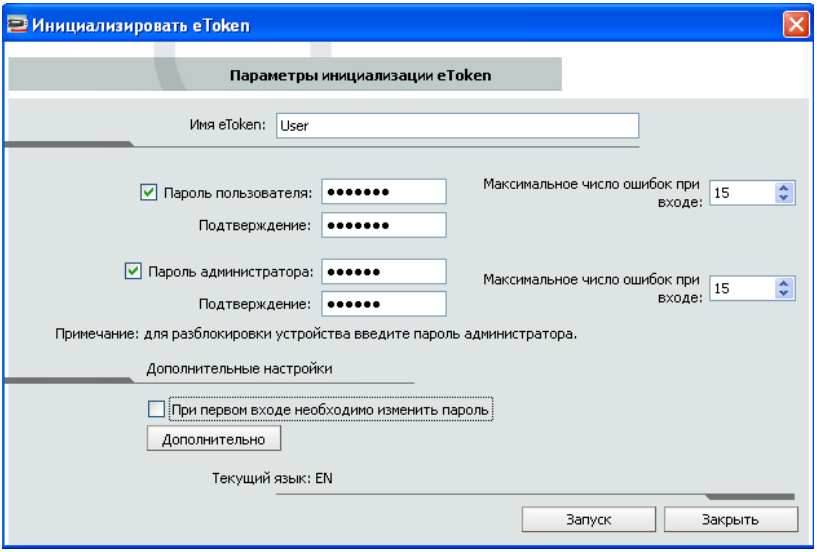

Рисунок 6 – Параметры инициализации eToken

Выберите подключенный eToken. На панели инструментов выберите значок «Вход с правами администратора». Введите PIN-код администратора (рис. 7). Администратору предоставляются дополнительные функции. На панели инструментов выберите значок «Установить пароль пользователя». Эта функция позволяет

администратору задать новый PIN-код eToken, если пользователь забыл свой текущий PIN-код.

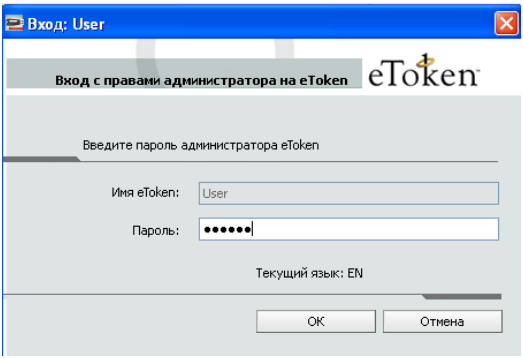

Рисунок 7 – Ввод пароля администратора

Настройки интерфейса утилиты «Свойства eToken» можно изменять через «Групповые политики», используя соответствующий административный шаблон. Откройте оснастку gpedit.msc и добавьте административный шаблон eTokenPKIClient.adm (расположен на «Рабочем столе»). В появившемся разделе «eToken PKI Client Settings» можно разрешать или запрещать доступ к любой настройке рассматриваемой утилиты. Например, запретите доступ к режиму «Подробный вид» (значение 0 настройки «OpenAdvancedView» параметра «Access Control» раздела «UI Access Control List», рис. 8). Для проверки внесённых изменений перезапустите утилиту «Свойства eToken».

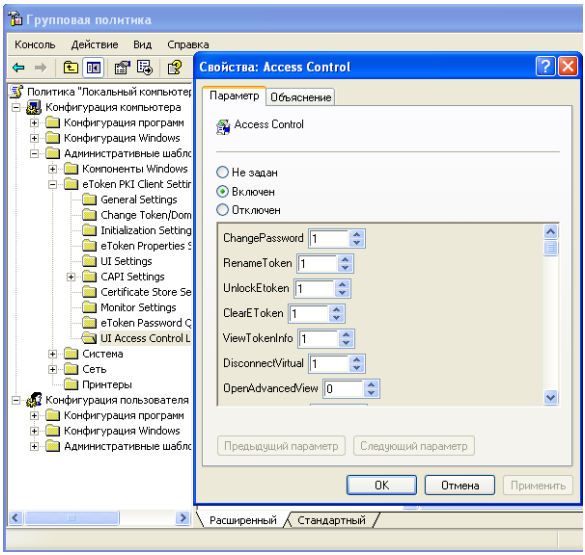

Рисунок 8 – Запрет доступа к режиму «Дополнительно»

4. Аутентификация в ОС при помощи eToken

Запустите утилиту для создания профиля входа в операционную систему: «Пуск – Программы – eToken – eToken Network Logon – eToken Network Logon Profile Wizard». Нажмите «Далее». Введите логин пользователя (например, «User») и название рабочей станции (либо домена), для которых создаётся профиль (рис. 9). Нажмите «Далее».

Рисунок 9 – Ввод информации пользователя для входа в ОС

Введите и подтвердите пароль для входа в ОС, принадлежащий выбранному пользователю (рис. 10). Дважды нажмите «Далее». Введите PIN-код eToken для подтверждения записи на него созданного профиля.

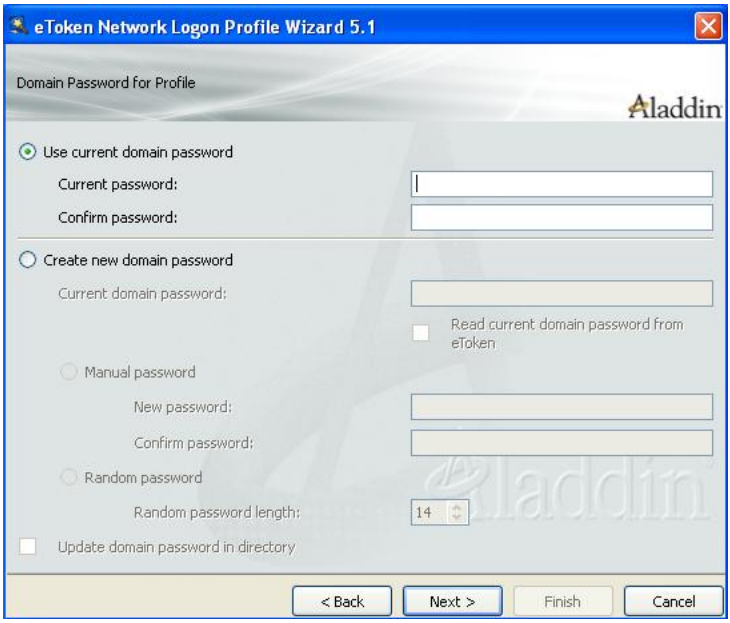

Рисунок 10 – Ввод пароля для входа в ОС

Завершите текущий сеанс пользователя и отключите eToken. При появлении «окна приветствия» Windows подключите eToken. Появится окно, изображённое на рис. 11. Введите PIN-код eToken и нажмите кнопку «OK». С eToken будет считана необходимая аутентификационная информация и произведён вход в ОС. После входа в ОС отключите eToken – в этом случае сеанс пользователя блокируется. Подключите eToken и разблокируйте сеанс.

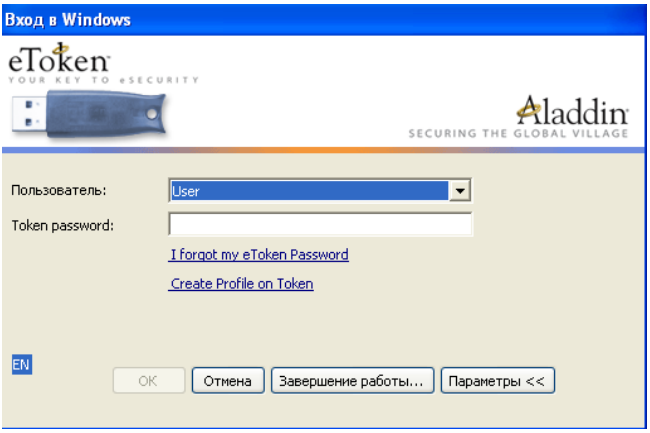

Рисунок 11 – Двухфакторная аутентификация при помощи eToken

Сменить пароль для входа в ОС можно, используя встроенные в ОС средства. Нажмите Ctrl-Alt-Del и выберите «Смена пароля…». В появившемся окне (рис. 12), кроме нового пароля и его подтверждения необходимо ввести PIN-код eToken для записи на него нового пароля.

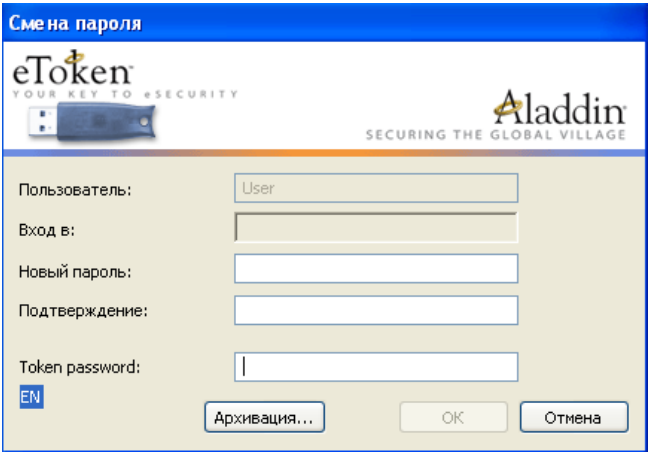

Рисунок 12 – Смена пароля для входа в ОС

Сменить пароль также можно при помощи утилиты «eToken Network Logon Profile Wizard». В окне (рис. 13) выберите существующий на eToken профиль. В окне (рис. 14) выберите создание нового пароля и включите параметр обновления пароля в хранилище ОС («Update domain password in directory»). Введите текущий и новый пароли. Если текущий пароль уже есть на eToken, то включите

параметр «Read current domain password from eToken» и утилита автоматически считает его из существующего профиля.

Рисунок 13 – Выбор существующего на eToken профиля

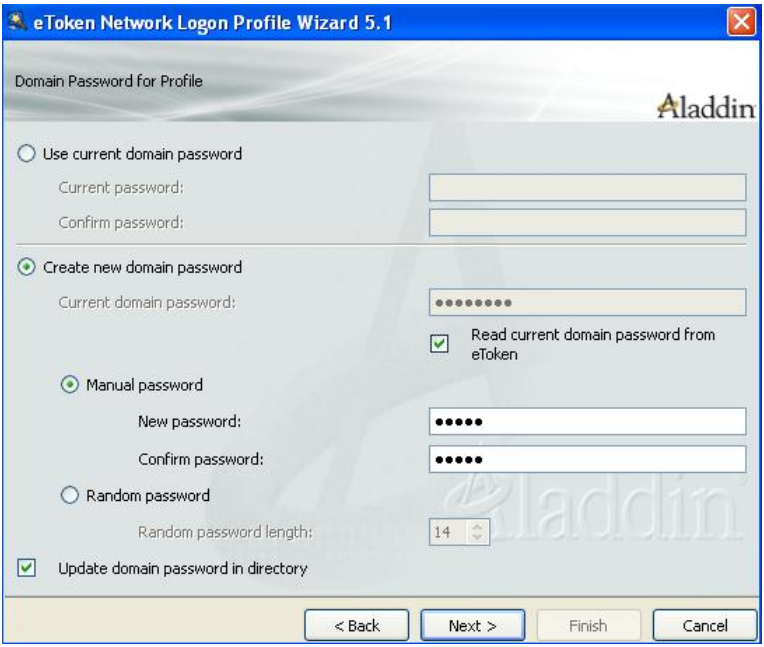

Рисунок 14 – Смена пароля для входа в ОС

Для удаления существующего на eToken профиля нужно в окне (рис.15) выбрать «Remove an existing profile». Удалите существующий профиль.

Рисунок 15 – Выбор двухфакторной аутентификации

5. Аутентификация в ОС на основе случайного пароля

Создайте новый профиль для входа в ОС, выбрав задание случайного пароля определённой длины (рис. 16). Тогда пароль для входа в ОС будет храниться только на eToken, иметь высокую сложность, не будет известен пользователю, уменьшая возможность подбора или разглашения пароля. После создания профиля завершите сеанс пользователя. Отключите eToken. При попытке стандартного входа в ОС (через Ctrl-Alt-Del) старый пароль пользователя будет отклонён, т.к. произошла смена пароля на случайный с заданной длиной. Войдите в ОС с использованием eToken.

Рисунок 16 – Задание случайного пароля для входа в ОС

Сменить случайный пароль для входа в ОС пользователь может, выбрав «Смена пароля…» при нажатии Ctrl-Alt-Del (рис. 17). В этом

случае достаточно ввести PIN-код eToken, а новый пароль для входа в ОС будет сгенерирован случайным образом. Длина случайного пароля будет задана в соответствии с настройками.

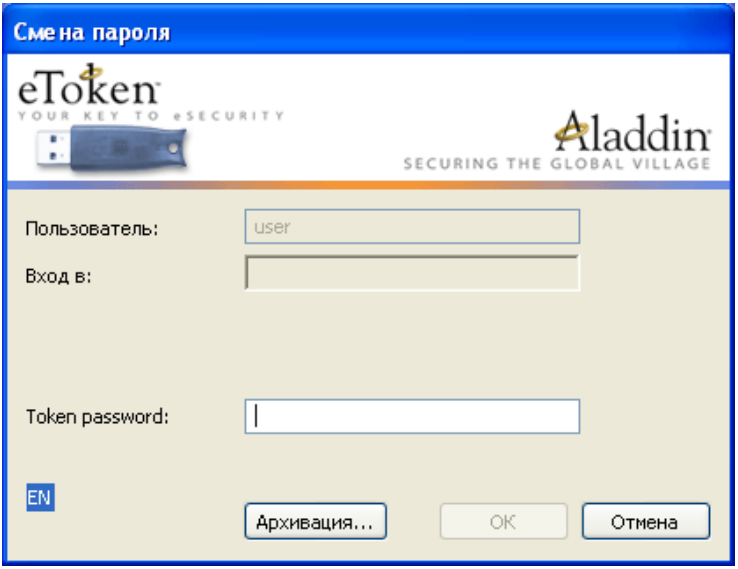

Рисунок 17 – Смена случайно заданного пароля для входа в ОС

6. Администрирование eTokenNetworkLogon

Настройки рассматриваемой утилиты можно изменять через «Групповые политики», используя соответствующий административный шаблон. Под учётной записью «Администратор» откройте gpedit.msc, добавьте административный шаблон «C:\Program Files\Aladdin\eToken\eTNLogon\eTokenNetworkLogon.adm». В разделе «eTokenNetworkLogon» можно разрешать или запрещать доступ к любой настройке, а также включать и отключать функции рассматриваемой утилиты. Например, запретите стандартный вход в ОС через Ctrl-Alt-Del (значение 0 параметра «Allow Standard Windows Logon») – будет разрешён вход только с использованием eToken (рис. 18). Завершите сеанс пользователя. Попытайтесь воспользоваться стандартным методом входа в ОС.

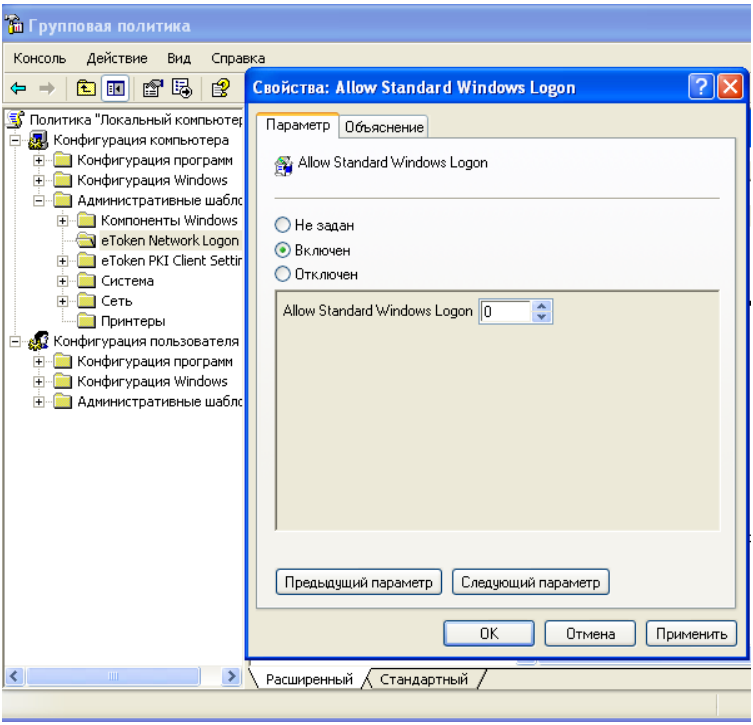

Рисунок 18 – Запрет стандартного входа в ОС

Для входа с правами администратора создайте для учётной записью «Администратор» новый профиль на eToken при помощи функции «Create profile on Token» (рис. 19).

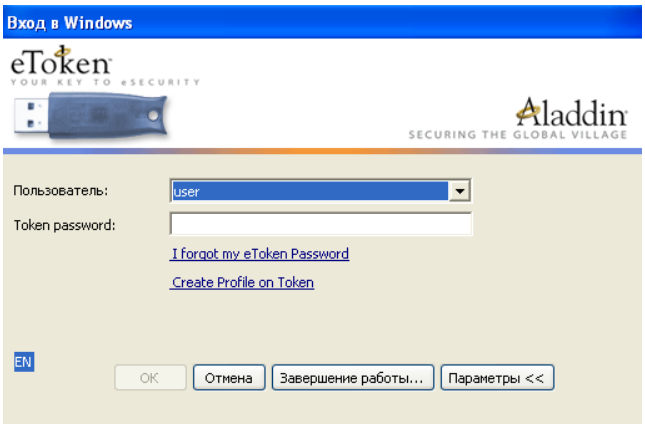

Рисунок 19 – Функции по работе с eToken, доступные до входа в ОС

Задание

1. Создайте пользователя с именем, совпадающим с Вашим именем в кафедральной сети.

2. Установите требования к качеству PIN-кода eToken в соответствии с Вашим вариантом (табл. 1).

3. Отформатируйте eToken, присвоив ему имя созданного пользователя и установив пароль, соответствующий требованиям п. 2.

4. Создайте профиль для входа в ОС созданного пользователя.

5. Продемонстрируйте преподавателю процедуру смены пароля для входа в ОС в соответствии с параметрами, указанными в Вашем варианте.

Таблица 1 – Варианты заданий

Вар.	Требования к качеству PIN-кода	Параметры входа в ОС
1	Мин. длина пароля – 8 символов. Макс. срок действия пароля – 30 дней.	Ввод нового пароля вручную. Ввод текущего пароля вручную.
2	Мин. длина пароля – 12 символов. Количество хранимых последних паролей – 5.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
3	Мин. длина пароля – 12 символов. Пароль должен содержать только буквы обоих регистров.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
4	Макс. срок действия пароля – 30 дней. Пароль должен содержать все типы символов.	Генерация случайного нового пароля длиной 10 символов. Ввод текущего пароля вручную.
5	Макс. срок действия пароля – 40 дней. Количество хранимых последних паролей – 8.	Генерация случайного нового пароля длиной 10 символов. Считывание текущего пароля с eToken.
6	Мин. длина пароля – 10 символов. Пароль должен содержать только буквы обоих регистров и числа.	Генерация случайного нового пароля длиной 10 символов. Ввод текущего пароля вручную.
7	Мин. длина пароля – 12 символов. Пароль может содержать все типы символов.	Генерация случайного нового пароля длиной 15 символов. Ввод текущего пароля вручную.

8	Макс. срок действия пароля – 30 дней. За сколько дней пользователь должен быть предупреждён о смене пароля – 3 дня.	Генерация случайного нового пароля длиной 15 символов. Считывание текущего пароля с eToken.
9	Количество хранимых последних паролей – 7. Пароль должен содержать только буквы обоих регистров и числа.	Изменение пароля через Ctrl-Alt-Del.
10	Количество хранимых последних паролей – 9. Пароль должен содержать все типы символов.	Изменение случайно заданного пароля через Ctrl-Alt-Del.

Контрольные вопросы

1. Какой PIN-код для eToken используется по умолчанию?
2. Каким образом можно узнать размер свободной памяти на eToken?
3. Какие дополнительные возможности предоставляются администратору eToken?
4. Какие можно установить требования к качеству PIN-кода eToken?
5. Где хранятся требования к качеству PIN-кода eToken, используемые при смене этого PIN-кода?
6. Опишите отличия двухфакторной аутентификации при использовании eToken от однофакторной.
7. Что включает профиль входа в операционную систему, создаваемый приложением eToken Network Logon?
8. С использованием каких способов может происходить смена пользователем пароля на вход в операционную систему?
9. Каким образом происходит смена пользователем случайно установленного пароля для входа в операционную систему?
10. Каким образом настраивается доступность для пользователя различных функций eToken Properties и eToken Network Logon?

ЛАБОРАТОРНАЯ РАБОТА №2

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ НА ОСНОВЕ ТЕХНОЛОГИИ SSO

В данной лабораторной работе рассмотрены утилиты, позволяющие производить аутентификацию в прикладных приложениях и на web-сайтах при помощи физического объекта – eToken. Рассматриваемые утилиты:

– eToken SSO Template Editor – позволяет создавать шаблоны окон различных приложений и web-сайтов, в которые могут входить поля для ввода аутентификационных данных (устанавливается только на компьютере администратора);

– eToken SSO Client – позволяет использовать eToken для хранения аутентификационных данных различных приложений и вносить эти данные в соответствующие окна приложения (устанавливается на каждую рабочую станцию).

Ход работы

1. Создание шаблона аутентификационного окна приложения

Запустите утилиту управления шаблонами ввода данных для приложений и web-сайтов: «Пуск – Программы – eToken – eToken SSO – Template Editor». Создайте шаблон для формирования при помощи приложения «7-Zip» архива, защищённого паролем. В контекстном меню произвольного файла выберите «7-Zip»-«Добавить к архиву».

Для создания шаблона на нижней панели окна утилиты нажмите «New» (рис. 1).

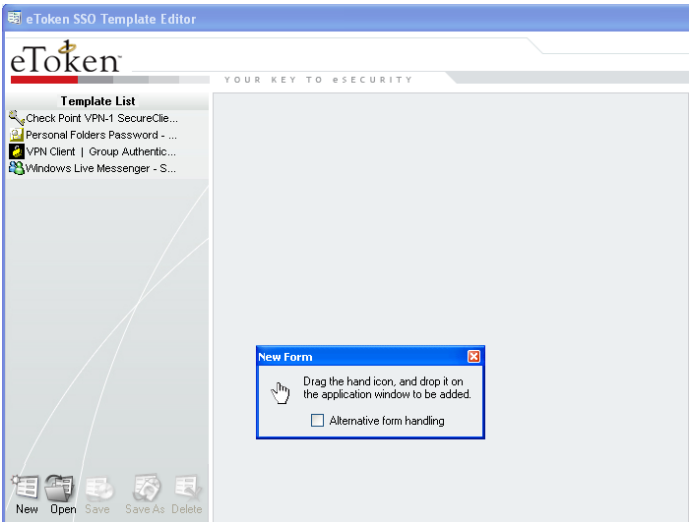

Рисунок 1 – Основное окно утилиты «eToken SSO Template Editor»

После чего перетащите изображённую ладонь на окно «7-Zip» (рис. 2). При этом для редактирования становится доступен шаблон (рис. 3).

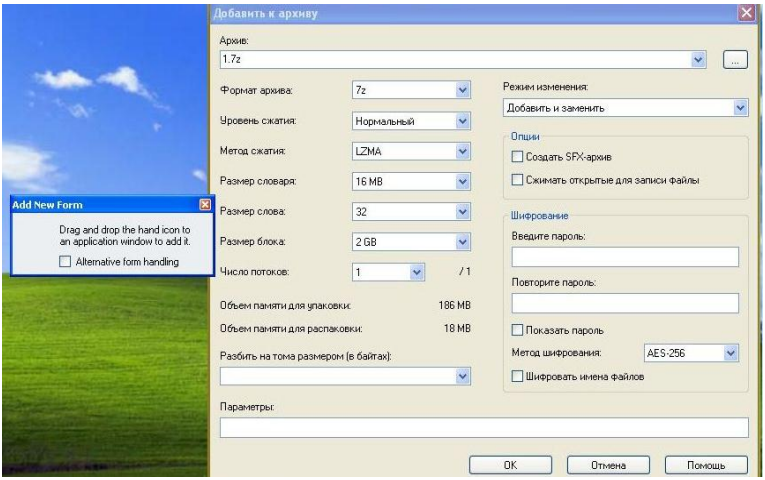

Рисунок 2 – Выбор окна для создания шаблона

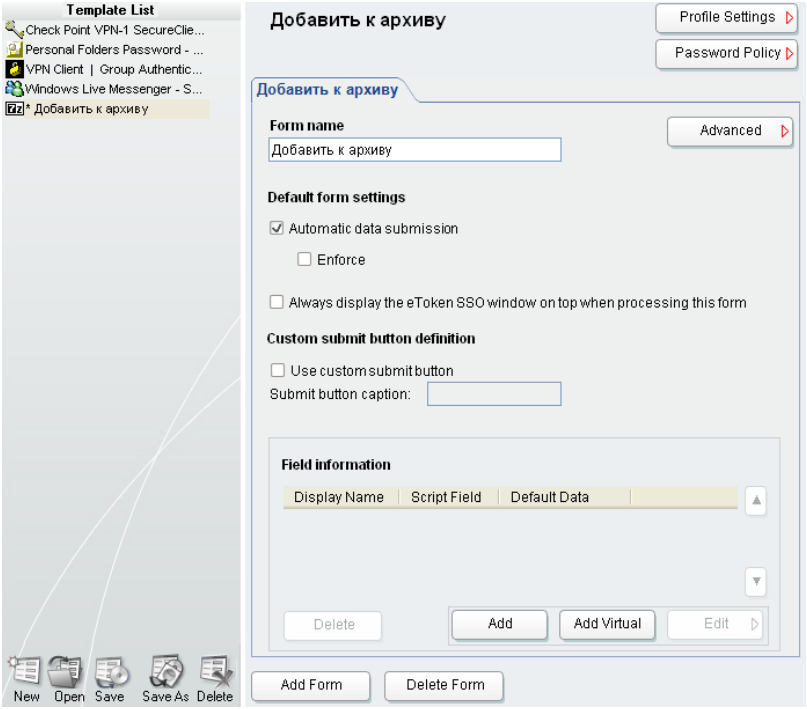

Рисунок 3 – Настройки шаблона для выбранного окна приложения

Поля для ввода данных, содержащиеся в окне, добавляются нажатием кнопки «Add» и перетаскиванием появившейся ладони. Добавьте поля: «Введите пароль» (рис.4) и «Повторите пароль».

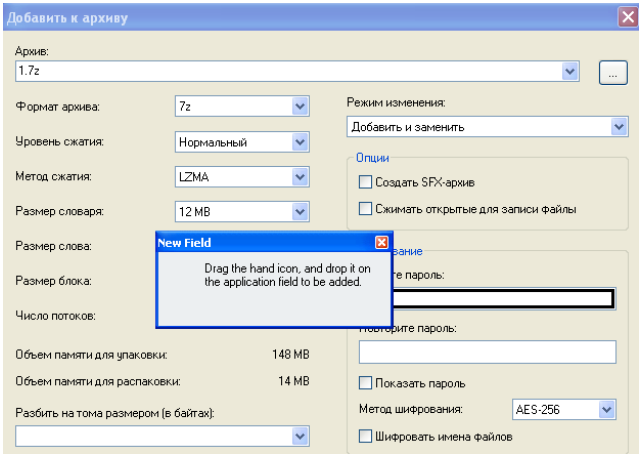

Рисунок 4 – Выбор поля «Введите пароль»

При этом для поля «Повторите пароль» поменяйте «роль» поля с «General» на «Password» (рис. 5), что позволит отображать вводимые в поле символы в виде звёздочек (отобразить данные настройки можно, нажав кнопку «Edit» для соответствующего поля).

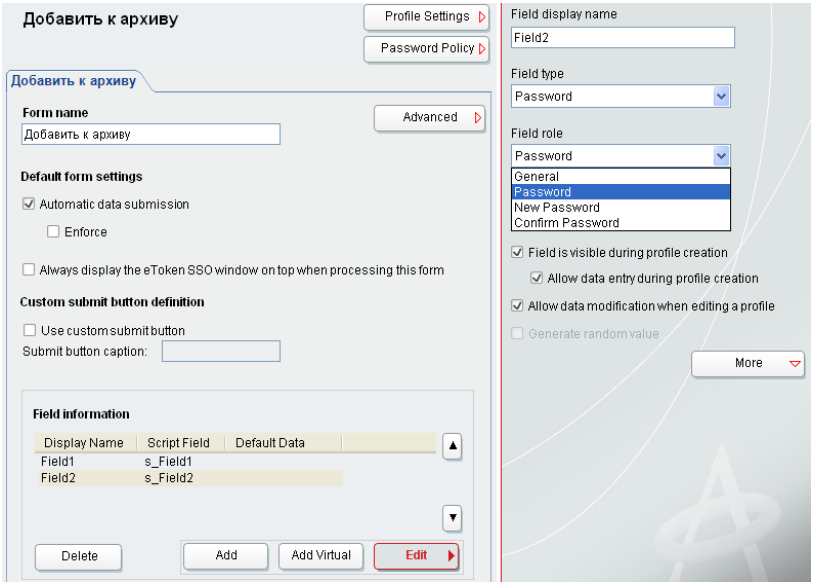

Рисунок 5 – Изменение «роли» поля

Для упрощения использования шаблона переименуйте («Field display name») добавленные поля Field1 и Field2 (рис. 6). Сохраните шаблон, нажав «Save» на нижней панели основного окна.

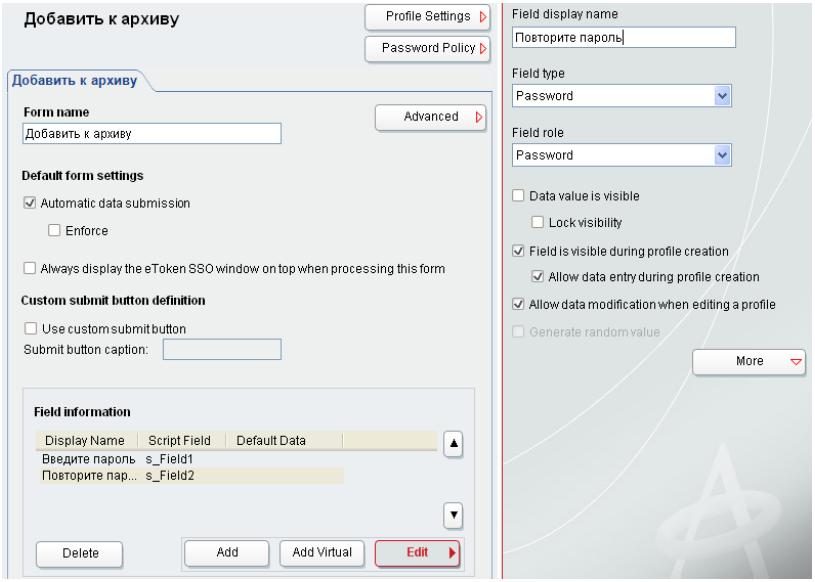

Рисунок 6 – Переименование шаблона

Создайте шаблон для извлечения файлов из архива, защищённого паролем. В контекстном меню архива выберите «7-Zip»-«Распаковать». Добавьте в шаблон поле для ввода пароля (рис. 7). Переименуйте полученное поле. Сохраните шаблон.

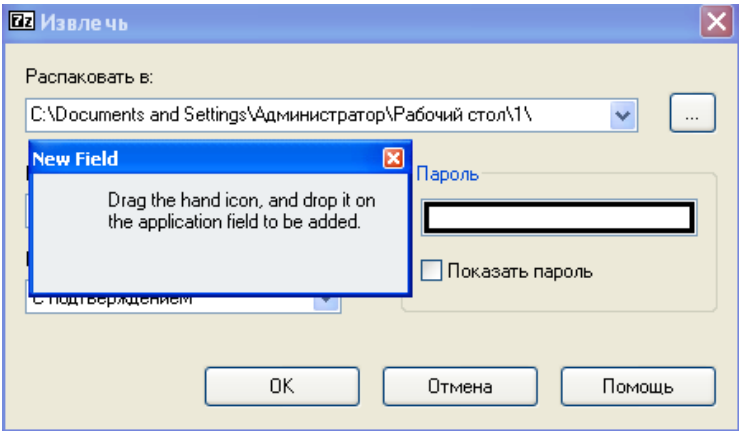

Рисунок 7 – Выбор поля «Пароль» для окна извлечения файлов

2. Создание профиля на eToken с аутентификационными данными приложения

По умолчанию шаблоны сохраняются в каталог «Мои документы\eToken SSO Templates». Чтобы пользователи на своём компьютере могли работать с шаблонами, необходимо скопировать эти шаблоны в каталог «Мои документы\eToken SSO Client Templates», находящийся в профиле пользователя.

Откройте eToken SSO Client (рис. 8). На панели инструментов нажмите «Обновить» («Refresh Profile List»). После чего откройте настройки eToken SSO Client (рис. 9). Если созданные шаблоны корректно загружены eToken SSO Client, то они должны отобразиться в списке, который открывается при нажатии кнопки «Show Loaded Templates».

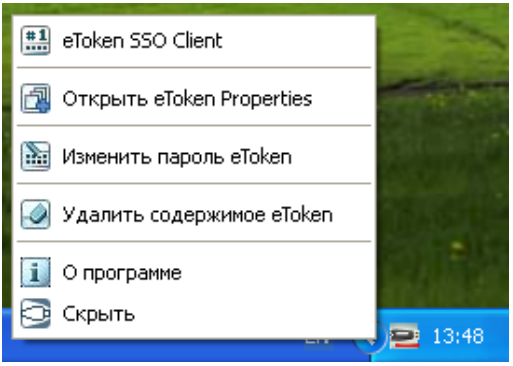

Рисунок 8 – Запуск eToken SSO Client

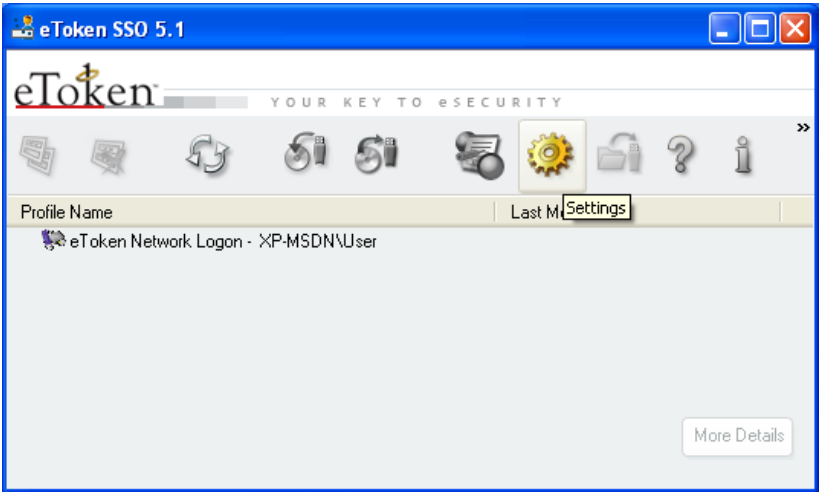

Рисунок 9 – Вид основного окна утилиты «eToken SSO Client»

Откройте для произвольного файла окно «Добавить к архиву». При первом запуске окна, для которого поддерживается шаблон, предлагается создать профиль на eToken с данными, предназначенными для полей этого шаблона (рис. 10). Введите в окно создания профиля пароль для архивирования и его подтверждение. Проделайте те же операции для распаковки файлов. Таким образом, при архивировании/извлечении файлов автоматически будет вводиться пароль из профиля, сохранённого на eToken. Произведите тестовое архивирование/извлечение произвольного файла.

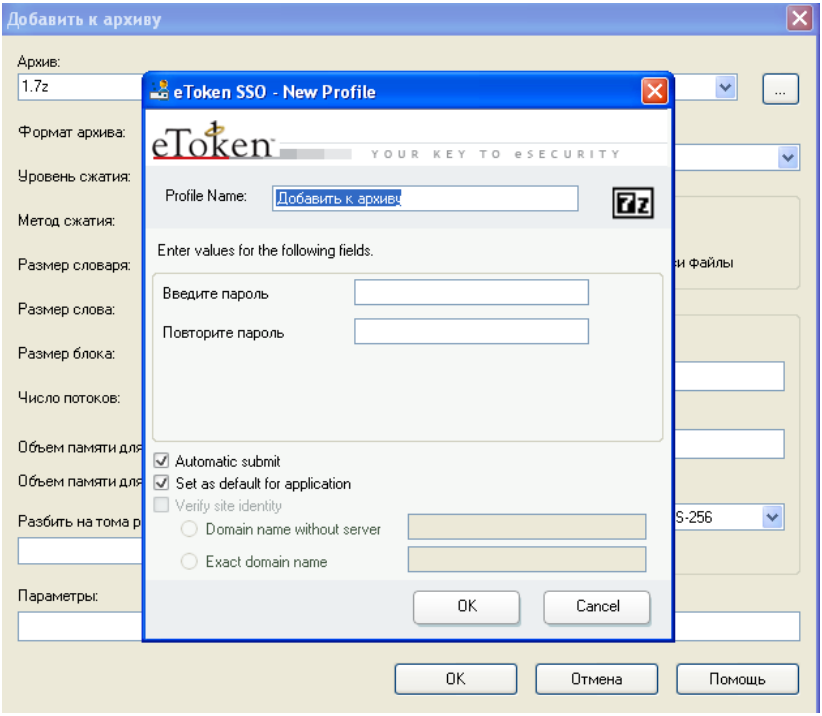

Рисунок 10 – Создание профиля на eToken для окна приложения

Созданные профили отображаются в основном окне утилиты eToken SSO Client (рис. 11). При помощи этой утилиты можно редактировать и удалять профили, сохранённые на eToken. Выберите один из профилей, созданных для «7-Zip», и нажмите кнопку «More Details» для отображения окна настроек выбранного профиля (рис. 12). В данном окне можно изменять настройки выбранного профиля (например, автоматическое нажатие кнопки OK – «Automatic submit») и содержимое профиля (пароль).

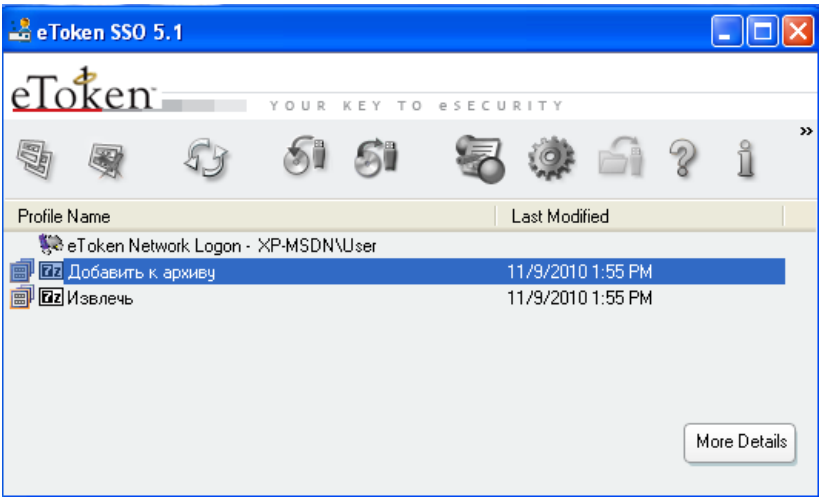

Рисунок 11 – Список профилей, сохранённых на eToken

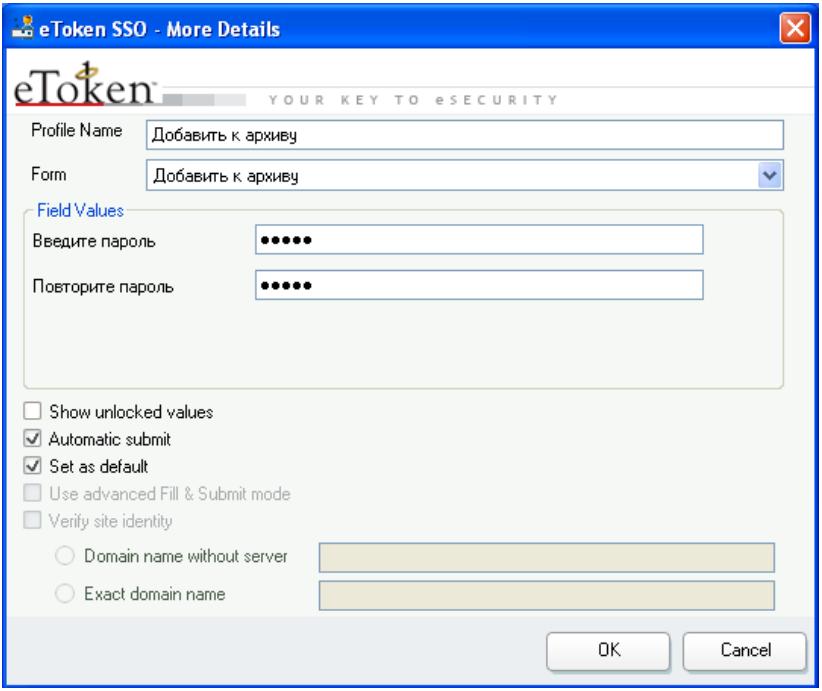

Рисунок 12 – Редактирование профиля и его настроек

3. Двухфакторная аутентификация на web-сайтах

Аналогично работе с приложениями происходит создание шаблонов и профилей для аутентификации на web-сайтах. Откройте в Internet Explorer web-сайт, который требует аутентификации, создайте для него шаблон. Перед сохранением шаблона в разделе «Profile Settings» отключите настройки, разрешающие редактирование («Enable profile editing») и удаление («Enable profile deletion») профиля, созданного на основе этого шаблона (рис. 13). Сохраните шаблон в «Мои документы\eToken SSO Client Templates». Создайте на основе этого шаблона профиль на eToken и попытайтесь его удалить и отредактировать через eToken SSO Client.

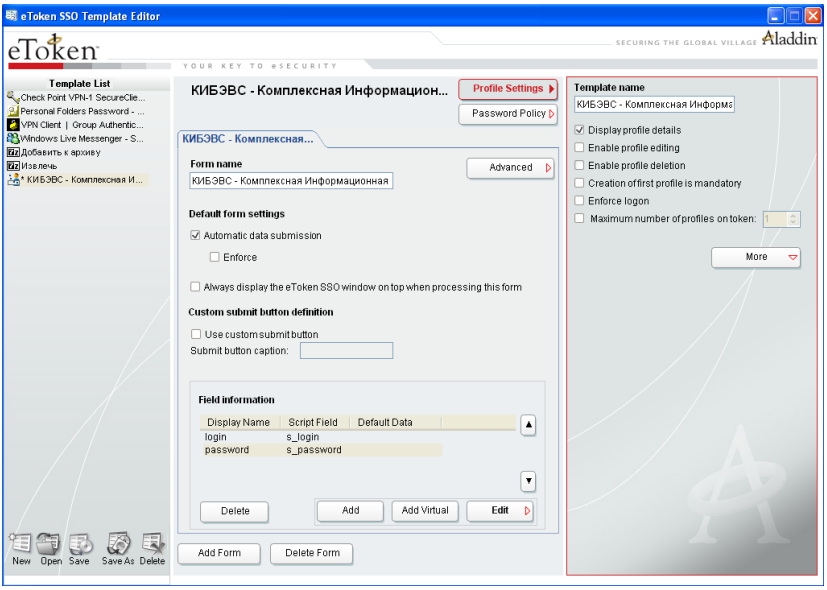

Рисунок 13 – Запрет редактирования и удаления профиля при создании шаблона

Для создания профилей web-сайтов не обязательно использовать шаблоны. Создание профилей возможно непосредственно при работе в Internet Explorer. Откройте какую-либо страницу в Интернете, на которой есть поля ввода аутентификационных данных. Введите логин и пароль, затем нажмите кнопку «Save» на панели инструментов SSO (рис. 14). При сохранении профиля возможно изменение следующих настроек: имени профиля, аутентификационных данных пользователя и автоматического подтверждения ввода (рис. 15). Сохраните профиль, содержащий данные для сайта, на eToken. Кроме того, через панель инструментов возможен быстрый доступ к сохранённым профилям

web-сайтов с автоматическим переходом на выбранную страницу, а также возможно заполнение аутентификационных форм и включение/отключение eToken SSO. Основной недостаток автоматического создания профилей для web-сайтов состоит в том, что определяются и включаются в профиль все поля для ввода данных (например, поле для ввода запроса на поиск).

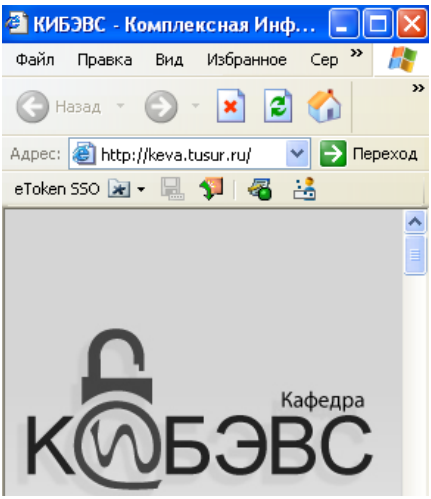

Рисунок 14 – Панель инструментов eToken SSO в Internet Explorer

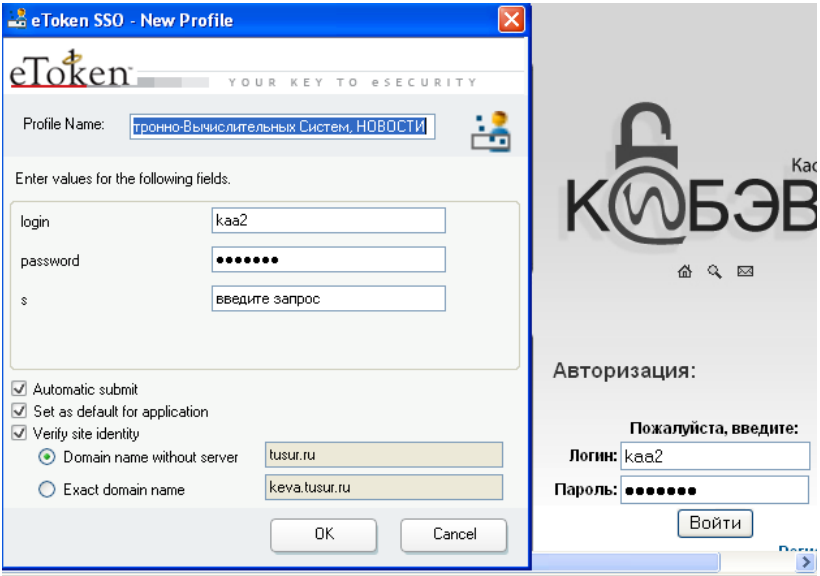

Рисунок 15 – Автоматическое создание профиля для web-сайта

4. Администрирование eToken SSO

Настройки утилиты «eToken SSO Client» можно изменять через «Групповые политики», используя соответствующий административный шаблон. Откройте оснастку gpedit.msc и добавьте административный шаблон «C:\Program Files\Aladdin\eToken\ eTokenSSO\eTokenSSO.adm». В появившемся разделе «SSO Management System Settings» можно разрешать или запрещать доступ к любой настройке, а также включать и отключать определённые функции рассматриваемой утилиты. Например, ограничьте количество профилей, которые можно сохранять на eToken. Для этого установите значение «True 4» у параметра «Set a Profiles Quota» (рис. 16). True – вводит в действие ограничение на количество профилей, а 4 – устанавливает максимальное количество профилей Для проверки внесённых изменений перезапустите утилиту «eToken SSO Client» («Пуск – Программы – eToken – eToken SSO – Resume eToken SSO Client») и попытайтесь сохранить на eToken более четырёх профилей.

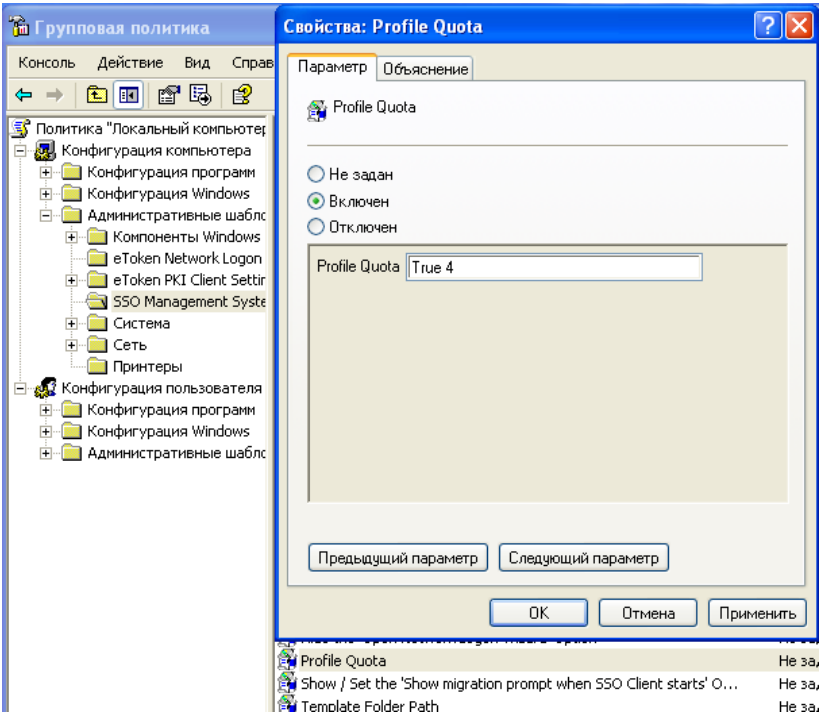

Рисунок 16 – Ограничение максимального количества профилей, сохраняемых на eToken.

Задание

1. Создайте шаблон для окна приложения, указанного в Вашем варианте (табл. 1).

2. При создании шаблона задайте для него настройки, указанные в Вашем варианте (табл. 1).

3. На основе сформированного шаблона создайте и сохраните на eToken соответствующий профиль.

Таблица 1 – Варианты заданий

Вар.	Приложение	Настройки шаблона
1	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет удаления профиля.
2	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет редактирования профиля.
3	Ввод пароля на proxy-сервер при запуске Internet Explorer.	Запрет отображения настроек профиля.
4	Запуск от имени администратора *.	Запрет удаления профиля.
5	Запуск от имени администратора *.	Запрет редактирования профиля.
6	Запуск от имени администратора *.	Запрет отображения настроек профиля.
7	Открытие файла из зашифрованного архива 7-Zip.	Запрет удаления профиля.
8	Открытие файла из зашифрованного архива 7-Zip.	Запрет редактирования профиля.
9	Открытие файла из зашифрованного архива 7-Zip.	Запрет отображения настроек профиля.
10	Добавление файлов к зашифрованному архиву 7-Zip.	Отключить автоматическое подтверждение введённых данных.

* – для демонстрации войдите под учётной записью «User» и запустите какую-либо оснастку MMC от имени учётной записи «Администратор».

Контрольные вопросы

1. При помощи какого приложения возможно использование eToken для аутентификации в различных прикладных программах на рабочих станциях пользователей?

2. Что такое «шаблоны приложений», применяемые eToken SSO?

3. Что включает в себя профиль, сохраняемый на eToken?

4. Каким образом происходит добавление полей окна приложения в шаблон?

5. Для чего предназначены папки «Мои документы\eToken SSO Templates» и «Мои документы\eToken SSO Client Templates»?

6. Как можно просмотреть список шаблонов, доступных для eToken SSO Client?

7. Каким образом можно при создании шаблона запретить удаление с eToken профиля, созданного на основе этого шаблона?

8. Каким образом можно редактировать данные, сохранённые в профиле eToken?

9. Какой параметр профиля отвечает за автоматическое подтверждение введённых данных?

10. В чём заключается преимущество создания профилей web-сайтов на основе шаблонов по сравнению с созданием профилей на основе открытой страницы?

ЛАБОРАТОРНАЯ РАБОТА №3

ДИСКРЕЦИОННЫЙ МЕХАНИЗМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ФАЙЛОВЫМ ОБЪЕКТАМ

Целью данной работы является практическое изучение дискреционного механизма разграничения доступа на основе встроенных средств операционной системы Windows XP Professional, позволяющих управлять доступом к файлам и папкам файловой системы NTFS.

Ход работы

Войдите в операционную систему под учётной записью «Администратор».

Для применения правил разграничения доступа необходимо воспользоваться вкладкой «Безопасность». Так как она по умолчанию отключена, её необходимо активировать. Для этого необходимо в разделе «Свойства папки» отключить опцию «Использовать простой общий доступ к файлам» (рис. 1).

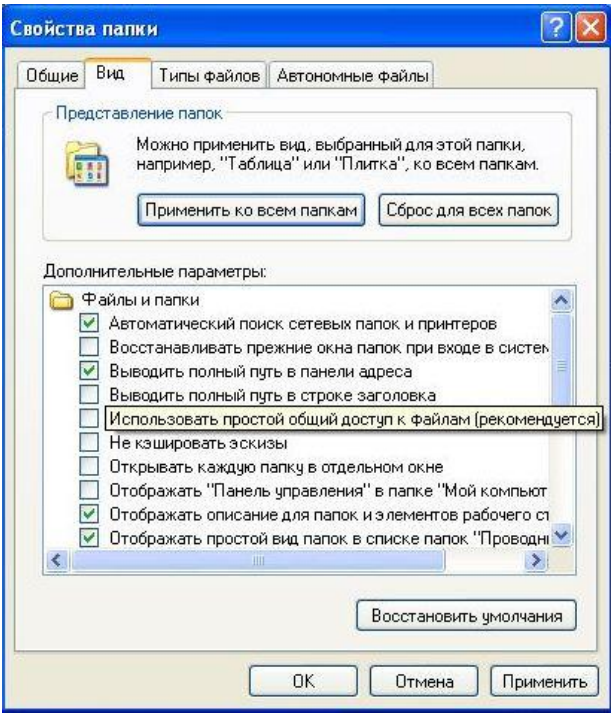

Рисунок 1 – Раздел «Свойства папки»

1. Основные права доступа к файловым объектам

В NTFS все разрешения сводятся к шести стандартным разрешениям (Полный доступ, Изменить, Чтение и выполнение, Список содержимого папки, Чтение, Запись). Данные разрешения могут предоставляться пользователю (или группе пользователей) на доступ к объектам – каталогам и файлам. Право «Полный доступ» не только включает в себя все остальные разрешения, но и позволяет управлять разграничением доступа к данному объекту.

Назначение прав доступа пользователей осуществляется для каждого объекта. Назначить или изменить права доступа можно в «Свойствах» выбранного каталога или файла во вкладке «Безопасность». Сначала необходимо выбрать пользователя (или группу), которому будут назначаться разрешения.

Откройте вкладку «Безопасность» в «Свойствах» каталога «D:\Список содержимого папки». Для изменения списка пользователей, имеющих право на доступ к объекту, нажмите на кнопку «Добавить» и выберите пользователя «user» (рис. 2).

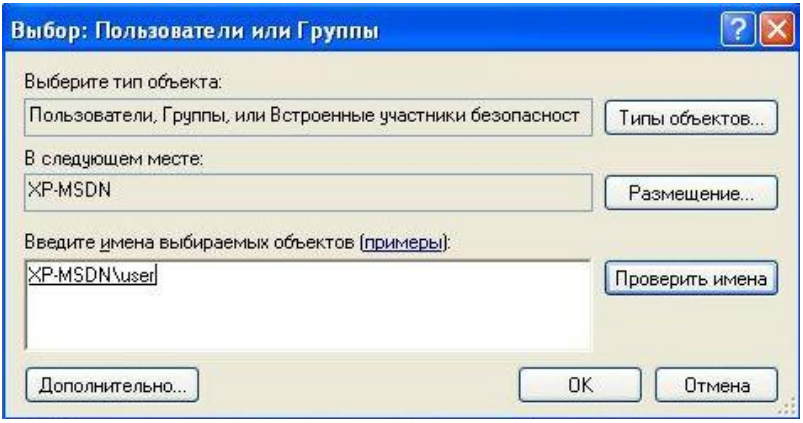

Рисунок 2 – Добавление нового пользователя

Установите пользователю «user» разрешение «Список содержимого папки» на доступ к текущему каталогу «D:\Список содержимого папки» (рис. 3).

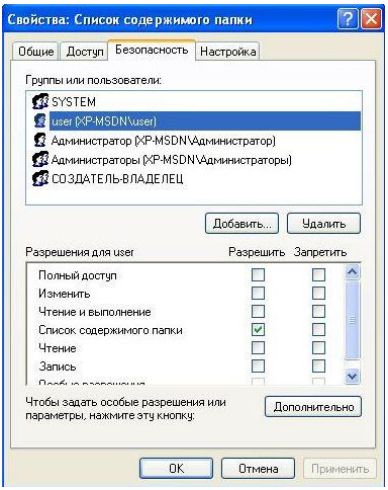

Рисунок 3 – Установка разрешения «Список содержимого папки»

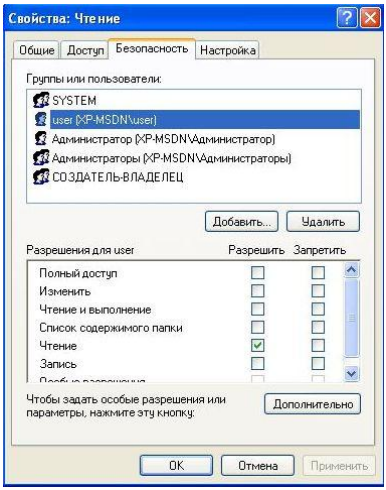

Рисунок 4 – Установка разрешения «Чтение»

Аналогично для пользователя «user» на каталоги «Чтение», «Чтение и выполнение», «Запись», «Изменение» и «Полный доступ» установите разрешения соответствующие названиям этих каталогов (рис. 4-8).

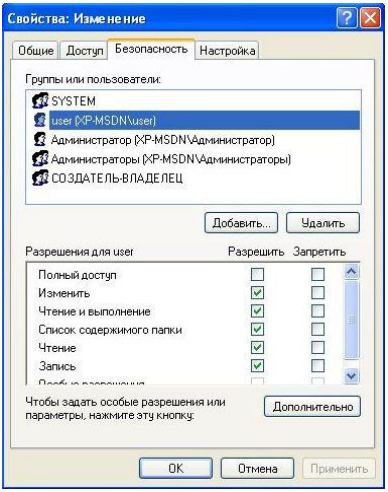

Рисунок 5 – Установка разрешения «Изменить»

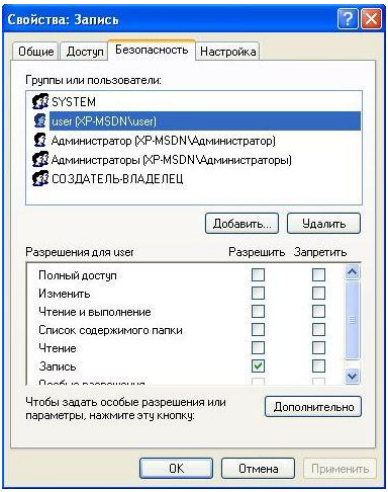

Рисунок 6 – Установка разрешения «Запись»

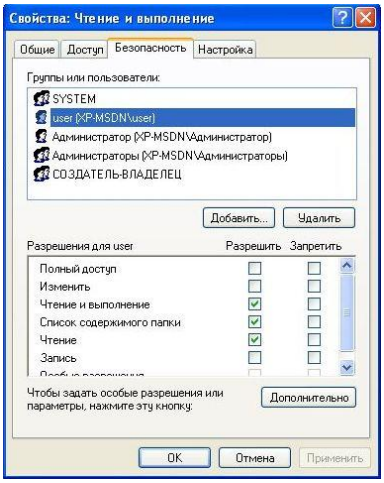

Рисунок 7 – Установка разрешения «Чтение и выполнение»

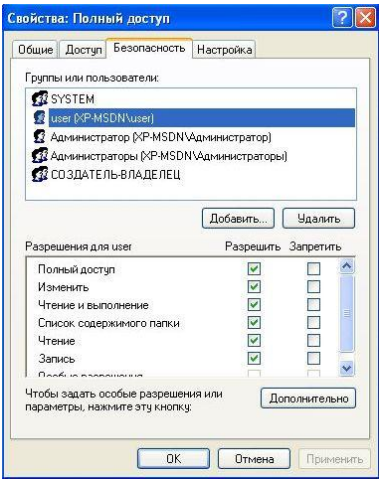

Рисунок 8 – Установка разрешения «Полный доступ»

Для проверки прав доступа, предоставленных пользователю при установке разрешений к заданным каталогам, войдите под учётной записью «user».

Разрешение «Список содержимого папки» предоставляет возможность просмотреть перечень объектов в данном каталоге. Войдите в соответствующий каталог и попытайтесь запустить исполняемый файл. Операционная система выдаст ошибку доступа к этому файлу (рис. 9). Попытайтесь открыть текстовый файл. Операционная система также выдаст ошибку доступа (рис. 10).

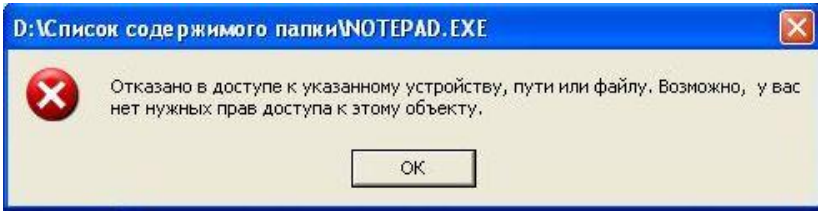

Рисунок 9 – Ошибка доступа к исполняемому файлу

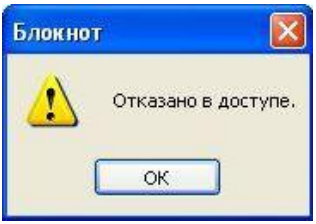

Рисунок 10 – Ошибка доступа к текстовому файлу

Разрешение «Чтение» предоставляет возможность открывать в данном каталоге все файлы, кроме исполняемых. Войдите в соответствующий каталог и откройте текстовый файл. Измените текст в открытом файле и попытайтесь сохранить его. Операционная система выдаст ошибку доступа на создание файла (рис. 11). Попытайтесь запустить исполняемый файл для проверки отказа в доступе.

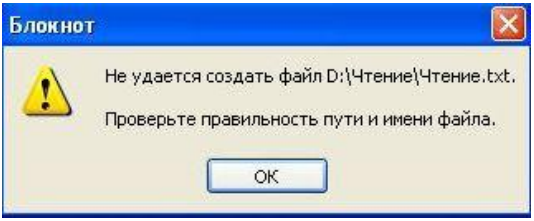

Рисунок 11 – Ошибка доступа на создание и сохранение измененённого текстового файла

Разрешение «Чтение и выполнение» предоставляет возможность открывать в данном каталоге все файлы. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и попытайтесь сохранить для проверки отказа в доступе на сохранение.

Разрешение «Запись» предоставляет возможность добавления файлов в данный каталог без права на доступ к вложенным в него объектам, в т.ч. на просмотр содержимого каталога. Попытайтесь войти в соответствующий каталог. Операционная система выдаст ошибку доступа к каталогу (рис. 12). Для проверки возможности добавления файла создайте файл с именем «Запись» (например, на «Рабочем столе») и попытайтесь перетащить его в каталог «Запись». Операционная система выдаст ошибку копирования, т.к. файл с таким именем в каталоге существует. Переименуйте файл и повторно попытайтесь его перетащить – копирование выполнится (кроме ого, наличие файла в каталоге можно проверить из под учётной записи «Администратор»).

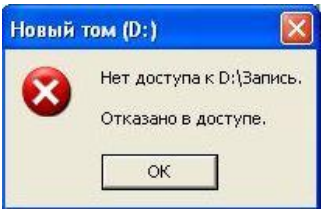

Рисунок 12 – Ошибка доступа к каталогу

Разрешение «Изменить» предоставляет возможность открывать и создавать (изменять) файлы в данном каталоге. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и сохраните его, создайте новый файл в каталоге. Откройте вкладку «Безопасность» у каталога «Изменение» или у любого вложенного файла и попытайтесь изменить права доступа к нему. Изменить права доступа нельзя (параметры включения разрешений неактивны), т.к. разрешение «Изменить» не включает возможность управления правами доступа (рис. 13).

Разрешение «Полный доступ» предоставляет все возможности для работы с каталогом и вложенными файлами, включая изменение разрешений. Для проверки откройте вкладку «Безопасность» у каталога «Полный доступ» или у любого вложенного файла и измените права доступа к нему.

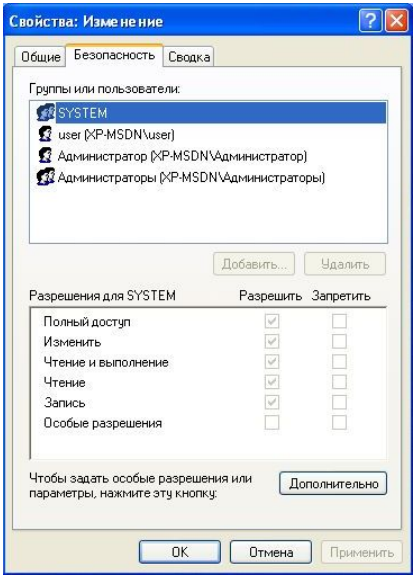

Рисунок 13 – Невозможность изменения разрешений на доступ

2. Элементы разрешений на доступ

Каждое стандартное разрешение состоит из нескольких элементов. Элементы разрешений позволяют более гибко настраивать права доступа пользователей.

Войдите под учётной записью «Администратор».

Просмотреть элементы разрешений на доступ можно, нажав на кнопку «Дополнительно» во вкладке «Безопасность» и выбрав любой элемент разрешений (рис. 14). Наборы элементов, включаемых в стандартные разрешения, приведены на рис. 15-20.

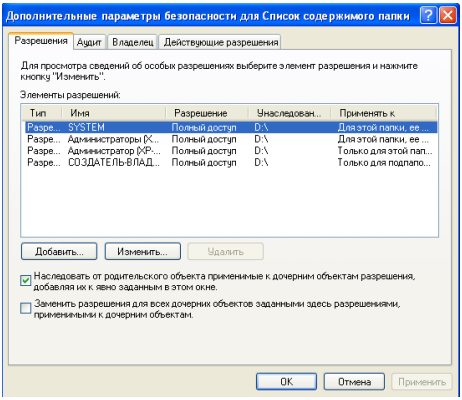

Рисунок 14 – Дополнительные параметры безопасности

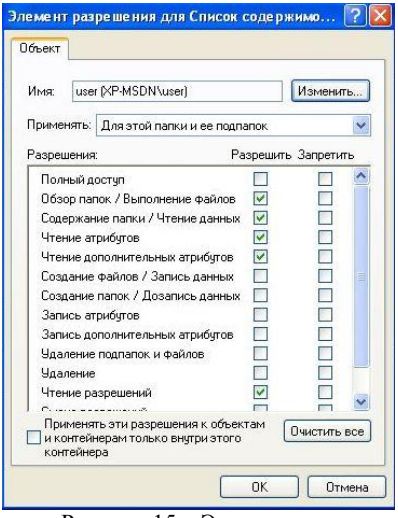

Рисунок 15 – Элементы разрешений для «Списка содержимого папки»

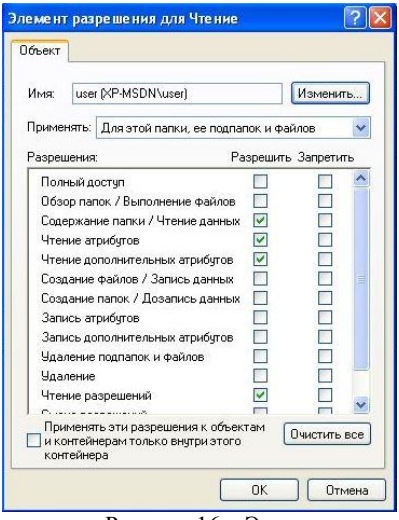

Рисунок 16 – Элементы разрешений для «Чтения»

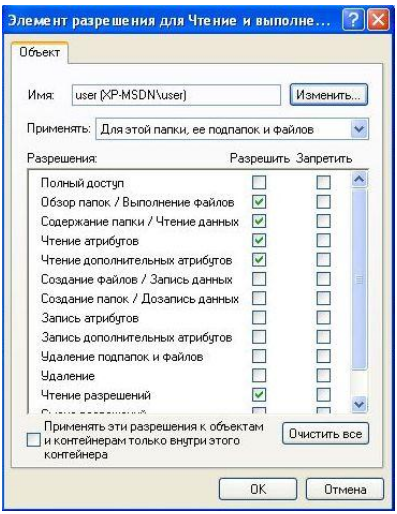

Рисунок 17 – Элементы разрешений для «Чтения и выполнения»

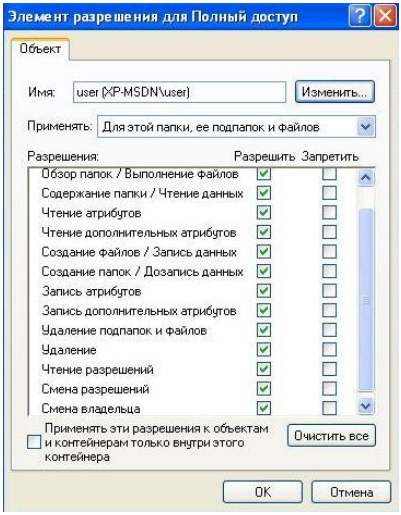

Рисунок 18 – Элементы разрешений для «Полного доступа»

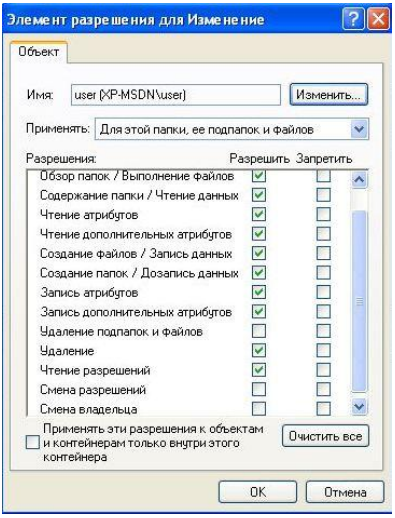

Рисунок 19 – Элементы разрешений для «Изменить»

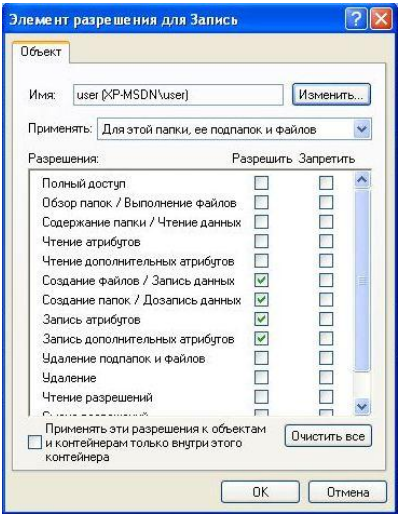

Рисунок 20 – Элементы разрешений для «Записи»

Использование возможностей элементов разрешений наиболее оправдано при разграничении доступа на удаление файла или каталога. Через элементы разрешений запретите пользователю «user»

удаление каталога «Изменение», а также разрешите запись атрибутов на каталог «Чтение» (рис. 21-22).

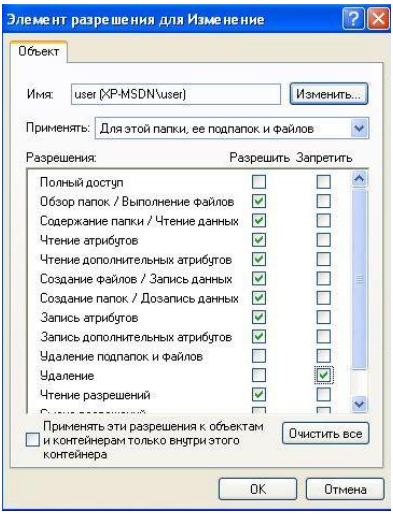

Рисунок 21 – Запрет удаления

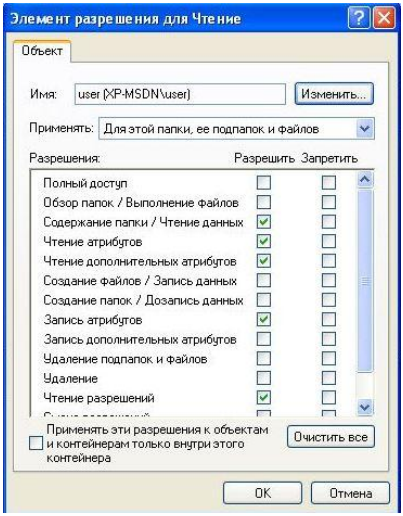

Рисунок 22 – Разрешение записи атрибутов

Для проверки установленных прав доступа войдите под учётной записью «user». Попытайтесь удалить файл из каталога «Изменение». Операционная система выдаст ошибку доступа на удаление файла (рис. 23).

Измените атрибуты файла в каталоге «Чтение» (например, атрибут «Скрытый» в свойствах файла). Примените сделанные изменения. Измените дополнительные атрибуты текстового файла в каталоге «Чтение» (например, автора документа во вкладке «Сводка» свойств файла). Попытайтесь применить сделанные изменения. Операционная система выдаст ошибку сохранения дополнительных атрибутов (рис. 24).

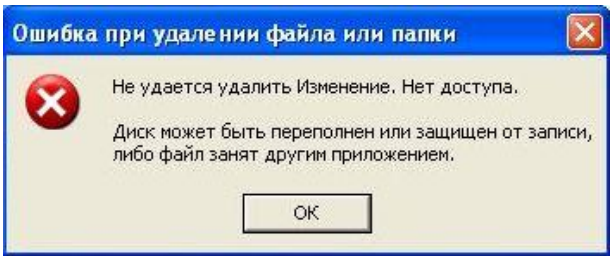

Рисунок 23 – Ошибка доступа на удаление файла

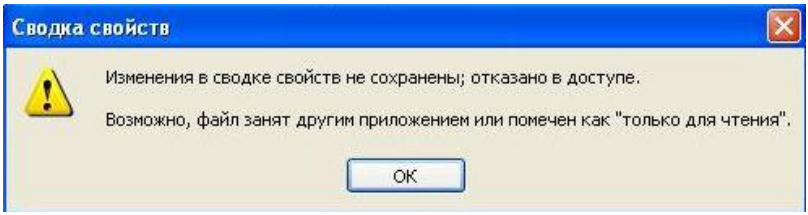

Рисунок 24 – Ошибка доступа на изменение дополнительных атрибутов

3. «Владелец» файла

В файловой системе NTFS у каждого объекта есть владелец. Владелец управляет назначением разрешений на доступ к объекту независимо от установленных разрешений.

Создайте под учётной записью «user» в каталоге «Изменение» новый каталог (например, «test») и в нём текстовый файл (например, «test.txt»). Скопируйте в созданный текстовый файл информацию из файла «Изменение». Откройте вкладку «Владелец» файла «test.txt». В ней указывается текущий владелец объекта (рис. 25). Предоставьте полный доступ к созданному каталогу пользователю «user1» (рис. 26).

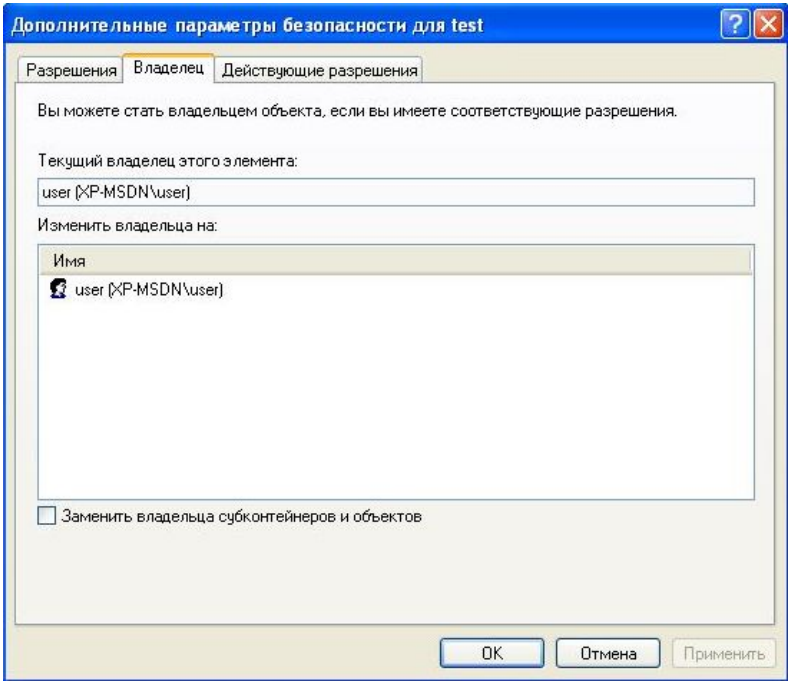

Рисунок 25 – Вкладка «Владелец»

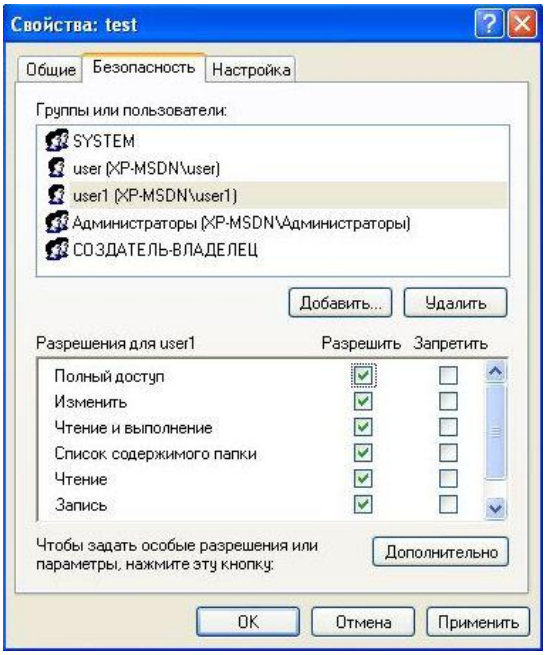

Рисунок 26 – Предоставление прав пользователю «user1»

Войдите под учётной записью «user1».

Попытайтесь перейти в каталог «D:\Изменение\test» при помощи иерархического представления каталогов в «Проводнике». Переход невозможен, потому что у пользователя «user1» нет доступа к промежуточным каталогам. Попытайтесь перейти в тот же каталог, указав его полный путь в адресной строке «Проводника» (рис. 27). Откройте файл «test.txt». Таким образом, пользователь «user» может несанкционированно предоставить доступ пользователю «user1» к конфиденциальной информации.

Наличие полного доступа у пользователя «user1» к каталогу «test» позволяет ему изменять разрешения. Запретите доступ пользователя «Администратор» к файлу «test.txt» (рис. 28).

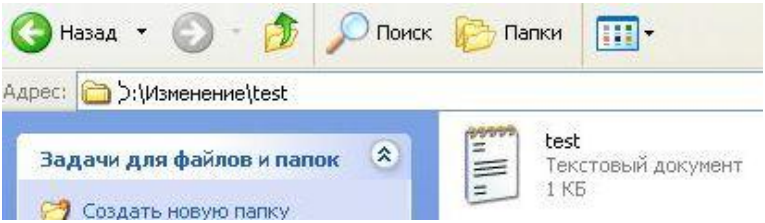

Рисунок 27 – Доступ к каталогу через адресную строку

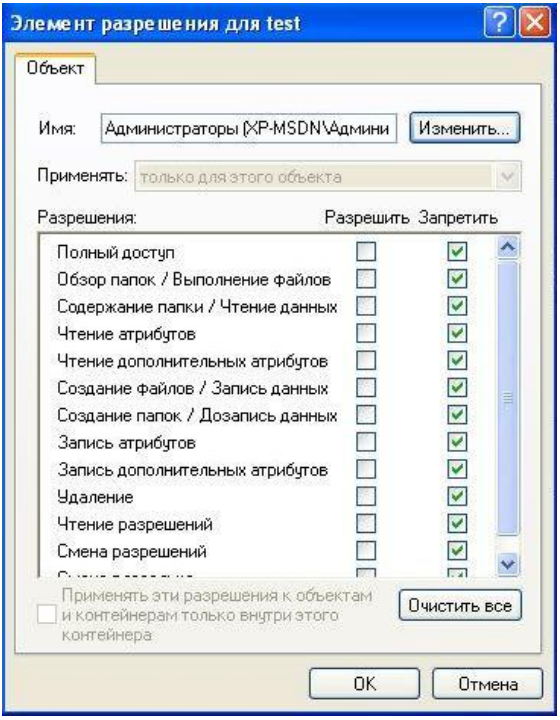

Рисунок 28 – Запрет доступа к файлу

Дополнительно разрешение «Полный доступ» даёт возможность смены владельца файла. Смените владельца файла «test.txt» на пользователя «user1» (рис. 29).

Попытайтесь изменить владельца другого файла/каталога, к которому нет полного доступа (например, диска D:\). Операционная система выдаст ошибку изменения владельца (рис. 30).

Войдите под учётной записью «Администратор».

Попытайтесь получить доступ к файлу «test.txt». Несмотря на то, что «Администратор» не может получить доступ к файлу, он может сменить владельца. Измените владельца файла на группу «Администраторы». Закройте свойства файла. При повторном входе в свойства файла у пользователя появляется возможность устанавливать права доступа (рис.31). Пользователи и группы, имеющие право менять владельца, не обладая полным доступом к нему, перечисляются в групповых политиках в параметре «Овладение файлами и другими объектами» (рис.32).

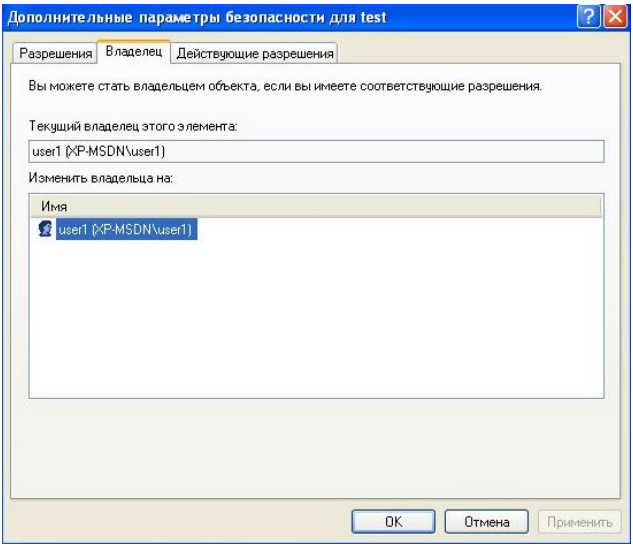

Рисунок 29 – Смена владельца файла

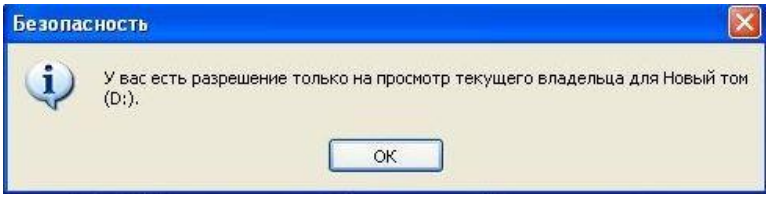

Рисунок 30 – Ошибка смены владельца файла

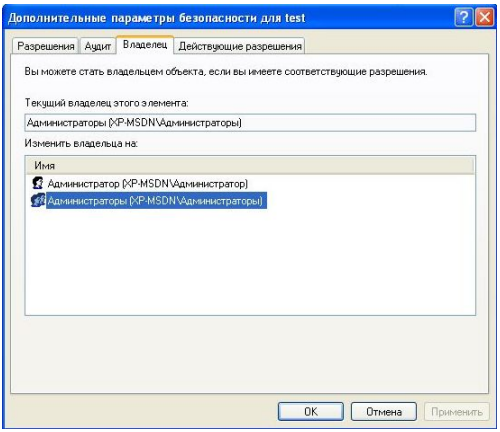

Рисунок 31 – Установка группы «Администраторы» в качестве владельца файла

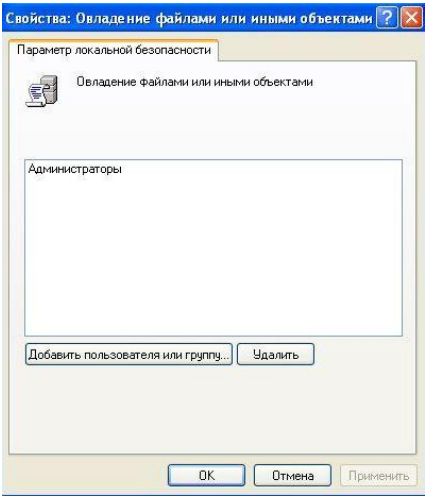

Рисунок 32 – Параметр «Овладение файлами и другими объектами»

4. Наследование прав доступа

NTFS поддерживает наследование разрешений, которое означает, что по умолчанию разрешения каталога распространяются на все его файлы и подкаталоги. Любые изменения разрешений на доступ к родительскому каталогу будут отражаться на его вложенных объектах.

Изменить унаследованные разрешения можно и со стороны вложенного объекта. Откройте вкладку «Разрешения» в дополнительных параметрах безопасности каталога «D:\Чтение\Чтение1» и отключите наследование (параметр «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне»). При отключении наследования скопируйте текущие разрешения (рис. 33).

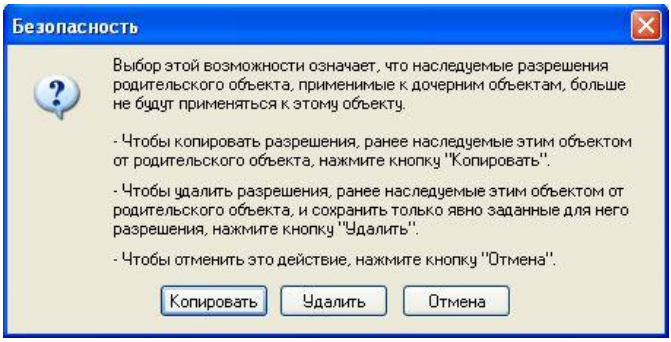

Рисунок 33 – Выбор действия при отключении наследования

После отключения наследования каталогом разрешений от родительского в разделе «Унаследовано» у каждого элемента устанавливается значение «не унаследовано» (рис. 34). Описание изменений в разделе «Унаследовано».

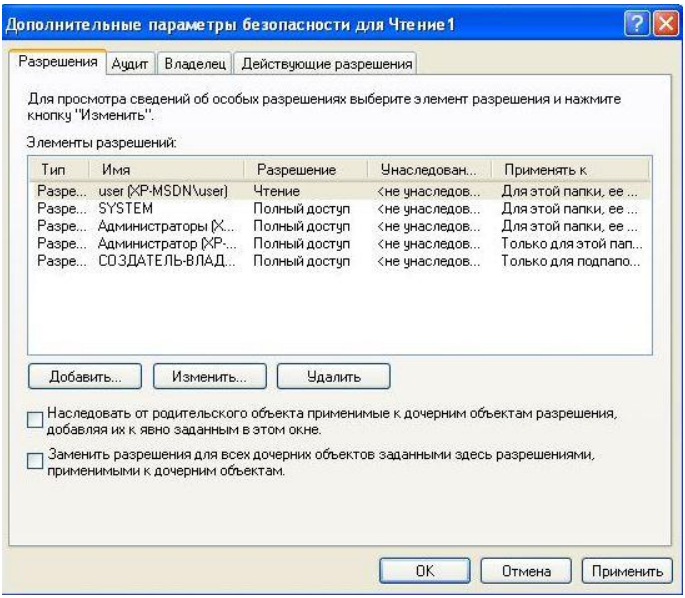

Рисунок 34 – Элементы разрешений при отключенном наследовании

Изменить действующие разрешения у вложенных объектов можно при помощи параметра «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Удалите учётную запись «user» из числа санкционированных пользователей каталога «Чтение1». В родительском для него каталоге «Чтение» установите изменение прав дочерних объектов (рис. 35). Проверьте восстановление учётной записи «user» в перечне санкционированных пользователей каталога «Чтение1».

При установке прав доступа на элементы можно выставлять не только разрешения, но и запреты. Запретите группе «Пользователи», членом которой является «user» (учётной записи «user» чтение разрешено) чтение файла «Чтение» (рис. 36). Войдите под учётной записью «user». Попытайтесь открыть файл «Чтение». Невозможность открыть файл обусловлена тем, что запреты приоритетнее разрешений.

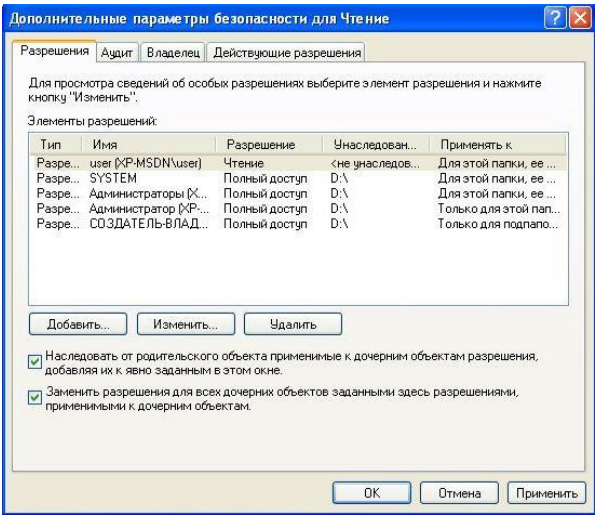

Рисунок 35 – Включение принудительного наследования

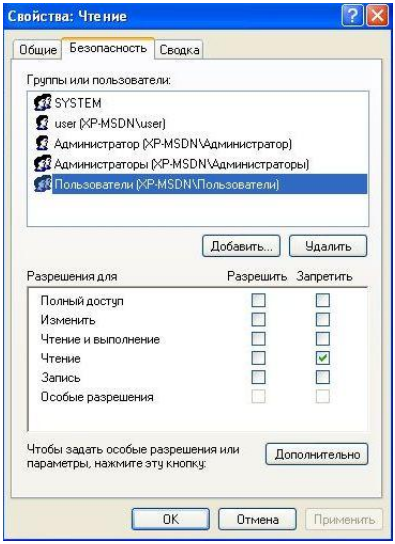

Рисунок 36 – Установка запрета на чтение

Действующие разрешения можно просмотреть в одноимённой вкладке Дополнительных параметров безопасности, выбрав интересующего пользователя или группу. Войдите под учётной записью «Администратор». Просмотрите действующие разрешения на файл «Чтение» для пользователя «user» (рис. 37). Удалите группу

«Пользователи» из перечня разрешений. Повторно просмотрите действующие разрешения пользователя «user» (рис. 38). Таким образом, разрешения предоставленные пользователю и группе, в которую он входит, суммируются. И после удаления элемента, запрещающего группе «Пользователи» чтение, у пользователя «user» остались только свои права.

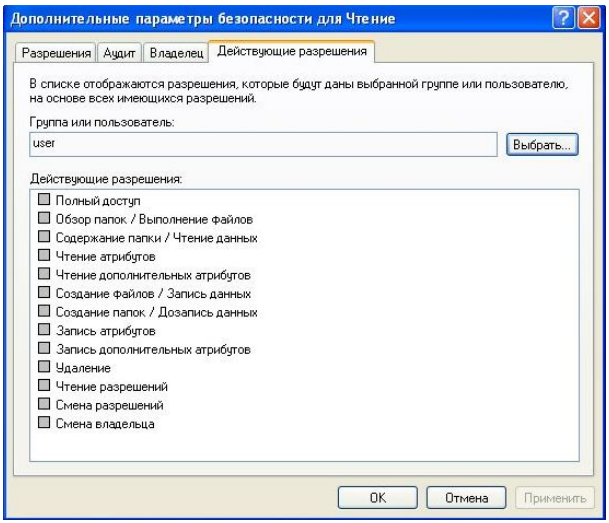

Рисунок 37 –Действующие разрешения пользователя

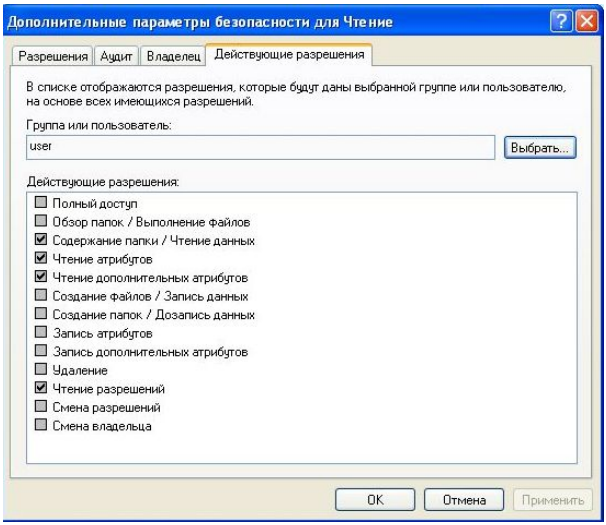

Рисунок 38 –Действующие разрешения пользователя после изменения разрешений

При выставлении разрешений существует возможность указывать глубину наследования и типы объектов. Можно распространить установленные разрешения на данный каталог, только на вложенные объекты или на каталог и все его вложенные объекты, а также можно указать на вложенные каталоги или файлы будут распространяться разрешения.

Разрешите на каталог «Чтение» пользователю «user» создание папок только для подпапок, вложенных в этот каталог (рис. 39), т.е. в каталогах «Чтение» и «Чтение2» подпапки создавать будет запрещено, а в каталоге «Чтение1» (непосредственно вложенном в «Чтение») – разрешено. Войдите под учётной записью «user». Проверьте возможность создания папок во всех указанных каталогах.

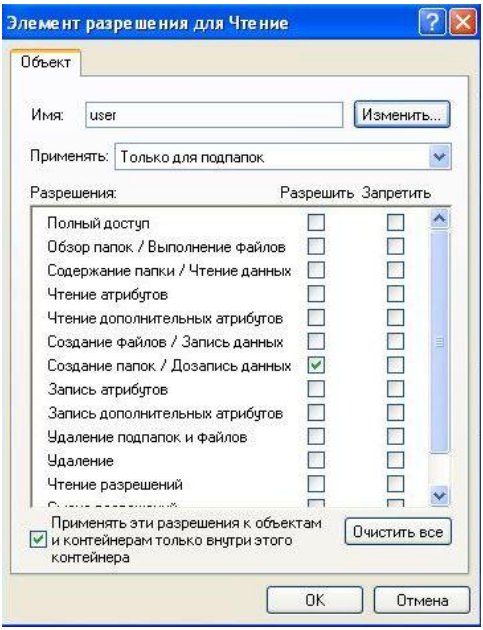

Рисунок 39 – Выбор глубины и типа объектов наследования

5. Разграничение доступа к принтерам

Под учётной записью «user» отправьте текстовый файл на печать при помощи принтера doPDF.

В разделе «Принтеры и факсы» меню «Пуск» попытайтесь изменить настройки принтера (рис. 40). Невозможность изменения настроек объясняется наличием у группы «Все» только права на «Печать» (отсутствием права на «Управление принтерами») (рис. 41).

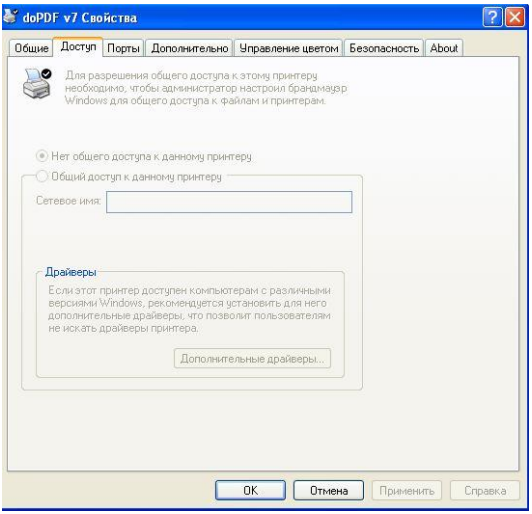

Рисунок 40 – Свойства принтера

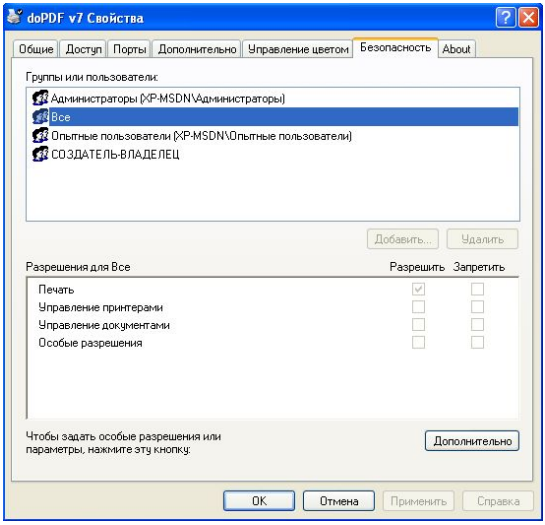

Рисунок 41 – Разграничение доступа к принтеру

Войдите под учётной записью «Администратор». Удалите из списка доступа к принтеру doPDF группу «Все».

Войдите под учётной записью «user».

Попытайтесь напечатать текстовый файл. Откройте раздел «Принтеры и факсы», в котором doPDF отсутствует, т.к. «user не» входит в список пользователей, имеющих право на работу с принтером.

Задание

Создайте каталоги «Общедоступно» и «Конфиденциально». В каждом из этих каталогов скопируйте исполняемый и текстовый файлы. Разграничьте доступ к принтеру, а также созданным каталогам и файлам в соответствии со своим вариантом.

Вариант 1

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение	Полный доступ
user	Чтение	Изменить, кроме удаления	Печать Управление документами
user1	Изменить	Нет доступа	Печать

Вариант 2

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение и выполнение	Полный доступ
user	Изменить	Чтение	Печать
user1	Чтение и выполнение	Изменить	Печать Управление документами

Вариант 3

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Конфиденциально»
Администратор	Полный доступ	Список содержимого	Нет доступа
user	Чтение	Изменить, кроме удаления	Изменить
user1	Изменить	Нет доступа	Нет доступа

Вариант 4

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Конфиденциально»
Администратор	Изменить	Чтение и выполнение	Нет доступа
user	Чтение	Изменить	Запрет удаления
user1	Полный доступ, кроме смены владельца	Запись	Нет доступа

Вариант 5

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Администратор	Полный доступ	Список содержимого	Выполнение
user	Чтение	Чтение и удаление	Выполнение, запрет удаления
user1	Изменить, кроме удаления	Запись	Нет доступа

Вариант 6

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Администратор	Полный доступ	Чтение	Изменить
user	Чтение и удаление	Список содержимого	Выполнение
user1	Изменить	Нет доступа	Нет доступа

Вариант 7

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Общедоступно»
Администратор	Список содержимого	Полный доступ	Нет доступа

user	Изменить, кроме удаления	Чтение	Изменить
user1	Нет доступа	Изменить	Нет доступа

Вариант 8

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Конфиденциально»
Администратор	Чтение и выполнение	Изменить	Нет доступа
user	Изменить	Чтение	Изменить, запрет изменения дополнит. атрибутов
user1	Запись	Изменить, кроме удаления	Нет доступа

Вариант 9

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Администратор	Список содержимого	Полный доступ	Выполнение
user	Чтение и удаление	Чтение	Выполнение, запрет удаления
user1	Запись	Полный доступ	Нет доступа

Вариант 10

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Администратор	Чтение	Полный доступ	Изменить
user	Список содержимого	Чтение и удаление	Выполнение
user1	Нет доступа	Изменить	Нет доступа

Контрольные вопросы

1. Охарактеризуйте дискреционную модель управления доступом.
2. Перечислите стандартные права доступа к файловым объектам, существующие в файловой системе NTFS.
3. Объясните принцип работы разрешения «Запись».
4. Перечислите элементы разрешений.
5. Кто может стать владельцем объекта?
6. Раскройте понятие наследования разрешений.
7. Как отключить наследование разрешений?
8. Как реализовать принудительное наследование вложенными объектами установленных разрешений?
9. Перечислите приоритеты применения разрешений при определении действующих разрешений на доступ к файловым объектам.
10. Перечислите стандартные права доступа к принтерам, существующие в файловой системе NTFS.

ЛАБОРАТОРНАЯ РАБОТА №4

МАНДАТНЫЙ МЕХАНИЗМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ФАЙЛОВЫМ ОБЪЕКТАМ

Целью данной работы является практическое изучение мандатного механизма разграничения доступа на основе программного продукта Secret Net 5.1 (автономный вариант).

Ход работы

1. Настройка категорий конфиденциальности

Доступ пользователя к информации, содержащейся в конфиденциальном файле, осуществляется при условии, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов.

Запустите «Локальные параметры безопасности» под учетной записью «Администратор»: «Пуск – Все программы – Secret Net 5 – Локальная политика безопасности», перейдите в группу «Параметры Secret Net 5 Настройка подсистем – настройка подсистем».

Параметр «Полномочное управление доступом: название уровней конфиденциальности» настройте, как показано на рис. 1.

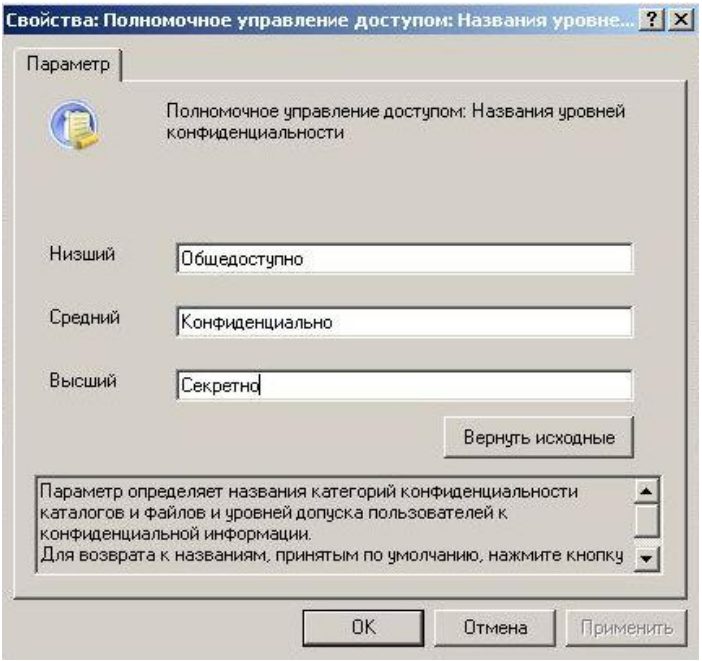

Рисунок 1 – Параметр «Название уровней конфиденциальности»

2. Настройка субъектов доступа

Запустите «Управление компьютером» под учётной записью «Администратор»: «Пуск – Все программы – Secret Net 5 – Управление компьютером», перейдите в группу «Локальные пользователи и группы – Пользователи».

Далее настройте права администратора. Для этого в свойствах учётной записи «Администратор» перейдите на вкладку Secret Net 5. В группе «Доступ» установите следующие значения (рис. 2).

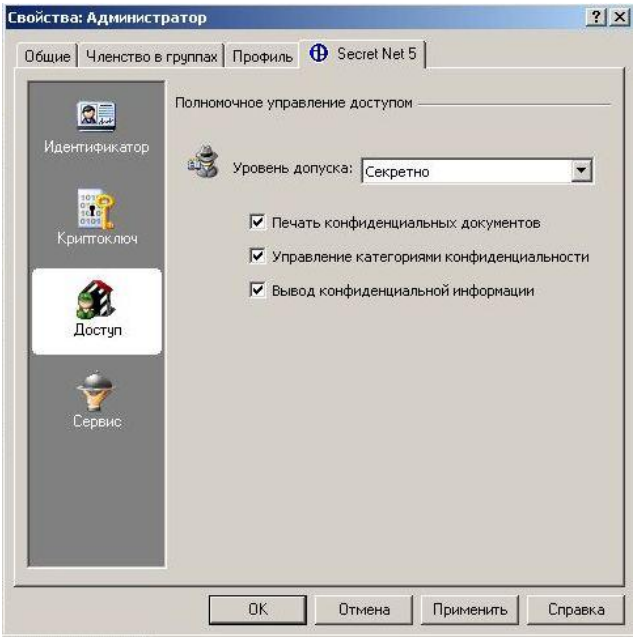

Рисунок 2 – Настройка прав доступа пользователя «Администратор»

– Управление категориями конфиденциальности – пользователь может изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; управлять режимом наследования категорий конфиденциальности каталогов.

– Печать конфиденциальных документов – используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов.

– Вывод конфиденциальной информации – пользователю разрешается выводить конфиденциальную информацию на внешние носители.

После чего вернитесь в оснастку «Локальные пользователи и группы – Пользователи». Создайте пользователя, выбрав «Новый пользователь» в контекстном меню или в меню «Действие». Настройте учётную запись как показано на рис. 3 и нажмите кнопку «Создать».

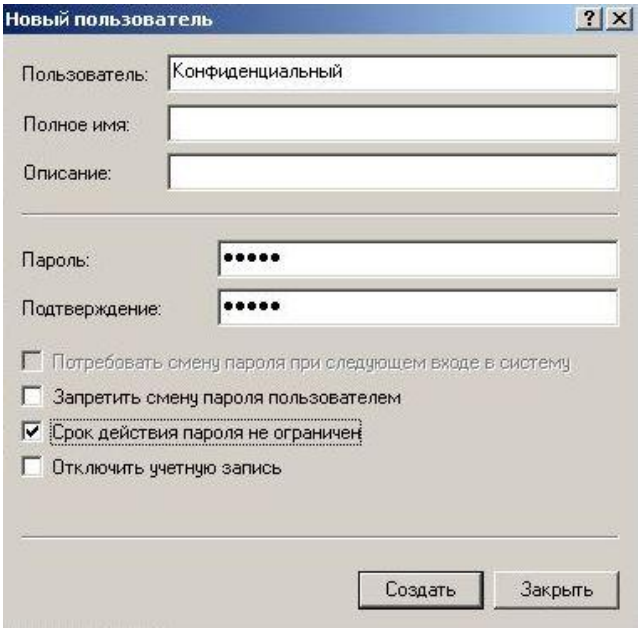

Рисунок 3 – Создание пользователя

По аналогии создайте пользователя «Секретный».

Для настройки прав доступа перейдите в группу «Пользователи», выделите пользователя «Конфиденциальный». В контекстном меню выберите «Свойства». В группе «Доступ» настройте параметры как показано на рис. 4, предоставив право вывода информации на внешние носители и печать конфиденциальных документов.

Для пользователя «Секретный» выберите уровень допуска «Секретно», запретив вывод на внешние носители и печать конфиденциальных документов (рис. 5).

Для применения настроек завершите сеанс и повторно войдите под учётной записью «Администратор».

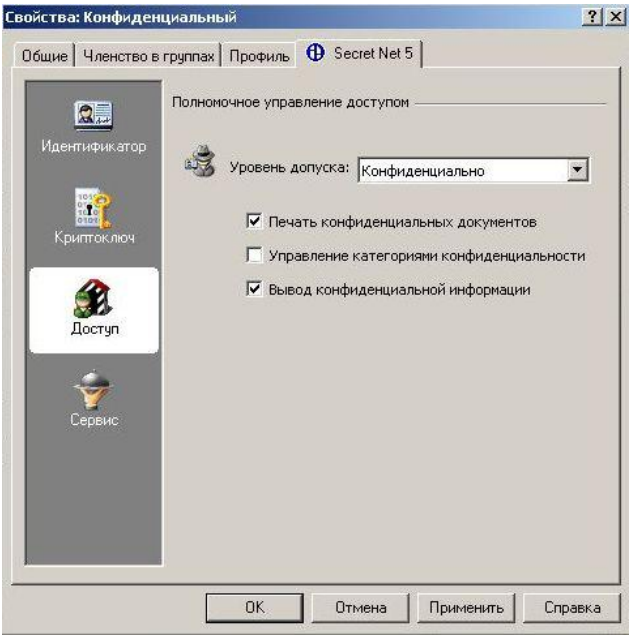

Рисунок 4 – Настройка прав доступа пользователя «Конфиденциальный»

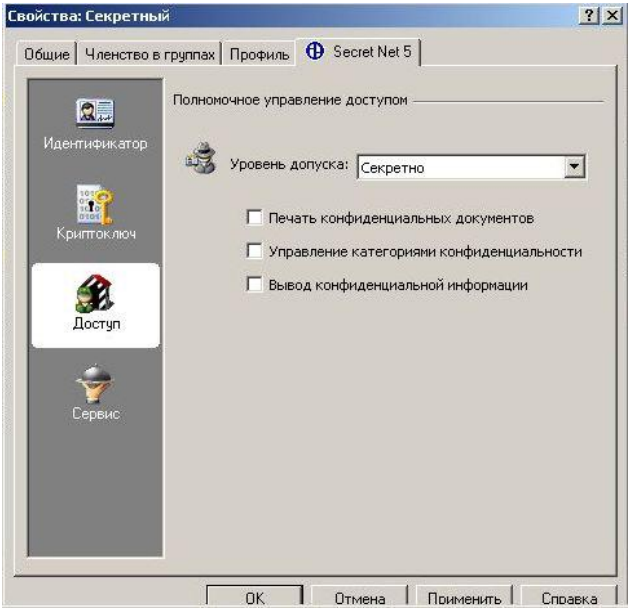

Рисунок 5 – Настройка прав доступа пользователя «Секретный»

3. Настройка объектов доступа (данные)

В механизме полномочного управления доступом используются следующие категории конфиденциальности:

– неконфиденциально (в нашем случае «общедоступно»);

– конфиденциально;

– строго конфиденциально (в нашем случае «секретно»).

Категория конфиденциальности относится к атрибутам ресурса (каталога или файла). Повышение категорий конфиденциальности нужных ресурсов осуществляется пользователями в пределах своих уровней допуска. В механизме полномочного управления доступом используется принцип наследования файлами категории конфиденциальности каталога.

Присвоение новым файлам категории конфиденциальности каталога может выполняться автоматически или по запросу. Включение и отключение режима автоматического присвоения категории осуществляется в диалоговом окне настройки свойств каталога (параметр «Автоматически присваивать новым файлам», рис. 6).

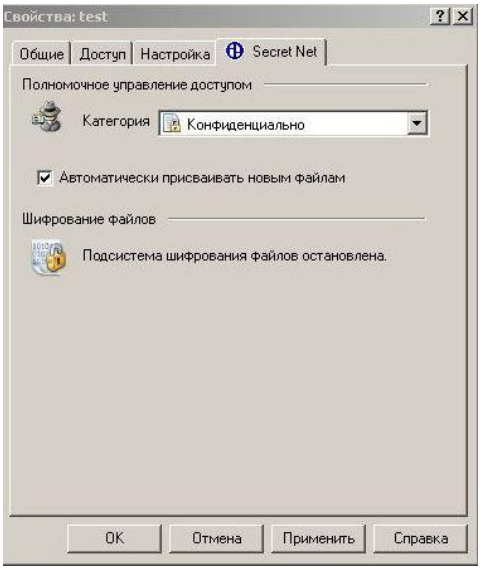

Рисунок 6 – Выбор категории конфиденциальности ресурса

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию «Управление категориями конфиденциальности». Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Для изменения категории конфиденциальности каталога или файла в режиме мандатного разграничения доступа необходимо обладать привилегией «Управление категориями конфиденциальности». Если у пользователя нет такой привилегии, то он может только повысить категорию конфиденциальности файла, но не выше своего уровня допуска или уровня конфиденциальности сеанса.

В проводнике вызовите контекстное меню каталога «D:\temp» и выберите «Свойства». В окне «Свойства» откройте вкладку «Secret Net» (рис. 6).

Укажите для каталога следующие значения параметров:

– выберите в раскрывающемся списке поля «Категория» категорию «Конфиденциально»;

– установите режим автоматического присвоения категории конфиденциальности файлам каталога, включив параметр «Автоматически присваивать новым файлам».

Нажмите кнопку «ОК».

Если каталог содержит файлы и подкаталоги, на экране появится диалоговое окно, предлагающее изменить категории конфиденциальности вложенным файлам и каталогам (рис. 7).

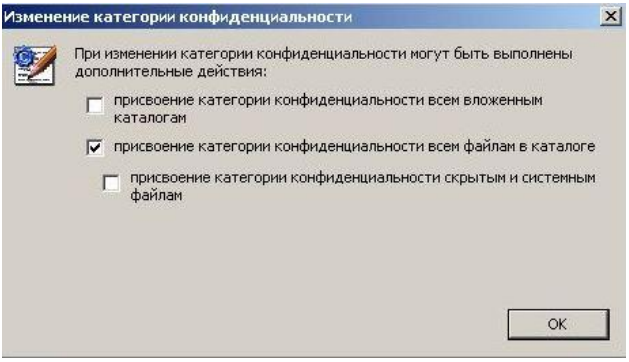

Рисунок 7 – Изменение категории конфиденциальности вложенных каталогов и файлов

Изменение категории конфиденциальности файла производится аналогично.

Пользователю разрешается доступ к файлу, если уровень допуска пользователя не ниже категории конфиденциальности файла. Например, пользователю с уровнем допуска «Конфиденциально» разрешается выполнять чтение файлов с категориями «Конфиденциально» и «Общедоступно», но запрещено открывать файлы с категорией «Секретно». Уровень допуска «Секретно» предоставляет возможность открывать файлы с любой категорией конфиденциальности.

Если категория допуска пользователя выше, чем метка конфиденциальности каталога с документами, то пользователь может открывать документы, но изменять и сохранять в этой же папке не сможет, также запрещено создавать и удалять документы в папках, категория конфиденциальности которых меньше категории допуска пользователя.

Войдите под учётной записью «user» (уровень допуска «Общедоступно»). Попытайтесь открыть файл «D:\temp\Конф.txt». Операционная система выдаст ошибку доступа к этому файлу (рис. 8). Попытайтесь удалить этот файл. Операционная система выдаст ошибку удаления этого файла (рис. 9). Попытайтесь скопировать файл в общедоступный каталог (например, «Рабочий стол»). Операционная система выдаст ошибку копирования файла (рис. 10). Попытайтесь создать новый файл в каталоге «test». Операционная система выдаст ошибку создания файла (рис. 11).

Таким образом, под учётной записью с уровнем допуска «Общедоступно» запрещены любые действия с файловыми объектами уровня «Конфиденциально» (пользователь не может работать с документами, чья категория конфиденциальности выше его уровня допуска).

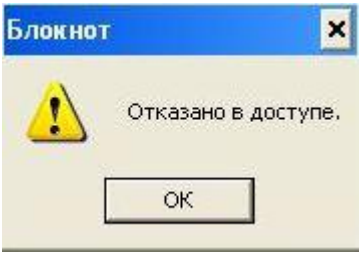

Рисунок 8 – Ошибка доступа к конфиденциальному файлу

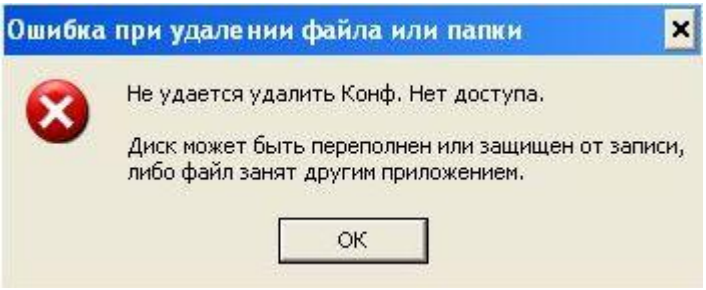

Рисунок 9 – Ошибка удаления конфиденциального файла

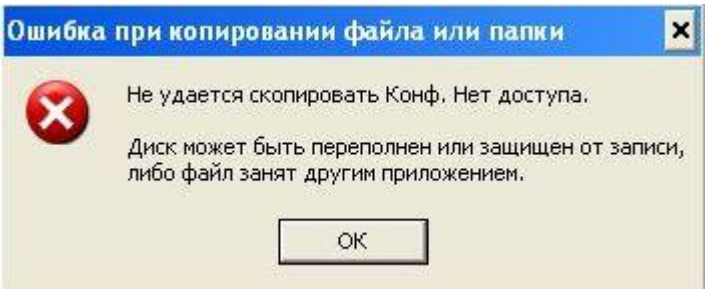

Рисунок 10 – Ошибка копирования конфиденциального файла

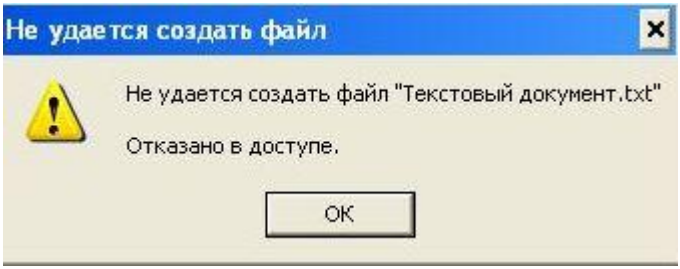

Рисунок 11 – Ошибка создания файла в конфиденциальном каталоге

Войдите под учётной записью «Секретный». Попытайтесь открыть файл «D:\temp\Конф.txt» – будет выдано окно с предложением о повышении уровня конфиденциальности приложения (рис. 12). Работа с файлом будет разрешена только после повышения уровня. Скопируйте файл в общедоступный каталог (например, «Рабочий стол»). Посмотрите уровень конфиденциальности у скопированного файла. После копирования был присвоен уровень «Общедоступно». Попытайтесь скопировать данные из файла «D:\temp\Конф.txt» в любой файл с меткой «Общедоступно». Уровень конфиденциальности у общедоступного файла не изменился.

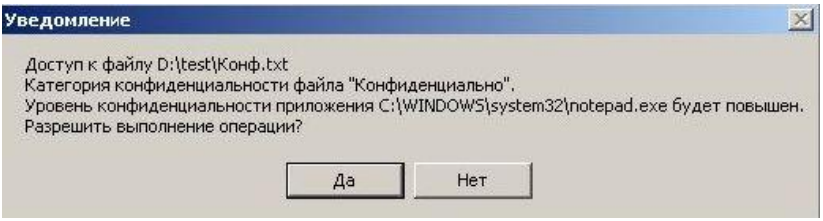

Рисунок 12 – Повышение уровня конфиденциальности приложения

Таким образом, возможность копирования конфиденциальных файлов в общедоступный каталог или самих конфиденциальных данных в общедоступный файл может привести к утечке информации.

При таком подходе ответственность за конфиденциальность информации лежит на пользователях, которым разрешён доступ к информации.

4. Контроль потоков данных

4.1. Включение контроля потоков данных

Запретить пользователям возможность понижения уровня конфиденциальности информации можно при помощи контроля потоков данных.

Войдите под учётной записью «Администратор». Запустите «Локальные параметры безопасности»: «Пуск – Все программы – Secret Net 5 – Локальная политика безопасности», перейдите в группу «Параметры Secret Net – Настройки подсистем». Выберите параметр «Полномочное управление доступом: Режим работы» и включите контроль потоков.

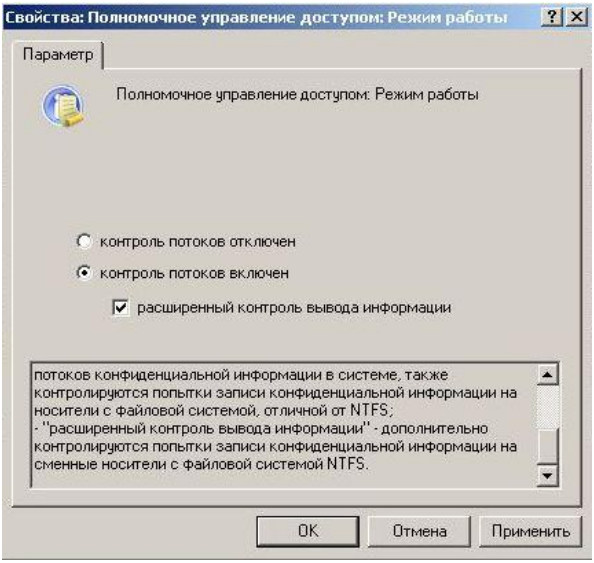

Рисунок 13 – Включение контроля потоков данных

4.2. Работа с конфиденциальными файлами при более высоком уровне сеанса

Перезагрузите операционную систему для применения настроек и войдите под учётной записью «Секретный». При входе появляется предложение выбрать уровень сеанса, определяющего, с каким уровнем конфиденциальности файлов будет проходить работа (рис. 14). Выберите уровень сеанса «Секретно».

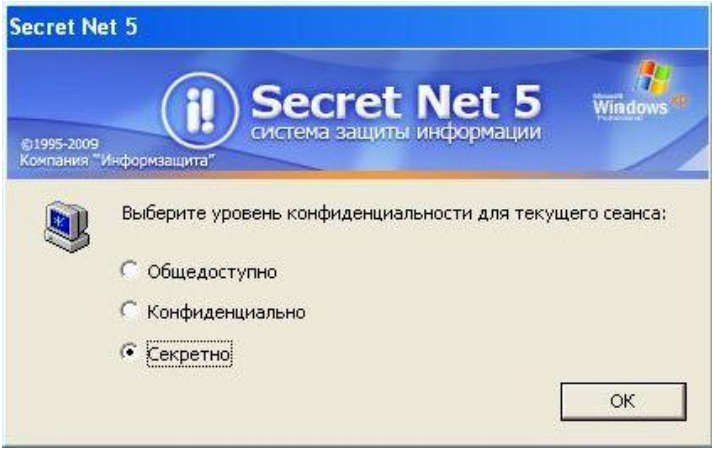

Рисунок 14 – Выбор уровня конфиденциальности сеанса

Откройте файл «D:\temp\Конф.txt». Попытайтесь удалить этот файл, изменить и сохранить его, скопировать в общедоступный каталог (например, «Рабочий стол»). Попытайтесь создать новый файл в каталоге «test». Таким образом, если включен контроль потоков данных, то при уровне сеанса более высоком, чем уровень конфиденциальности файла, все действия, кроме чтения, запрещены.

Измените файл «D:\temp\Конф.txt» и попытайтесь его сохранить под другим именем или в другой каталог. Сохранение будет невозможно (рис. 15), т.к. уровень сеанса выше, чем уровень конфиденциальности каталогов.

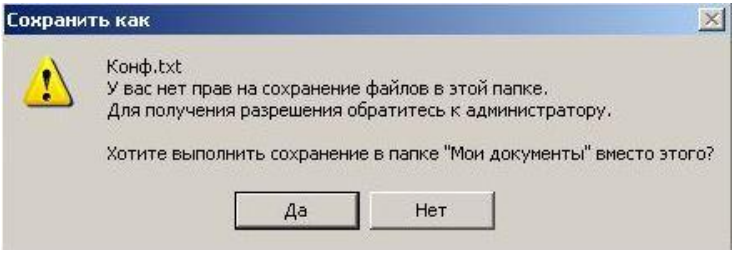

Рисунок 15 – Ошибка сохранения информации при контроле потоков в каталог с меньшим уровнем конфиденциальности, чем уровень сеанса

4.3. Работа с конфиденциальными файлами при равном уровне сеанса

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Конфиденциально».

Откройте файл «D:\temp\Конф.txt». Измените и сохраните этот файл, создайте новый файл в каталоге «test». Попытайтесь

скопировать его в общедоступный каталог (например, «Рабочий стол»).

Скопируйте текст из файла «Конф.txt» в файл «Общее.txt» и попытайтесь сохранить файл «Общее.txt». Произойдёт отказ в доступе из-за попытки понизить уровень конфиденциальности информации. Сохраните файл «Общее.txt» в конфиденциальный каталог «test».

Измените какую-либо настройку операционной системы (например, отображение вкладки «Безопасность»: измените параметр «Использовать простой общий доступ к файлам» в разделе «Панель управления – Свойства папки»). Перезапустите вкладку «Свойства папки» и проверьте состояние параметра. Попытайтесь запустить «Outlook». Изменения настроек операционной системы и приложений записываются в общедоступные файлы, поэтому их сохранение не происходит.

Таким образом, если включен контроль потоков данных, то при уровне сеанса, равном уровню конфиденциальности файла, все действия разрешены, кроме копирования информации в файлы с более низким уровнем конфиденциальности.

Попытайтесь скопировать файл «D:\temp\Конф.txt» на сменный носитель. Копирование не удастся, т.к. данному пользователю не было представлено право копирования конфиденциальной информации на сменный носитель.

4.4. Работа при уровне сеанса «Общедоступно»

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Общедоступно».

Попытайтесь открыть, удалить файл «D:\temp\Конф.txt», скопировать его в общедоступный каталог (например, «Рабочий стол») и на сменный носитель. При уровне сеанса «Общедоступно» любой доступ к конфиденциальной информации запрещён. В то же время доступ к общедоступной информации неограничен: запустите «Outlook», скопируйте общедоступный файл на сменный носитель.

Таким образом, за счёт подхода, основанного на контроле потоков данных, исключается возможность утечки конфиденциальной информации.

4.5. Копирование конфиденциальных файлов на сменный носитель

Войдите под учётной записью «Конфиденциальный». При первом входе необходимо настроить операционную систему, что возможно только при сеансе «Общедоступно», поэтому доступ к конфиденциальной информации запрещён (рис. 16).

Завершите сеанс и снова войдите под учётной записью «Конфиденциальный», выбрав уровень сеанса «Конфиденциально».

Скопируйте файл «D:\temp\Конф.txt» на сменный носитель. При

копировании появится предупреждение о потере файлом уровня конфиденциальности (рис. 17). Несмотря на потерю конфиденциальности, копирование будет разрешено, т.к. пользователю было предоставлено вывода конфиденциальной информации на сменные носители (рис. 4).

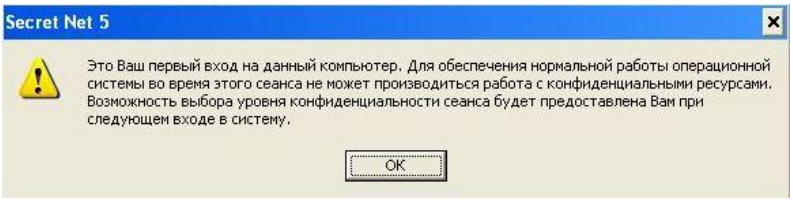

Рисунок 16 – Первый вход в операционную систему

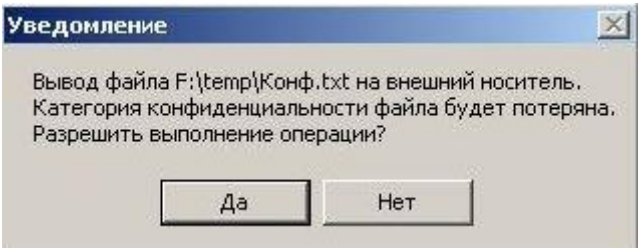

Рисунок 17 – Предупреждение о потере файлом конфиденциальности при копировании на сменный носитель

Задание

1. В соответствии с табл. 1 от имени администратора присвойте каталогам (находящимся в корне диска D:\) категории конфиденциальности.
2. В каждом каталоге создайте 2-4 документа от имени пользователя, допуск которого соответствует категории конфиденциальности каталога.
3. Проверьте возможность доступа к созданным документам.

Таблица 1 – Варианты заданий

Вари-ант	Каталог и его категория конфиденциальности		
	доступно	конфиденциально	секретно
1	D:\БД\Заказы	D:\БД\Поставщики	D:\БД\Клиенты
2	D:\Договоры\ Спонсоры	D:\Договоры\Инве-сторы	D:\Договоры\ Партнёры

3	D:\Документация\Отчёты	D:\Документация\ Приёмные документы	D:\Документация\ Информация о сотрудниках
4	D:\Подразделения\Отдел сбыта	D:\Подразделения\ Отдел кадров	D:\Подразделения \Финансовый отдел
5	D:\Файлы\ Пользователи	D:\Файлы\Опытные пользователи	D:\Файлы\ Администраторы
6	D:\БД\ Поставщики	D:\БД\Заказы	D:\БД\Клиенты
7	D:\Договоры\ Партнёры	D:\Договоры\ Спонсоры	D:\Договоры\ Инвесторы
8	D:\Подразделения\Отдел кадров	D:\Подразделения\ Финансовый отдел	D:\Подразделения \Отдел сбыта
9	D:\Файлы\ Опытные пользователи	D:\Файлы\ Пользователи	D:\Файлы\ Администраторы
10	D:\Документация\Приёмные документы	D:\Документация\ Отчёты	D:\Документация\ Информация о сотрудниках

Контрольные вопросы

1. На чём основан принцип действия мандатного механизма разграничения доступа?
2. Разрешается ли пользователю доступ к файлу, если уровень допуска пользователя выше категории конфиденциальности файла?
3. Что означает функция «Вывод конфиденциальной информации»?
4. Перечислите категории конфиденциальности по умолчанию.
5. Какой параметр предоставляет возможность управлять категориями конфиденциальности?
6. Можно ли присвоить категорию конфиденциальности ресурсу, расположенному на диске с файловой системой FAT32?
7. Поясните параметр «Автоматически присваивать новым файлам».
8. Для чего нужен контроль потоков данных?
9. При каком уровне сеанса пользователь может изменять настройки операционной системы и приложений?
10. Какие права предоставляются пользователю при доступе к конфиденциальной информации, уровень которой ниже уровня сеанса?

ЛАБОРАТОРНАЯ РАБОТА №5

РАЗГРАНИЧЕНИЕ ДОСТУПА К УСТРОЙСТВАМ

Целью данной работы является практическое изучение принципов разграничения доступа к устройствам на основе программного продукта DeviceLock.

В данной работе рассмотрены приложения, позволяющие администратору компьютера или домена контролировать доступ пользователей к дисководам, CD/DVD – приводам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа (съёмное устройство, принтеры, жёсткие диски и т.д). Некоторые устройства проверяются на обоих уровнях, в то время как другие – только на одном: либо на уровне интерфейса (порта), либо на уровне типа.

DeviceLock состоит из трёх частей:

– агента (DeviceLock Service). Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на компьютере-клиенте;

– сервера (DeviceLock Enterprise Server). Это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита;

– консоли управления. Это интерфейс контроля, который системный администратор использует для удалённого управления любой системой, на которой установлен агент.

Рассматриваемые утилиты и приложения:

– консоль управления DeviceLock Management Console. С её помощью можно просматривать и изменять разрешения и правила аудита, устанавливать DeviceLock Service, а также просматривать журналы аудита и теневого копирования для отдельных компьютеров.

Ход работы

1. Настройка DeviceLock Management Console

Войдите под учётной записью «Администратор». Запустите «DeviceLock Management Console»: «Пуск – Программы – DeviceLock» (рис. 1). Доступ к консоли можно также получить через «MMC», добавив оснастку «DeviceLock Management Console».

Подключите консоль «DeviceLock Management Console» к управляемому компьютеру. Для этого в контекстном меню «Сервис DeviceLock» выберите «Подключиться…» (рис. 2). Дополнительно включите настройку «Подключаться к локальному компьютеру при запуске» для автоматического подключения сервиса.

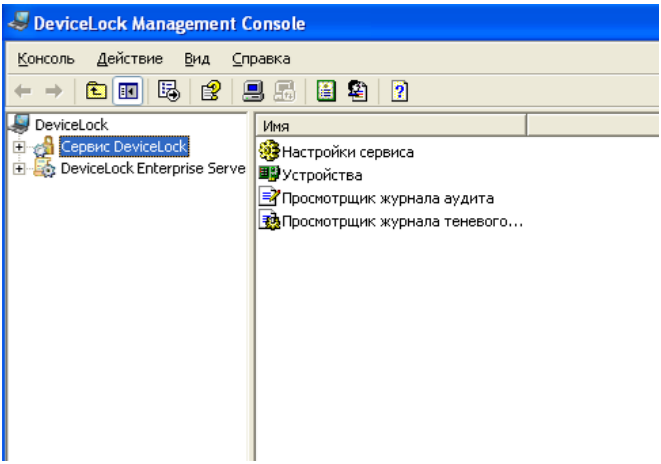

Рисунок 1 – «DeviceLock Management Console»

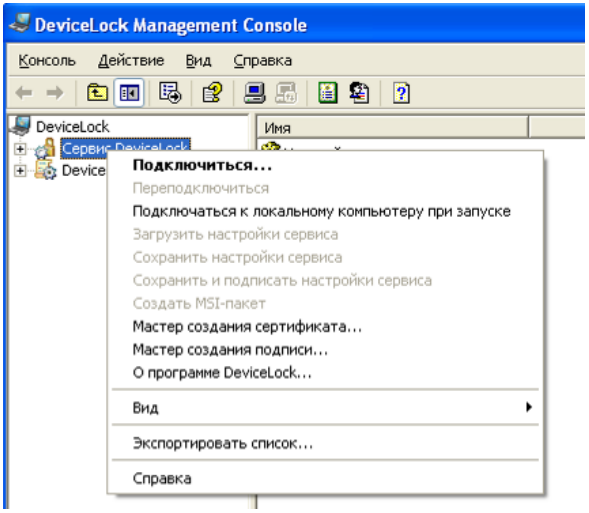

Рисунок 2 – Подключение консоли DeviceLock

Перейдите во вкладку «Настройка сервиса – Администраторы DeviceLock». Добавьте в качестве администратора DeviceLock учётную запись «Администратор» (рис. 3). В данной вкладке можно добавить и других пользователей с возможностью ограничения доступа к оснастке (полный доступ, изменение, только чтение). Пользователи, не внесённые в список, не будут иметь доступ к оснастке управления разграничением доступа к устройствам.

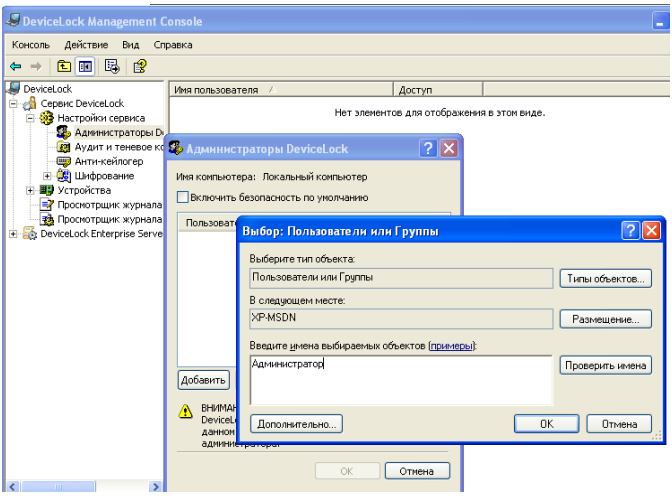

Рисунок 3 – Добавление администратора DeviceLock

2. Разграничение доступа к устройствам

Когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС. В зависимости от типа устройства и интерфейса подключения (например, USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке – «доступ запрещён».

Перейдите в раздел «Устройства – Разрешения» (рис. 4)

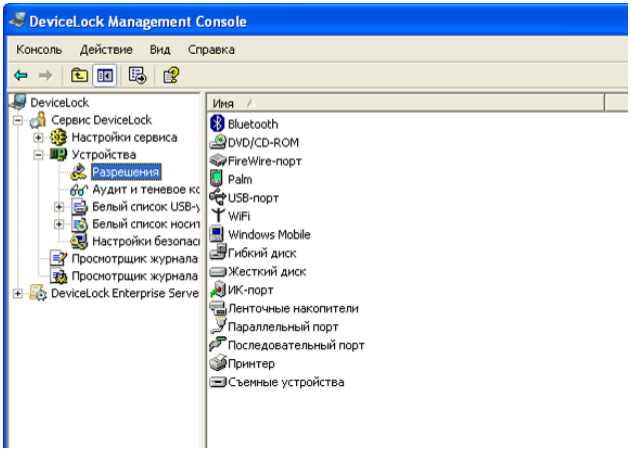

Рисунок 4 – Разрешения для устройств

Запретите доступ учётной записи «user» к приводу DVD/CD-ROM (рис. 5). Если на ПК установлено несколько CD/DVD-приводов, то можно воспользоваться белым листом устройств, для того чтобы выбрать определённый носитель.

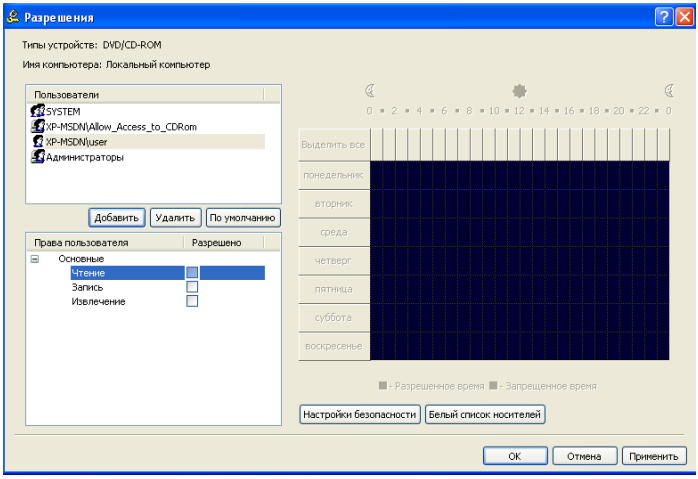

Рисунок 5 – Разрешения для DVD/CD-ROM

Войдите под учётной записью «user». Убедитесь что доступ к CD/DVD – приводу запрещен.

Под учётной записью «Администратор» разрешите пользователю «user» только чтение файлов со съёмных носителей (рис. 6).

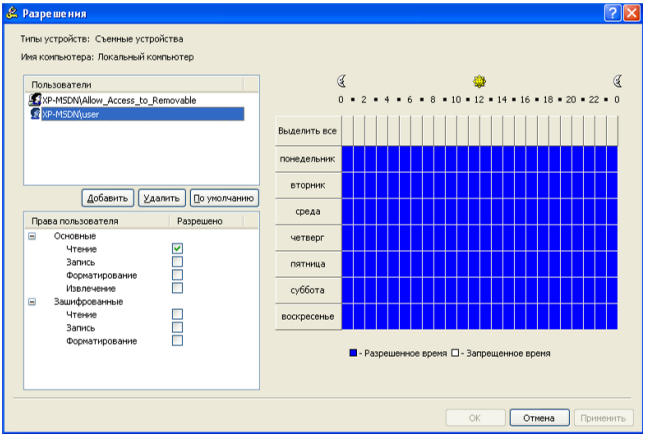

Рисунок 6 – Разрешения для съемных устройств

Примечания:

– если пользователь входит в какую-либо группу и у этой группы стоит полный доступ к устройству, то режим только чтение не будет работать (это связано с тем, что разрешения суммируются);

– если учётную запись не добавить в разрешения, то доступ ей будет запрещён.

Войдите под учётной записью «user».

Подключите съёмный носитель и убедитесь, что запись на него невозможна.

DeviceLock предоставляет возможность разграничения доступа к устройствам по дням недели и времени суток.

Войдите под учётной записью «Администратор» и установите пользователю «user» полный доступ к съёмным устройствам в будние дни с 8:00 до 17:00 либо на время занятий (рис. 7).

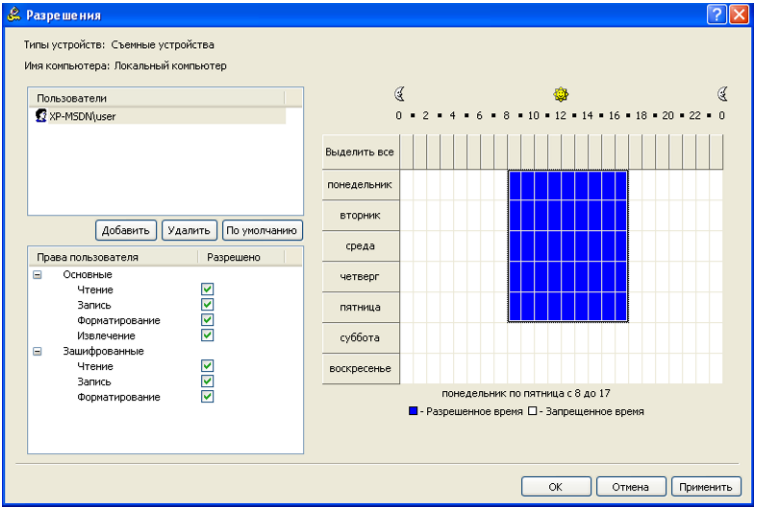

Рисунок 7 – Разграничения доступа к устройствам по дням недели и времени суток

Войдите под учётной записью «user». Подключите съёмный носитель и убедитесь, что доступ к нему разрешён.

Под учётной записью «Администратор» измените системное время на воскресенье.

Войдите под учетной записью «user» и проверьте запрет доступа к съёмному носителю.

3. Белый список устройств

Под учётной записью «Администратор» запретите доступ к USB-порту учётной записи «user» (рис. 8).

В случае с USB-устройствами DeviceLock в первую очередь проверит разрешения на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку «Windows» определяет USB-флэш как съёмное устройство, DeviceLock также проверит ограничения на уровне типа устройства (съёмное устройство). Под учётной записью «user» проверьте запрет доступа к съёмному носителю.

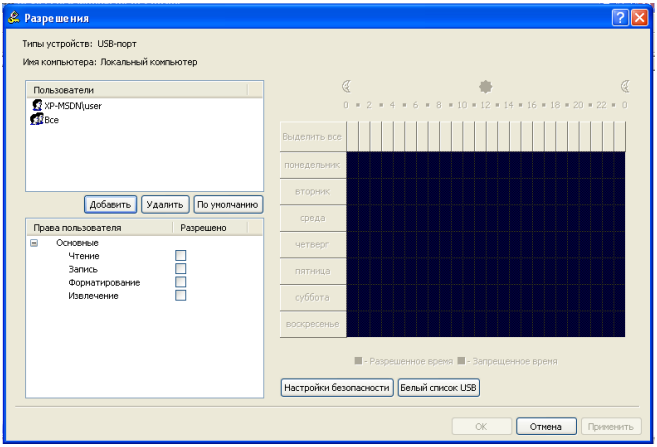

Рисунок 8 – Разрешения для USB-порта

Так как разграничению доступа подвергаются все USB-устройства, возникает необходимость делать исключения для USB-устройств, разрешённых к использованию в организации.

Исключения можно указывать двумя способами:

– через «Настройки безопасности» (рис. 9);

– через «Белый список» на основе идентификации модели или конкретного экземпляра устройства.

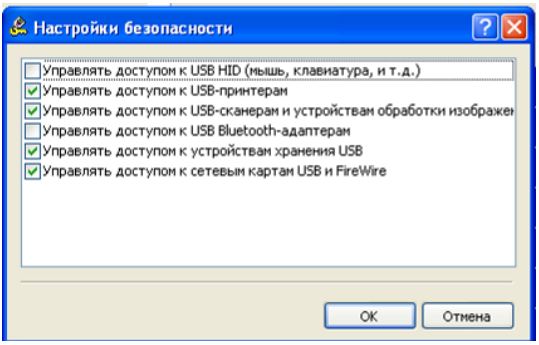

Рисунок 9 – Настройки безопасности

Если в «Настройках безопасности» включить настройки управления каким-либо классом устройств, то к устройствам этого класса применяется разграничение доступа. Если настройка отключена, то использовать устройства данного класса могут все пользователи.

При использовании белого списка есть два варианта идентификации устройств:

1) Device Model – описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).

Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.

2) Unique Device – описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.

Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Перед тем как устройство может быть авторизовано через белый список, оно должно быть добавлено в базу данных. Перейдите во вкладку «Устройства – Белый список USB», в контекстном меню выберите «Управление». В появившемся окне (рис. 10) перейдите в «Базу данных USB-устройств».

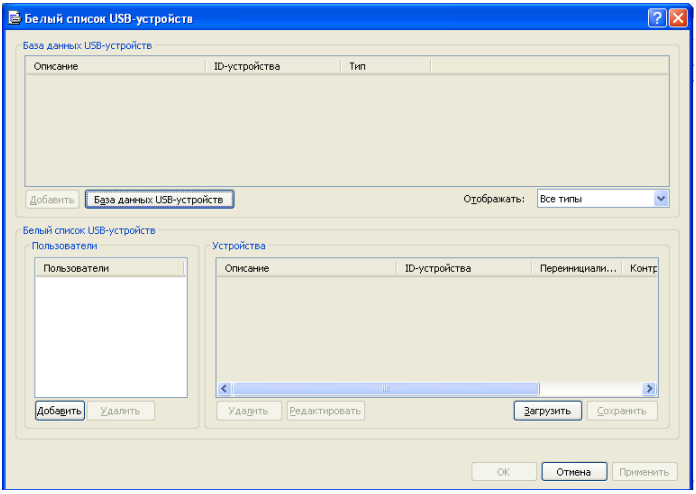

Рисунок 10 – Белый список USB-устройств

Добавьте в «Базу данных устройств» те USB-устройства, к которым необходимо разрешить доступ, выбрав устройство и нажав кнопку «Добавить» (рис. 11).

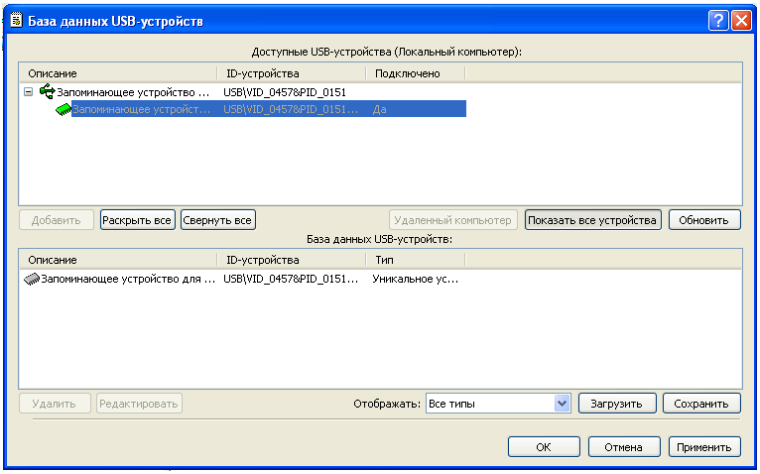

Рисунок 11 – База данных USB-устройств

Разрешите пользователю «user» доступ к USB-устройству из базы данных. Для этого добавьте учётную запись «user» и из «Базы данных USB-устройств» выберите необходимые устройства (рис. 12).

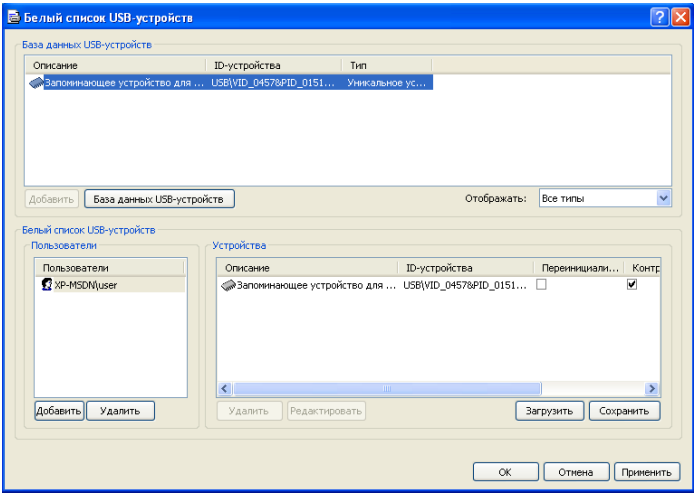

Рисунок 12 – Добавление устройства в белый список пользователя

4. Аудит использования устройств

Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств пользователями на локальном компьютере.

Чтобы включить протоколирование действий пользователя, необходимо установить соответствующие права аудита.

1) Чтение/запись – протоколируются попытки пользователя читать/записывать данные. Для типов устройств «Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, последовательный порт, USB-порт и WiFi».

2) Печать – протоколируются попытки пользователя посылать документы на принтеры. Применимо только к типу «Принтер».

3) Выполнение – протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Применимо только к типу «Windows Mobile».

4) Чтение/запись не файлов – протоколируются попытки пользователя читать/записывать не файловые объекты (календарь, контакты, задачи и т.п.). Применимо только к типам «Windows Mobile» и «Palm».

Существует возможность протоколировать успешный доступ к устройствам и ошибки доступа:

1) «Аудит разрешений» – все попытки доступа, которые были разрешены DeviceLock, т.е. пользователю был предоставлен доступ к устройству.

2) «Аудит запретов» – все попытки доступа, которые были заблокированы DeviceLock, т.е. пользователю был запрещён доступ к устройству.

Перейдите в раздел «Устройства – Аудит и теневое копирование». Примените к съёмным устройствам аудит для пользователя «user» (рис. 13).

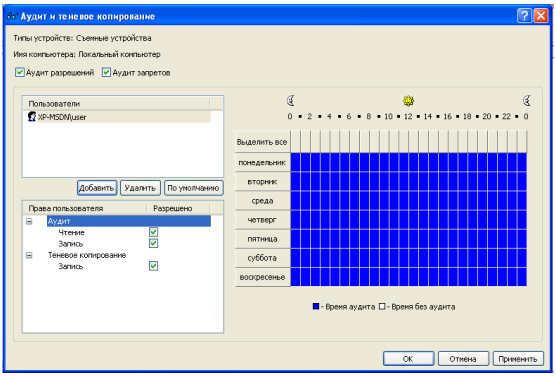

Рисунок 13 – Настройка аудита для съёмных устройств

Убедитесь, что пользователю «user» разрешён доступ к съёмным устройствам. Войдите под учётной записью «user», подключите съёмное устройство и скопируйте на него образцы рисунков «Windows» из каталога «*\Мои документы\Мои рисунки\Образцы рисунков».

Войдите под учётной записью «Администратор».

Доступ к результатам аудита можно получить во вкладке «Просмотрщик журнала аудита» (рис. 14).

Журналы аудита могут храниться как в стандартных журналах ОС «Windows», так и в журналах DeviceLock. Перейдите во вкладку «Настройка сервиса – Аудит и теневое копирование» (рис. 15).

Опция – «Тип журнала аудита» устанавливает вид журнала и может принимать три значения:

- «Журнал событий» – данные аудита записываются только в стандартный журнал «Windows», хранящийся на локальном компьютере;
- «Журнал DeviceLock» – данные аудита записываются только в собственный защищённый журнал, отсылаемый на DeviceLock Enterprise Server для централизованного хранения;
- «Журнал событий и DeviceLock» –запись в оба журнала.

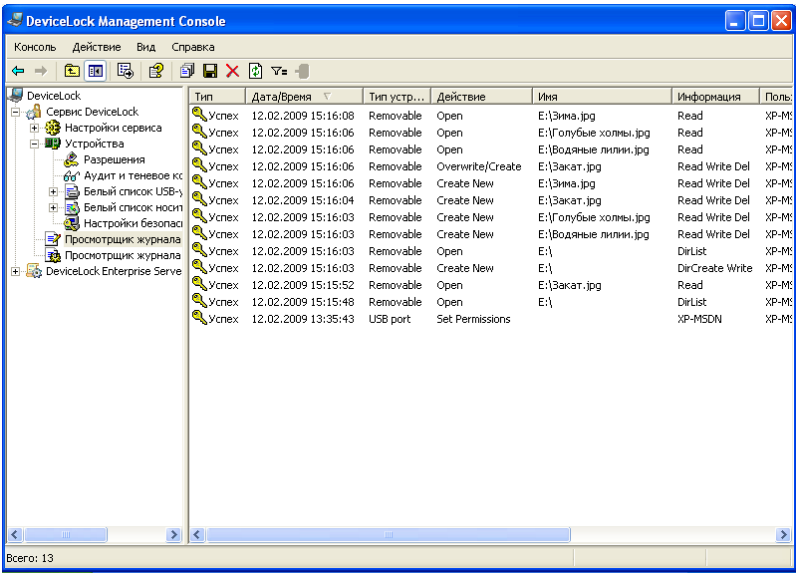

Рисунок 14 – Просмотрщик журнала аудита

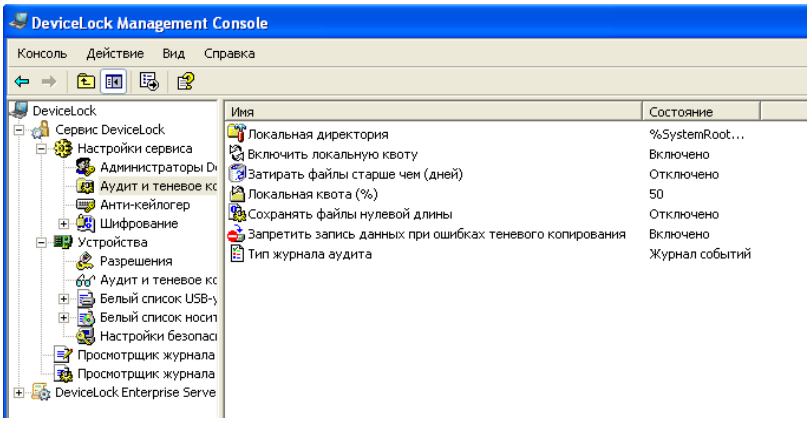

Рисунок 15 – Вкладка «Настройка сервиса – Аудит и теневое копирование»

Для того чтобы просмотреть журнал аудита через стандартный журнал «Windows», запустите консоль управления «Пуск – Выполнить – MMC». В ней добавьте оснастку «Просмотр событий». Вкладка «DeviceLock Log» предоставляет журнал аудита (рис. 16).

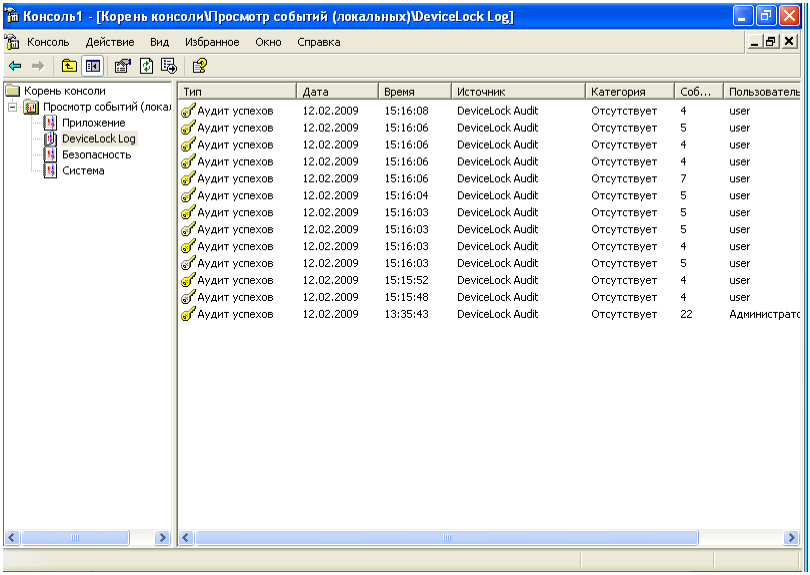

Рисунок 16 – Вкладка «Devicelock Log»

5. Теневое копирование файлов

Теневое копирование позволяет сохранять копии всех файлов, которые пользователь копирует на съёмные носители или отправляет

на печать. Сохранённые файлы могут быть в дальнейшем проанализированы на предмет наличия в них конфиденциальной информации.

Перейдите в раздел DeviceLock «Устройства – Аудит и теневое копирование». Включите для пользователя «user» теневое копирование файлов на съёмные устройства (рис. 17).

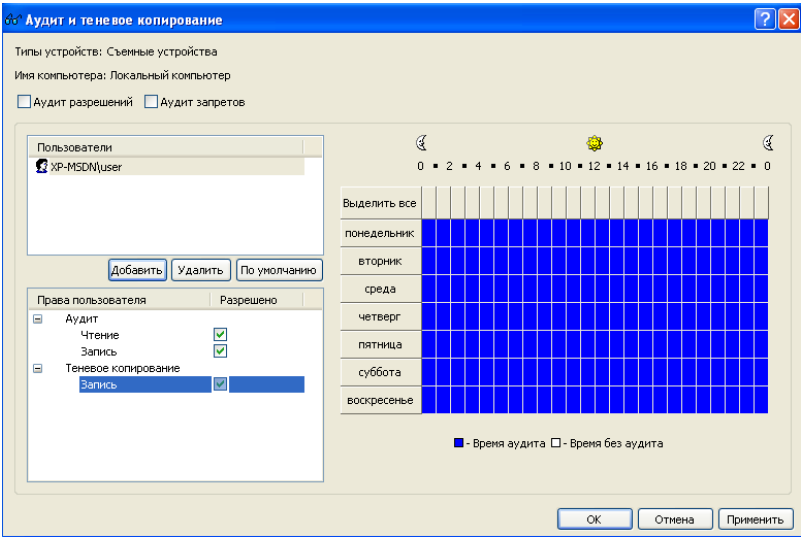

Рисунок 17 – Включение теневого копирования для съёмных устройств

Под учётной записью «user» подключите съёмное устройство и скопируйте на него текстовый или графический файл.

Под учётной записью «Администратор» откройте раздел DeviceLock «Просмотрщик журнала теневого копирования» (рис. 18).

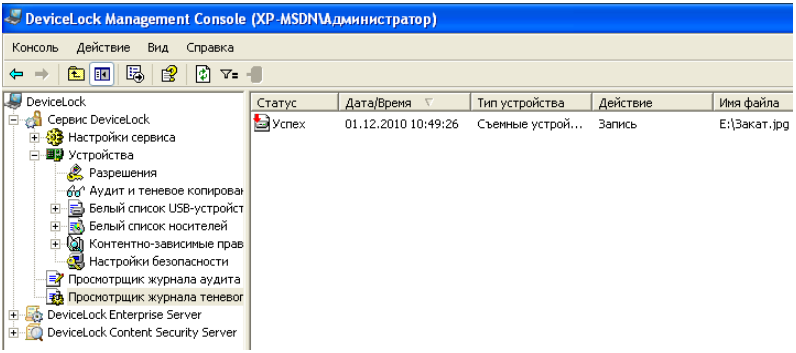

Рисунок 18 – Просмотрщик журнала теневого копирования

Откройте появившуюся в журнале запись. Это позволит увидеть содержимое файла, скопированного пользователем «user» на съёмное устройство.

Выбор места хранения теневых копий файлов возможен в разделе «Настройки сервиса – Аудит и теневое копирование – Локальная директория» (рис. 19).

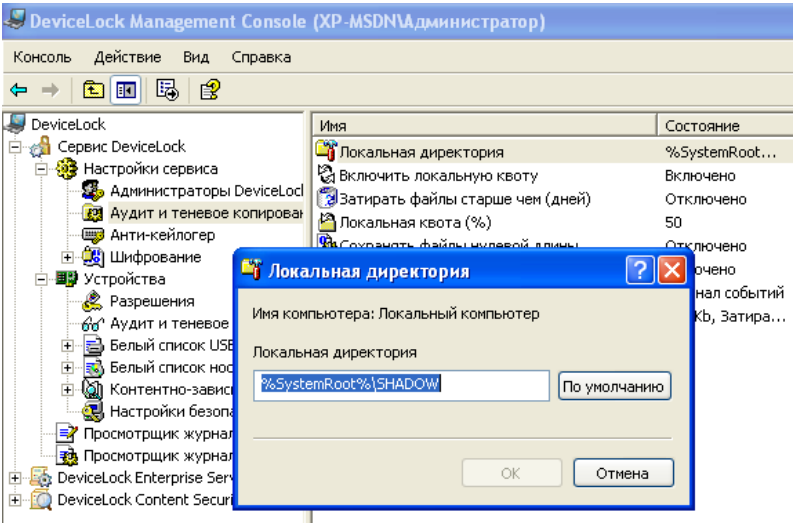

Рисунок 19 – Каталог хранения для теневого копирования

Задание

Учётной записи «user» установите разрешения в соответствии с вариантом.

Вариант 1

DVD/CD-ROM	Принтер	Жёсткий диск
Только чтение. Добавьте один носитель в белый список. Полный доступ к виртуальным приводам	Доступ по будням. Аудит печати и запретов доступа	Полный доступ. Аудит чтения и записи

Вариант 2

Съёмные устройства	USB-порт	WIFI
Чтение и извлечение	Аудит всех событий	Доступ по будням

Вариант 3

Съёмные устройства	USB-порт	DVD/CD-ROM
Чтение и извлечение	Запрет доступа к сканерам, принтерам, устройствам хранения usb. Добавьте 3 устройства в белый список	Доступ только по будням с 17 до 19 часов. Аудит записи и разрешений

Вариант 4

WindowsMobile	Съёмные устройства	USB-порт
Только чтение. Аудит всех событий	Запрет доступа вне рабочего времени	Только чтение. Добавить в белый список 2 устройства

Вариант 5

Параллельный порт	Жёсткий диск	Съёмные устройства
Запрет доступа.	Доступ по будням с 8 до 20 часов.	Чтение и извлечение. Аудит всех событий.

Вариант 6

DVD/CD-ROM	WindowsMobile	Съёмные устройства
Только чтение. Аудит всех событий.	Доступ без ограничений. Аудит всех событий.	Чтение и извлечение. Аудит всех событий вне рабочего времени.

Вариант 7

Последовательный порт	USB-порт	Принтер
Запрет доступа вне рабочего времени. Доступ к модемам, подключаемым через данный порт, без ограничений.	Запрет доступа. Добавить 4 устройства в белый список.	Доступ с 8 до 18 часов. Аудит всех событий.

Вариант 8

Bluetooth	Параллельный порт	WindowsMobile
Доступ без ограничений.	Доступ по будням.	Доступ без ограничений. Аудит записи.

Вариант 9

DVD/CD-ROM	USB-порт	Жёсткий диск
Только чтение.	Чтение, извлечение. Добавить в белый список 3 устройства.	Аудит всех событий.

Вариант 10

FireWire-порт	WIFI	Съёмные устройства
Только чтение. Аудит записи и запретов.	Доступ в рабочее время. Аудит чтения и записи.	Запрет доступа. Аудит запретов.

Контрольные вопросы

1. Существует ли возможность разграничения доступа к управлению приложением DeviceLock?
2. В чём отличие уровня интерфейса от уровня типа устройств?
3. Какие функции разграничения доступа к ресурсам предоставляет DeviceLock?
4. Каким образом можно исключить классы USB-устройств (например, мыши, клавиатуры и т.п.) из механизма разграничения доступа?
5. Для чего используются белые списки?
6. К каким классам устройств могут быть созданы белые списки?
7. Какие варианты идентификации устройства применяются в белом списке?
8. Для чего используется база данных устройств?
9. Где могут храниться журналы аудита работы с устройствами?
10. Для чего используется теневое копирование файлов?

ЛАБОРАТОРНАЯ РАБОТА №6

ОГРАНИЧЕННОЕ ИСПОЛЬЗОВАНИЕ ПРОГРАММ

Целью данной работы является ознакомление и практическое применение встроенных средств ограничения использования программ в ОС Windows XP Professional.

Политики ограниченного использования программ позволяют осуществлять идентификацию программ, запускаемых в ОС семейства Windows и управлять возможностью их выполнения на локальном компьютере.

Политики ограниченного использования программ (ПОИП) – это вид политик безопасности, который позволяет администраторам разрешить или запретить использовать программные приложения. Применение основано на использовании алгоритма хеширования файла, связи путей файлов с программным обеспечением, сертификата издателя программного обеспечения или зоны Интернета, в которой работает программное обеспечение.

Ход работы

1. Войдите в ОС под учетной записью администратора и перейдите по следующему пути: «Панель управления - Администрирование - Локальная политика безопасности», далее в дереве консоли раскройте узел «Политики ограниченного использования программ» (рис. 1). Также доступ к политикам ограниченного использования программ (далее ПОИП) можно получить через добавление оснастки «Локальные параметры безопасности» в консоль управления. Через контекстное меню создайте новую политику.

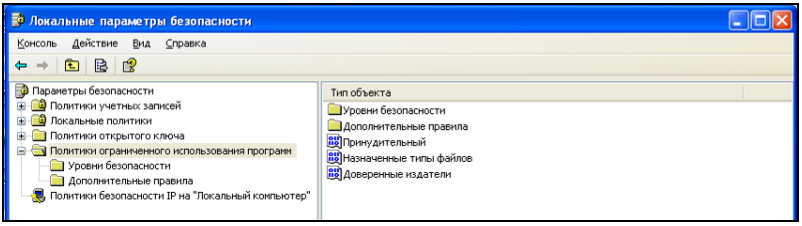

Рисунок 1 - Локальные параметры безопасности

2. Раскройте объект «Уровни безопасности» (рис. 2) в который включены два уровня: «Не разрешено», означающее запрет на запуск любого ПО, кроме разрешённого в ПОИП и «Неограниченный», означающий возможность работы с ПО в соответствии с правами пользователя. Уровень, используемый по умолчанию, обозначается «», чтобы его изменить дважды кликните на уровень безопасности и

выберите пункт «По умолчанию». Установите уровень «Неограниченный», в качестве уровня безопасности по умолчанию.

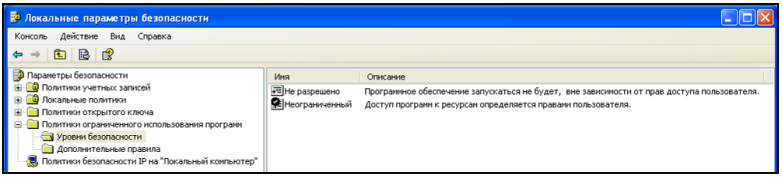

Рисунок 2 - Выбор уровня безопасности

3. Чтобы применить ПОИП к локальным администраторам, дважды кликните тип объекта «Принудительный» и выберите «Для всех пользователей» (рис. 3). Здесь же настраивается возможность исключать применение ПОИП к библиотекам программ, таких как DLL, которые могут использоваться другими разрешенными программами. Установите применение ПОИП ко всем пользователям и файлам.

4. В пункте «Назначенные типы файлов» раздела «Политики ограниченного использования программ» уже имеется список назначенных типов файлов, используемый для всех правил. Для того, чтобы определить с какими типами файлов будет работать ПОИП выберите пункт «Назначенные типы файлов», в появившемся окне (рис. 4) в поле «Расширение:» введите требуемое расширение, например, «exe». Таким образом, добавляются новые типы файлов, которые учитываются в правиле для пути.

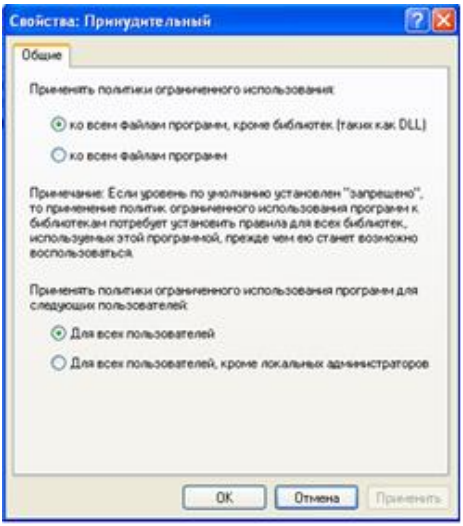

Рисунок 3 - Настройка дополнительных параметров

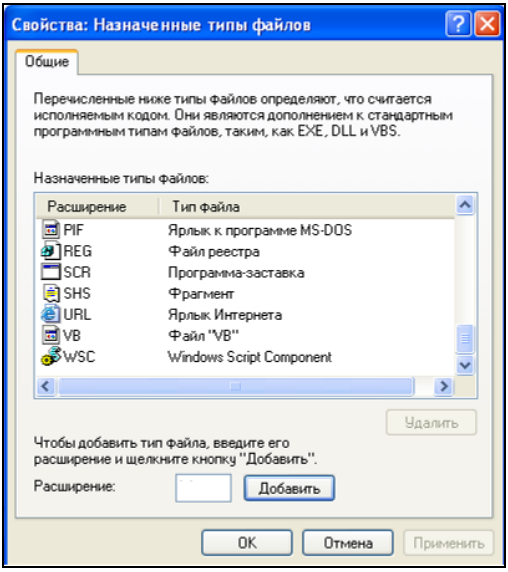

Рисунок 4 - Список файловых типов ПОИП

5. Перейдите в пункт «Дополнительные правила» (рис. 5) в нем уже имеются четыре правила пути. Они обеспечивают запуск ОС при выбранном по умолчанию уровне безопасности «Не разрешено». В меню выберите «Действие», далее «Создать правило для хеша…», в появившемся окне (рис. 6) при помощи кнопки «обзор» укажите файл, работу с которым вы хотите запретить, например, «utorrent.exe», информация о нем заполнится автоматически. Также можно вносить само значение хеша, рассчитанное другим пользователем, например, хеш вируса.

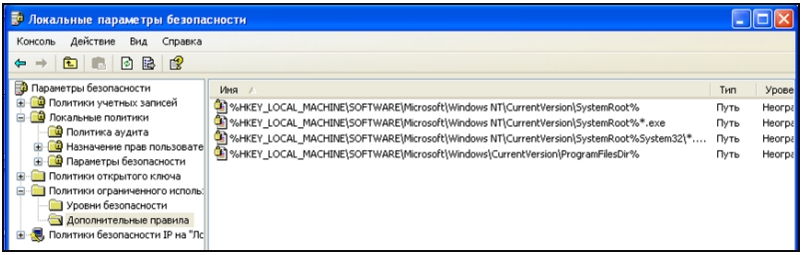

Рисунок 5 - Вкладка «Дополнительные правила»

Запустите файл «utorrent.exe», после чего отобразится сообщение (рис. 7), информирующее пользователя о запрете запуска файла.

Необходимо помнить, что любые изменения в файле приводят к изменению хеша.

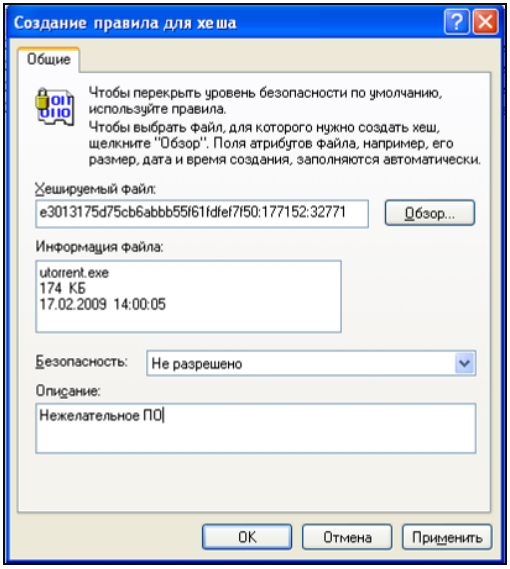

Рисунок 6 - Создание правила для хеша

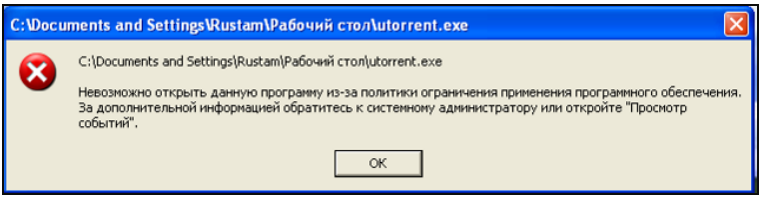

Рисунок 7 - Сообщение о запрете открытия

6. По аналогии с правилом хеша создайте правило пути. В появившемся окне (рис. 8) в поле «Путь:» введите путь к файлам, работу с которыми нужно ограничивать, например: «%programfiles%\Messenger» и выберите уровень безопасности «Не разрешено». Путь можно указывать и к конкретному файлу, а так же использовать подстановочные знаки «*» и «?», например: «c:\downloads*.*».

Попробуйте запустить программу обмена сообщений «Windows Messenger». Убедитесь в запрете запуска.

В правиле для пути имеется возможность использовать системные переменные, такие как «%programfiles%», «%systemroot%», «%userprofile%», «%windir%», «%appdata%» и «%temp%», а так же переменные окружения. Переменные окружения создаются

следующим образом: в свойствах системы по пути «Пуск – Панель управления – Свойства системы» во вкладке «Дополнительно», нажмите на кнопку «Перменные среды». Далее в появившемся окне (рис. 9) нажмите кнопку «Создать». Введите имя переменной, например, «Share» и значение переменной «C:\Documents and Settings\All Users\Документы». Создайте и проверьте правило пути, применив переменную «%Share%».

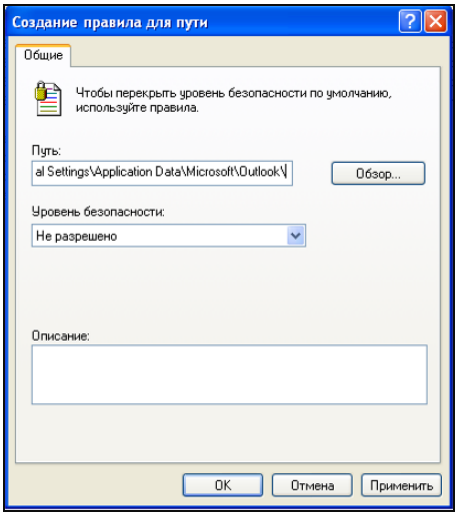

Рисунок 8 - Создание правила для пути

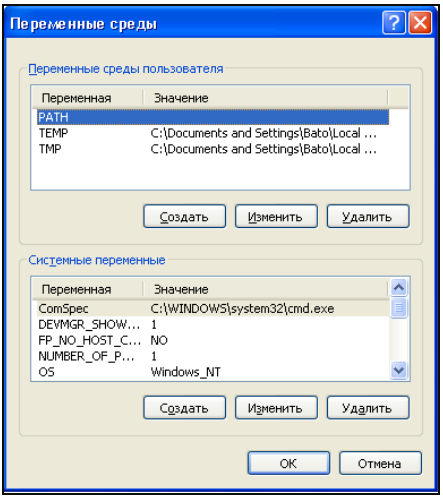

Рисунок 9 - Создание переменных окружения

7. Создаваемые «Правила для зоны Интернета…» применяются только к пакетам установщика программ Windows, добавление зон происходит с помощью свойств обозревателя «Internet Explorer» во вкладке безопасность.

8. Перед созданием правила для сертификата получите сертификат следующим образом: выберите, например, в свойствах файла программы «bootvis.msi», вкладку «Цифровые подписи» (рис. 10). Далее нажмите кнопку «Сведения» в появившемся окне (рис. 11) нажмите кнопку «Просмотр сертификата». Сертификат должен быть действителен. В появившемся окне (рис. 12) выберите вкладку «Состав» и нажмите кнопку «Копировать в файл…», при помощи мастера экспорта сертификатов сохраните сертификат, например, под именем «Microsoft.cer» (формат сохранения – X.509).

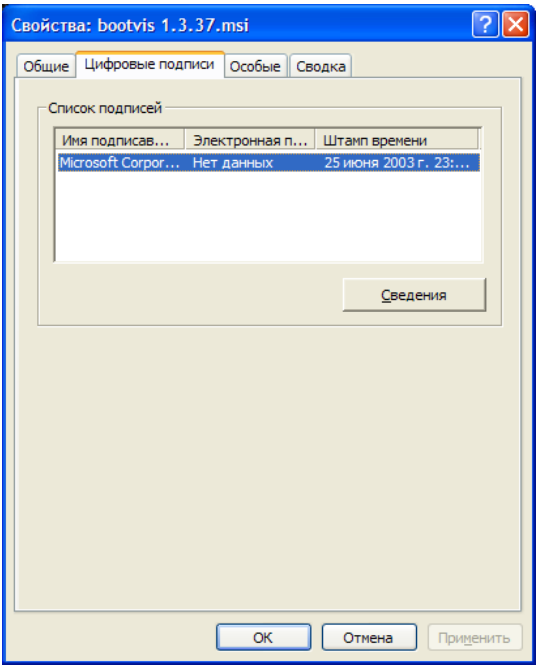

Рисунок 10 - Цифровые подписи файла

Назначьте по умолчанию уровень безопасности «Не разрешено». Далее в дополнительных правилах создайте «Правило для сертификата…», в появившемся окне (рис. 13) укажите путь к сохраненному файлу сертификата «Microsoft.cer» и выставите уровень безопасности «Неограниченный». Скопируйте файл «bootvis.msi» в папку «C:\Documents and Settings\All Users\Документы». При попытке

запустить установочный пакет, подписанный данным сертификатом, выполнится приоритет правила сертификата над правилом пути. Проверьте возможность запуска. Правило сертификатов также может ограничить запуск подписанных программ с переносных носителей информации.

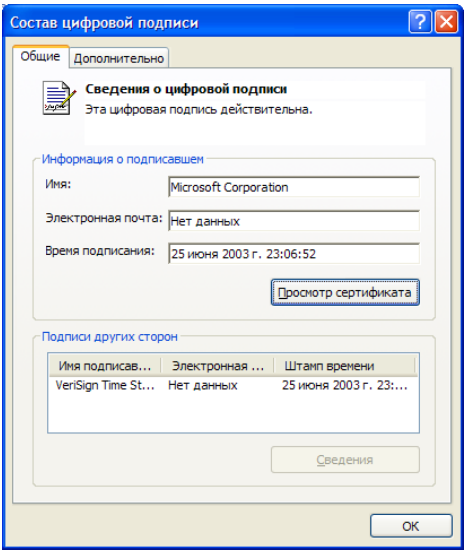

Рисунок 11 - Состав цифровой подписи файла

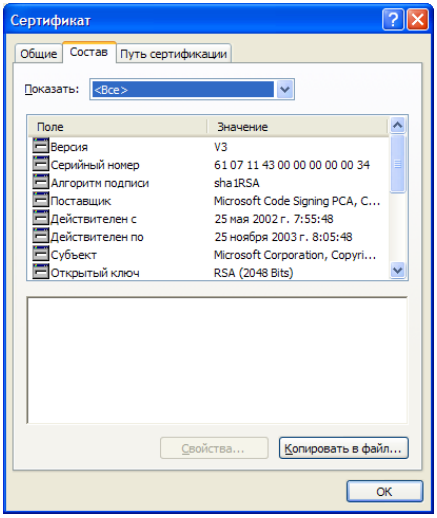

Рисунок 12 – Сертификат

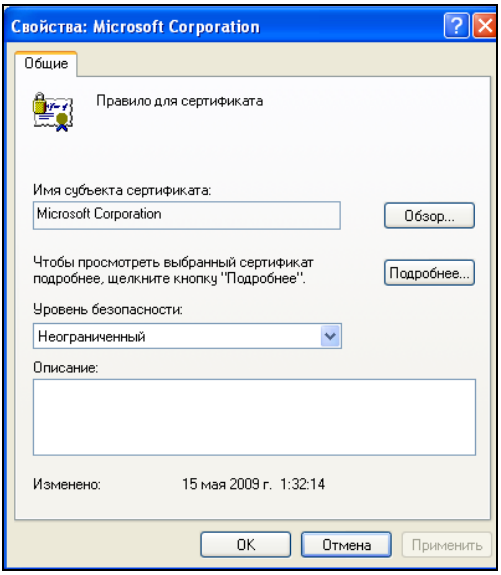

Рисунок 13 - Окно правила для сертификата

9. Для разрешения конфликтов, возникающих при использовании нескольких правил, используется приоритет. Ниже перечислены правила в порядке убывания приоритета.

1) Правило для хеша.
2) Правило для сертификата.
3) Правило для пути. При конфликте правил для пути приоритет имеет правило с большим ограничением. Ниже приведен набор путей в порядке от высшего приоритета (наибольшее ограничение) к низшему приоритету.

– диск:\папка1\папка2\имя_файла.расширение
– диск:\папка1\папка2*.расширение
– *.расширение
– диск:\папка1\папка2\
– диск:\папка1\

4) Правило для зоны Интернета.

При конфликте двух похожих правил для пути приоритет имеет правило с большим ограничением. Например, если имеется правило для пути «C:\Windows\» с уровнем безопасности «Не разрешено» и правило для пути «%windir%» с уровнем «Неограниченный», будет применяться более строгое правило с уровнем безопасности «Не разрешено».

В качестве примера создайте разрешающее правило хеша для программы «calc.exe», расположенного по запрещенному пути

«c:\downloads». Далее попытайтесь запустить эту программу из ранее запрещенного пути. Приоритет правила для хеша позволит запустить программу из этой папки.

Удалите все созданные правила перед выполнением задания.

Задание

Таблица 1 – Распределение заданий по вариантам

Номер варианта	Задания
1	с а по д
2	с б по е
3	с в по ж
4	с г по з
5	с д по и
6	с е по к
7	с ж по л
8	с з по м
9	с к по о
10	с л по п

1. Создайте следующую политику ограничения использования программ, которая будет удовлетворять следующим требованиям, согласно вашему варианту (табл. 1):

а) разрешает запуск ПО, подписанного сертификатом от «Microsoft»;

б) применяется ко всем пользователям, включая локальных администраторов;

в) не ограничивает использование программных библиотек, таких как «DLL»;

г) право выбора доверенных издателей разрешено только локальным администраторам;

д) запрещает запуск любых программ в качестве уровня безопасности по умолчанию;

е) разрешает запуск любых программ из папок: «C:\WINDOWS», «C:\Program Files», «C:\Documents and Settings\LocalService», «C:\Documents and Settings\All Users»;

ж) разрешает запуск любых программ пользователю из своей папки «C:\Documents and Settings\user» (где user – имя любого пользователя) при помощи переменной окружения;

з) при помощи приоритета правил пути пользователю запрещено запускать любые программы из папок других пользователей, как например, «C:\Documents and Settings\Администратор»;

и) разрешает установку ПО, подписанного сертификатом от «Microsoft»;

к) запрещает запуск программ «Паук», «Сапер» и «utorrent.exe» вне зависимости от их месторасположения;

л) запрещает запуск файла с именем «AUTORUN.INF» из любого места;

м) применяется ко всем пользователям, исключая локальных администраторов;

н) ограничивает использование программных библиотек, таких как «DLL»;

о) право выбора доверенных издателей разрешено любым пользователям;

п) запрещает установку ПО, подписанного сертификатом от «Microsoft».

2. Проверьте все созданные правила при помощи стандартного проводника «Explorer» и стороннего файлового менеджера, как например, «Far manager» или «Total Commander», игнорируют ли они ПОИП?

Контрольные вопросы

1) Как создать политику ограниченного использования программ?
2) Возможно ли исключение из ПОИП локальных администраторов?
3) Для чего служит пункт «Назначенные типы файлов»?
4) В чем основное преимущество правила хеша перед правилом пути?
5) Приведите пример, когда запрещенная правилом хеша программа может выполниться.
6) Для чего служит правило для сертификата?
7) Как можно получить сертификат из файла?
8) Приведите три примера использования приоритета правил.
9) Как запретить открытие любых файлов с расширением «.swf» из любого места на жестком диске?
10) Объясните различие между уровнями безопасности «Неограниченный» и «Не разрешено».

ЛАБОРАТОРНАЯ РАБОТА №7

АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Целью данной работы является ознакомление с интерфейсом управления подсистемой аудита безопасности и параметрами политики аудита на примере операционной системы Windows XP.

Ход работы

1. Политика аудита

Политика аудита определяет, какие категории сообщений о событиях отслеживаются и сохраняются в журнале безопасности. Настройка политики происходит при помощи оснастки «Локальная политика безопасности».

Войдите в операционную систему под учётной записью «Администратор». Откройте оснастку «Локальная политика безопасности» («Пуск – Панель управления – Администрирование»). Выберите раздел «Локальные политики – Политика аудита» (рис. 1).

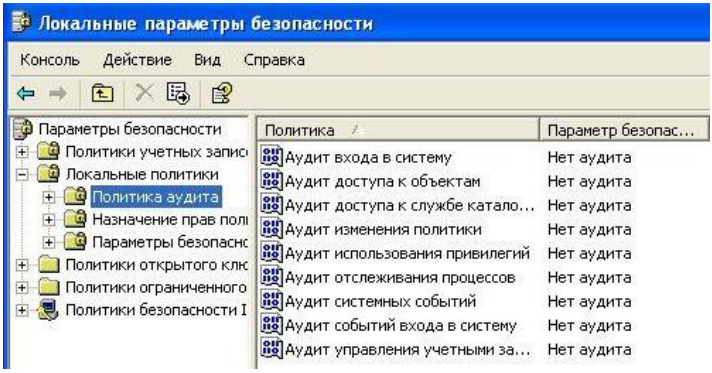

Рисунок 1 – Политика аудита Windows XP

В политике аудита представлен набор параметров, соответствующих различным категориям событий безопасности. В «Свойствах» каждого из параметров возможно включение фиксации событий, относящихся к соответствующей категории. Откройте параметр политики аудита «Аудит входа в систему» (рис.2). Включение аудита происходит по следующим типам событий:

- «Успех» – фиксируются события, осуществление которых было разрешено пользователю;
- «Отказ» – фиксируются события, осуществление которых было запрещено пользователю.

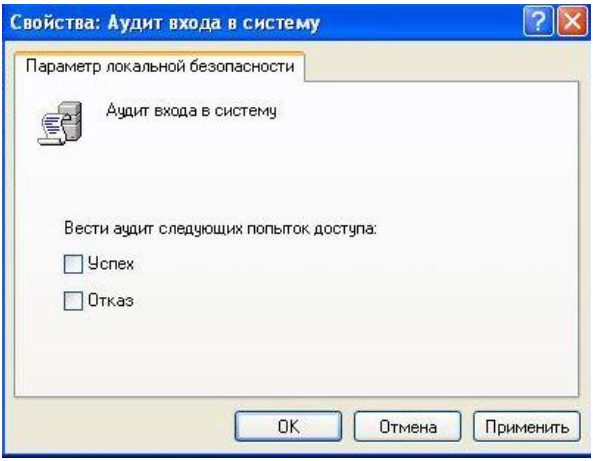

Рисунок 2 – Настройки параметра «Аудит входа в систему»

2. Аудит входа/выхода пользователей

Параметр «Аудит входа в систему» включает фиксацию каждой попытки входа пользователя в систему или выхода из неё на данном компьютере. Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит входа в систему».

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит событий входа в систему». Параметр «Аудит событий входа в систему» включает фиксацию каждой проверки данным компьютером учётных данных (в т.ч. контроллером домена при входе в домен на рабочей станции).

Завершите сеанс текущего пользователя. Введите неверный пароль при входе в операционную систему, чтобы сгенерировать событие типа «Отказ».

Войдите под учётной записью «Администратор». Откройте журнал «Безопасность» оснастки «Просмотр событий» (рис. 3).

Рисунок 3 – Журнал «Безопасность»

Записи журнала «Безопасность» включают в себя следующую информацию о событии: время и дата события; имя учётной записи пользователя, сгенерировавшего событие; имя компьютера, на котором произошло событие; категорию и тип события; код события; дополнительную информацию в зависимости от категории события.

В журнале «Безопасность» откройте запись категории «Вход/выход» типа «Аудит отказов». Данная запись описывает событие, сгенерированное при вводе неправильного пароля (рис. 4). Так как пользователь ещё не прошёл аутентификацию, событие было сгенерировано от имени пользователя «System». В записи о событии указывается имя пользователя, использовавшееся при осуществлении неудачной попытки входа в систему, и тип входа. Код данного события – 529.

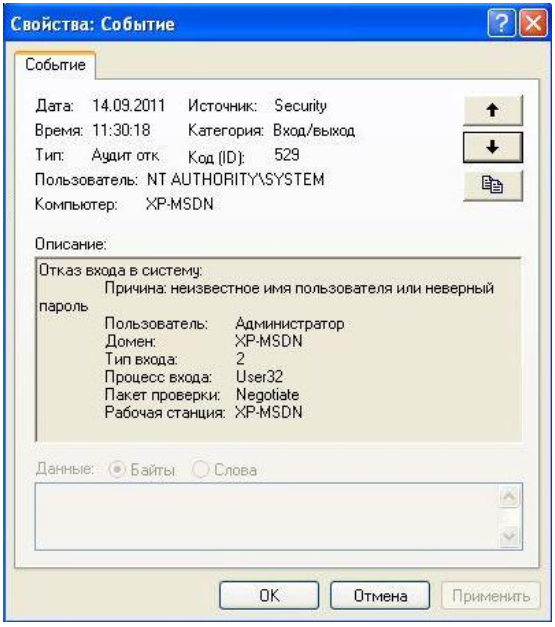

Рисунок 4 – Запись аудита об отказе входа в операционную систему

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 528. Данная запись описывает событие, сгенерированное при удачном входе в операционную систему (рис. 5).

В обеих записях (аудита успехов и отказов) указан тип входа в систему – 2. Этот тип означает интерактивный вход в систему. Типы входа в систему, фиксируемые в Windows XP, приведены в табл. 1.

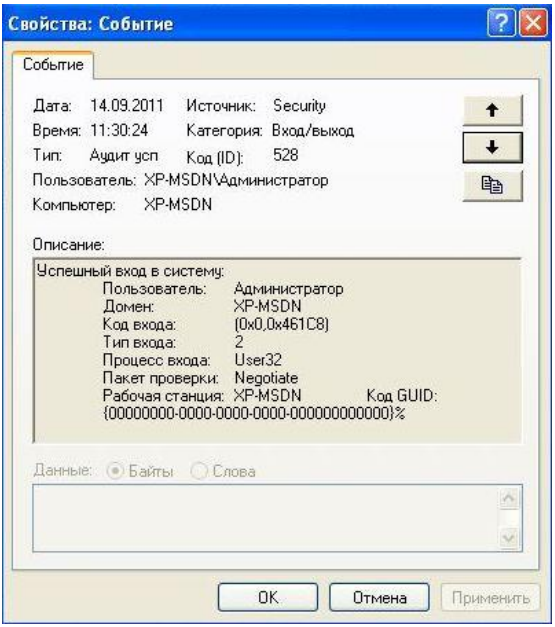

Рисунок 5 – Запись аудита об успешном входе в операционную систему

Таблица 1 – Описание типов входа в систему

Тип входа	Название типа входа	Описание
2	Интерактивный	Локальный вход пользователя на компьютер.
3	Сеть	Пользователь вошёл на данный компьютер через сеть.
4	Пакетный	Пакетный тип входа используется пакетными серверами.
5	Служба	Служба запущена Service Control Manager.
7	Разблокирование	Эта рабочая станция разблокирована.
8	NetworkCleartext	Пользователь вошёл на данный компьютер через сеть. Пароль пользователя передан в нехэшированной форме.
9	NewCredentials	Посетитель клонировал свой текущий маркер и указал новые учётные записи для исходящих соединений.

10	RemoteInteractive	Пользователь выполнил удалённый вход на этот компьютер, используя службу терминалов или удаленный рабочий стол.
11	CachedInteractive	Пользователь вошёл на этот компьютер с сетевыми учётными данными, которые хранились локально на компьютере.

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 551. Данная запись содержит информацию, связанную с успешным выходом пользователя из операционной системы.

Откройте записи категории «Вход учётной записи» (рис. 6, 7). Оба типа события («Успех» и «Отказ») имеют один код события – 680. Дополнительно в записи указывается механизм аутентификации – Microsoft Authentication Package.

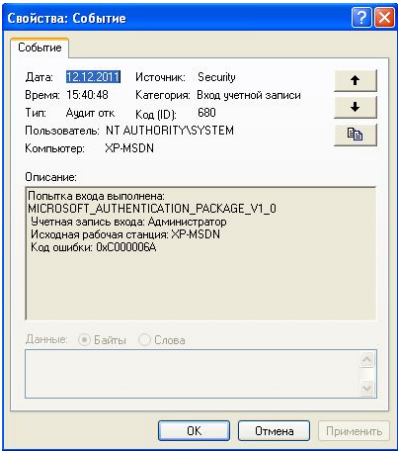

Рисунок 6 – Запись аудита об отказе входа учётной записи

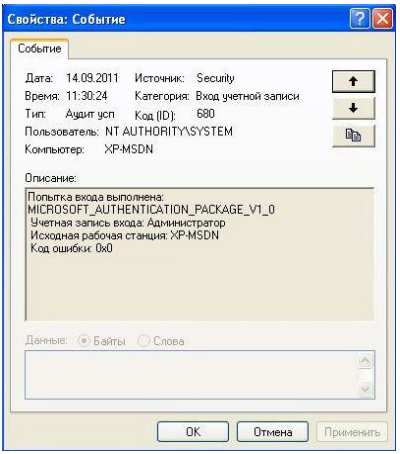

Рисунок 7 – Запись аудита об успешном входе учётной записи

3. Аудит событий, связанных с администрированием

Параметр «Аудит управления учётными записями» включает фиксацию событий, связанных с управлением учётными записями пользователей и групп пользователей. Включите тип событий «Успех» для «Аудита управления учётными записями».

Измените пароль пользователю «user», создайте нового пользователя «user1». Записи категории «Аудит управления учётными записями» содержат как имя учётной записи, у которой были

проведены изменения, так и имя учётной записи пользователя, изменявшего настройки.

Откройте в журнале «Безопасность» запись категории «Учётные записи» с кодом события 628 (при отсутствии записи обновите журнал). Данная запись содержит информацию об изменении пароля учётной записи (рис. 8). В записи аудита представлены имена учётных записей обоих пользователей – у которого пароль был изменён («user») и от имени которой он изменялся («Администратор»).

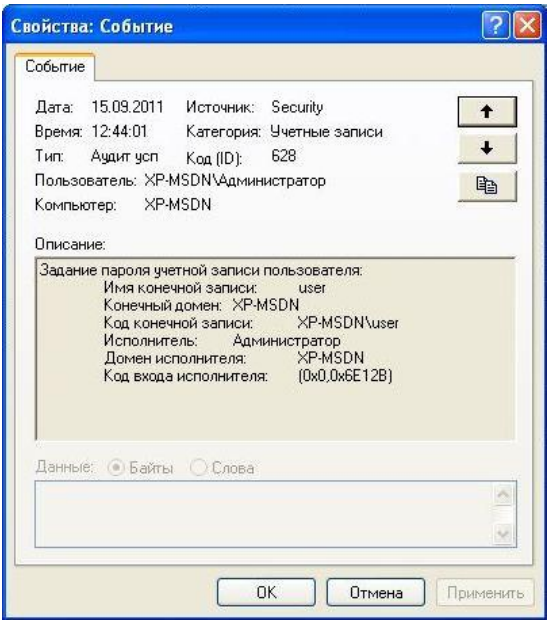

Рисунок 8 – Запись аудита об успешном изменении пароля учётной записи

Откройте запись категории «Учётные записи» с кодом события 626. Данная запись содержит информацию о включении (создании новой) учётной записи пользователя (рис. 9).

При создании нового пользователя автоматически происходит его добавление в группу. Откройте запись категории «Учётные записи» с кодом события 636. Данная запись содержит информацию о добавлении учётной записи пользователя в существующую группу (рис. 10). В записи указаны имя учётной записи пользователя, производившего добавление, имя учётной записи добавляемого пользователя и имя группы, в которую добавляется пользователь.

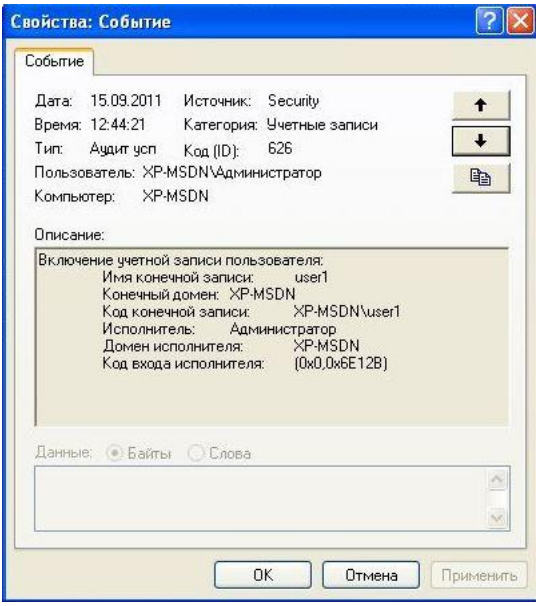

Рисунок 9 – Запись аудита о включении учётной записи

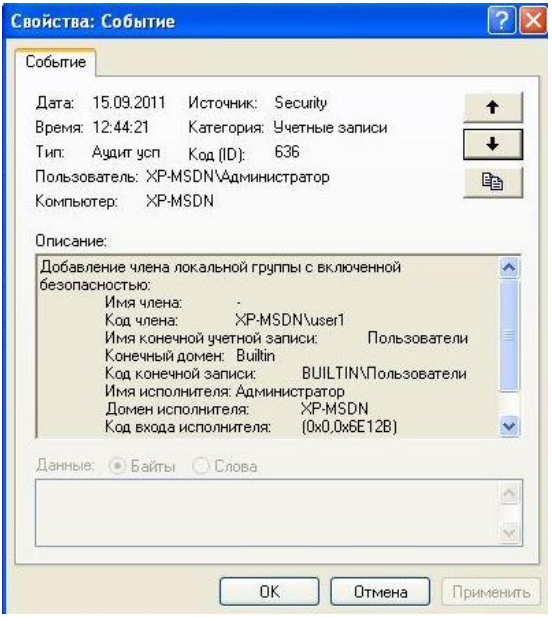

Рисунок 10 – Запись аудита о добавлении учётной записи в группу

Параметр «Аудит изменения политики» включает фиксацию событий, связанных с изменением политики аудита, назначения прав пользователям и т.д. Включите тип событий «Успех» для «Аудита изменения политики».

Откройте раздел «Локальные политики – Назначение прав пользователя» в «Локальной политике безопасности». Предоставьте пользователю «user» право «Архивирование файлов и каталогов», удалите право «Локальный вход в систему» у учётной записи «Гость».

Записи категории «Аудит изменения политики» содержат имя учётной записи, производившей изменение какой-либо политики, название изменяемой привилегии или настройки. Если происходило изменение привилегии учётной записи пользователя, то указывается имя этой учётной записи.

Откройте запись категории «Изменение политики» с кодом 608 (рис. 11). Данная запись содержит информацию о предоставлении пользователю права на резервное копирование информации (SeBackupPrivelege).

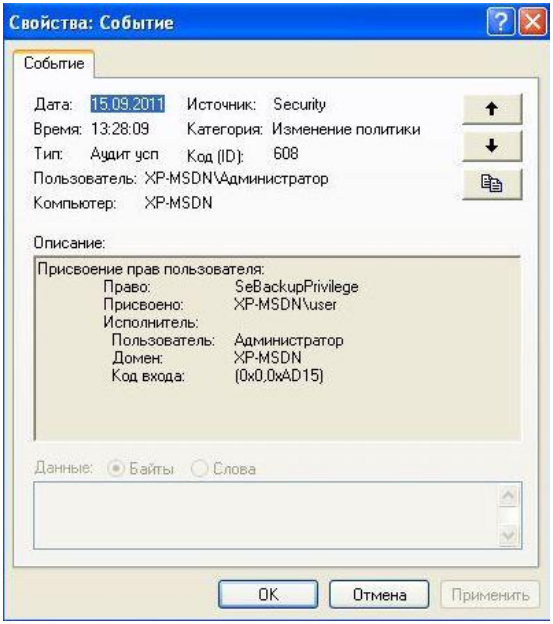

Рисунок 11 – Запись аудита о присвоении пользователю прав

Откройте запись категории «Изменение политики» с кодом 622 (рис. 12). Данная запись содержит информацию об удалении права локального входа пользователя в систему (SeInteractiveLogonRight).

Откройте запись категории «Изменение политики» с кодом 612 (рис. 13). Данная запись содержит информацию об изменении политики аудита. Зафиксировано включение аудита «Успехов» в категории «Изменение политики».

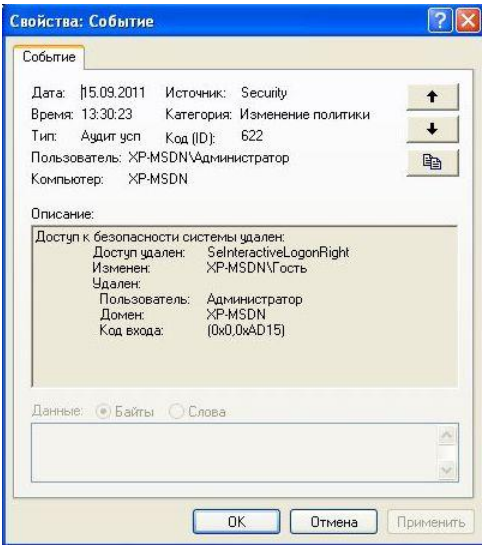

Рисунок 12 – Запись аудита об удалении прав у пользователя

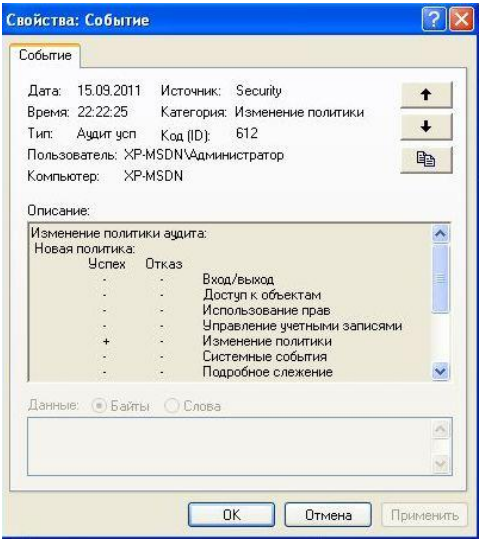

Рисунок 13 – Запись аудита об изменении политики безопасности

Параметр «Аудит использования привилегий» включает фиксацию событий, связанных с применением пользователем выданных ему привилегий. Включите тип событий «Успех» для «Аудита использования привилегий».

Измените системное время. Завершите сеанс пользователя. Войдите под учётной записью «Администратор».

Откройте запись категории «Использование прав» с кодом 577 (рис. 14). Данная запись содержит информацию об использовании привилегии изменения системного времени (SeSystemtimePrivelege) с указанием пользователя, применившего привилегию.

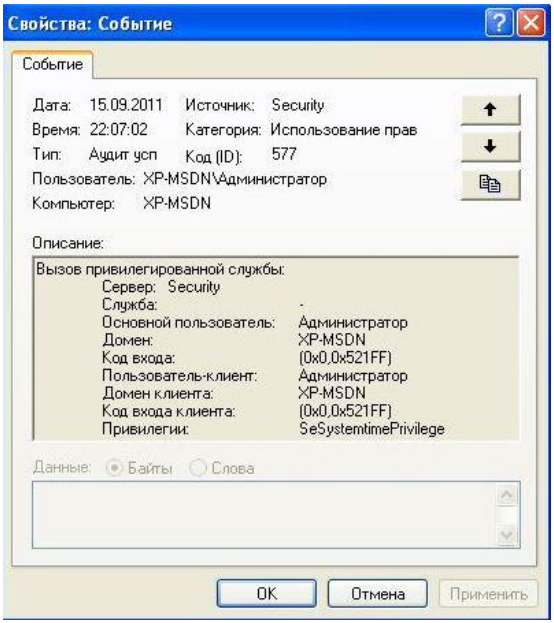

Рисунок 14 – Запись аудита о применении привилегии на изменение системного времени

Откройте запись категории «Использование прав» с кодом 576 (рис. 15). Данная запись содержит информацию о предоставлении пользователю набора привилегий при входе в операционную систему.

Откройте запись категории «Использование прав» с кодом 578 (рис. 16). Данная запись содержит информацию об операции с привилегированным объектом – открытие журнала аудита (EventLog).

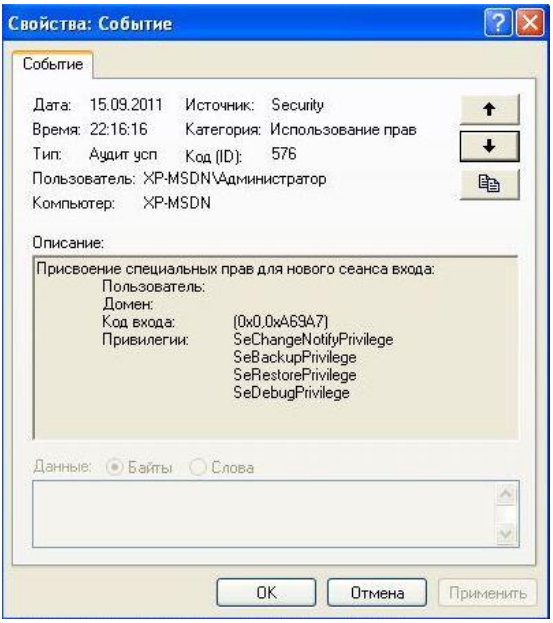

Рисунок 15 – Запись аудита о присвоении привилегий пользователю при входе в систему

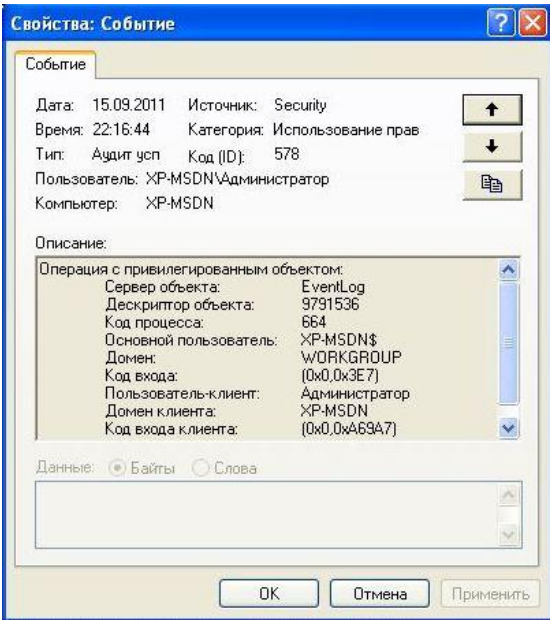

Рисунок 16 – Запись аудита о работе с журналом аудита

4. Аудит событий, связанных с работой операционной системы

Параметр «Аудит системных событий» включает фиксацию событий, связанных со следующими системными событиями: изменение системного времени; запуск и отключение элементов системы безопасности и др. Включите тип событий «Успех» для «Аудита системных событий».

Очистите журнал аудита (например, через контекстное меню журнала). Перезагрузите операционную систему.

Откройте запись категории «Системное событие» с кодом 517 (рис. 17). Данная запись содержит информацию о времени очистки журнала аудита и имя учётной записи пользователя, очистившего журнал.

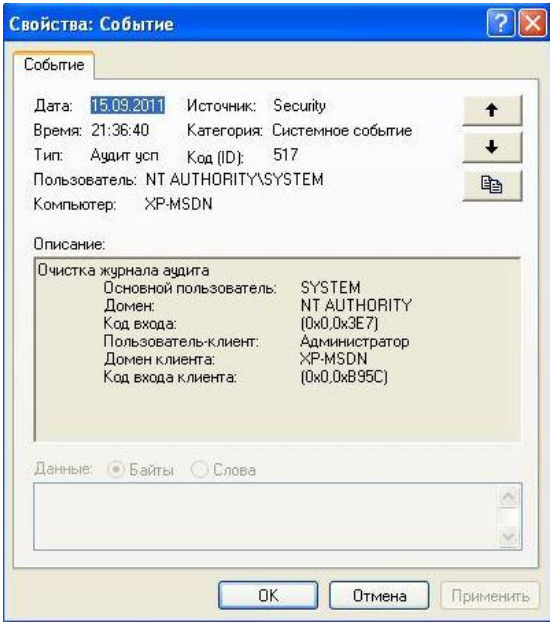

Рисунок 17 – Запись аудита об очистке журнала аудита

Откройте запись категории «Системное событие» с кодом 520 (рис. 18). Данная запись содержит информацию об изменении системного времени. Это событие может генерироваться как от имени учётной записи «System» при синхронизации времени с сервером, так и от имени пользователя. В записи указывается предыдущее и новое время.

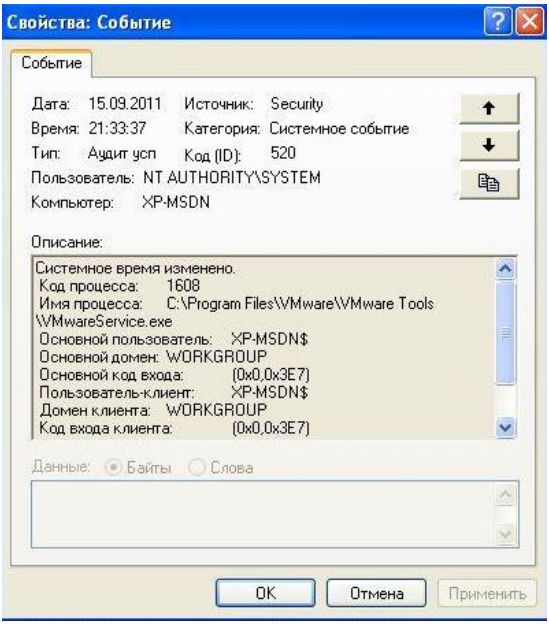

Рисунок 18 – Запись аудита об изменении системного времени

Параметр «Аудит отслеживания процессов» включает фиксацию событий, связанных с работой процессов (создание, завершение, дублирование и т.п.). Включите тип событий «Успех» для «Аудита отслеживания процессов».

Запустите какое-нибудь приложение и закройте его.

Откройте записи категории «Подробное отслеживание» с кодом 592 и 593 (рис. 19, 20). Эти записи содержат информацию о создании нового процесса и его завершении. В информацию о событии включается полное имя исполняемого файла, инициировавшего процесс.

5. Аудит доступа пользователей к ресурсам

Параметр «Аудит доступа к объектам» включает фиксацию событий, связанных с доступом к файлам, каталогам, ключам реестра, принтерам и т.д. Возможен аудит различных типов доступа: чтения, изменения, удаления, печати и др.

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит доступа к объектам».

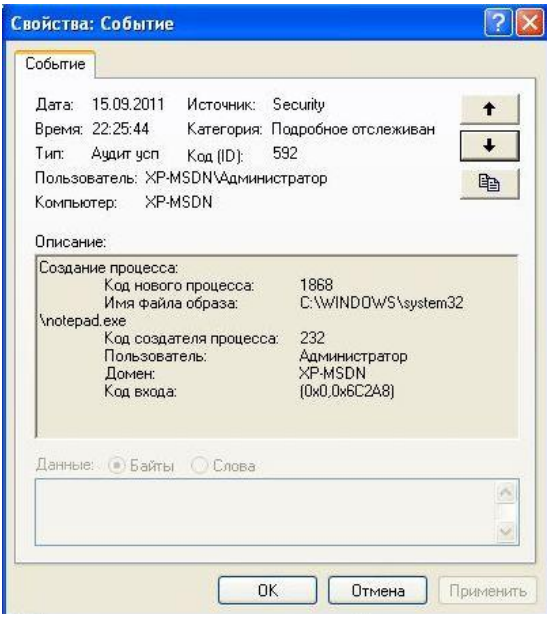

Рисунок 19 – Запись аудита о запуске приложения (создании процесса)

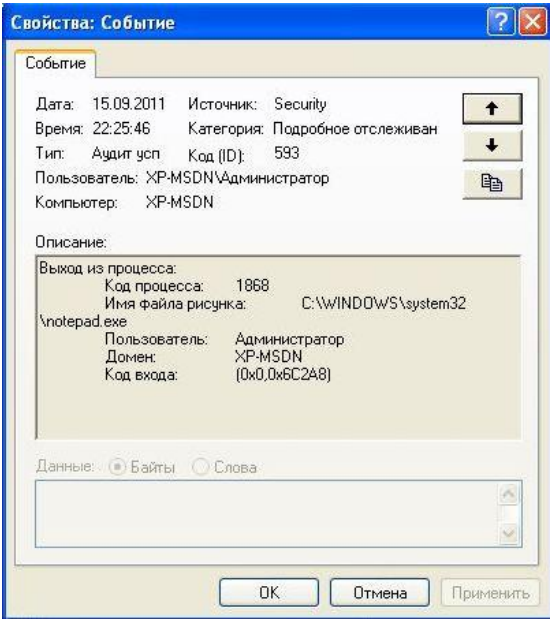

Рисунок 20 – Запись аудита о завершении приложения (выходе из процесса)

Аудит доступа к ресурсам возможен только на логических дисках с файловой системой NTFS. Аудиту подвергаются только те объекты, для которых явно указана необходимость фиксации событий. Таким образом, включение аудита доступа происходит в два этапа: включение «Аудита доступа к объектам» в политике аудита и включение аудита для каждого контролируемого объекта.

Создайте текстовый файл. Перейдите на вкладку «Аудит» в «Свойствах» созданного файла («Свойства – Безопасность – Дополнительно – Аудит»). Включите тип событий «Успех» на тип доступа «Изменение разрешений» для пользователя «Администратор» и тип событий «Отказ» на все типы доступа для пользователя «user» (рис. 21). Во вкладке «Безопасность» свойств созданного файла запретите пользователю «user» доступ на «Запись».

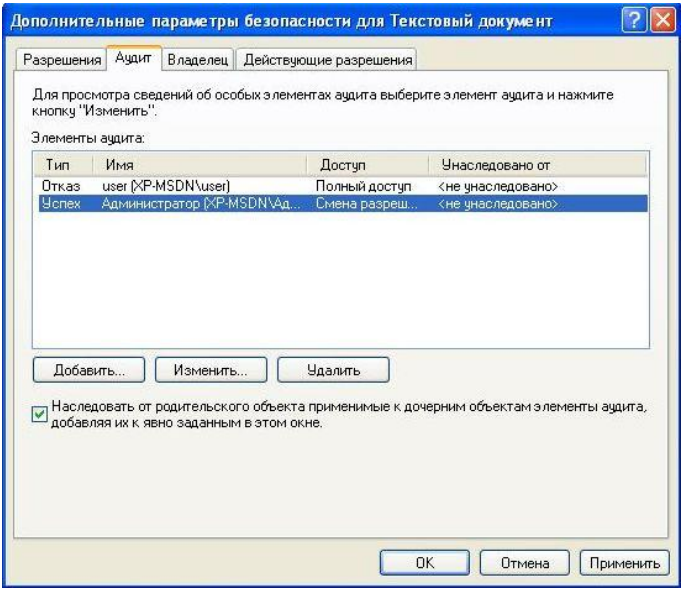

Рисунок 21 – Параметры аудита доступа к файлу

Откройте запись категории «Доступ к объекту» с кодом 560 (рис. 22, 23). Данная запись содержит информацию об успешной смене разрешений на доступ к объекту (тип доступа – WRITE_DAC). Кроме типа доступа, в записи указывается информация об объекте доступа: имя и тип (File). О субъекте доступа указывается следующая информация: имя учётной записи, осуществлявшей доступ, и полное имя исполняемого файла процесса, при помощи которого осуществлялся доступ.

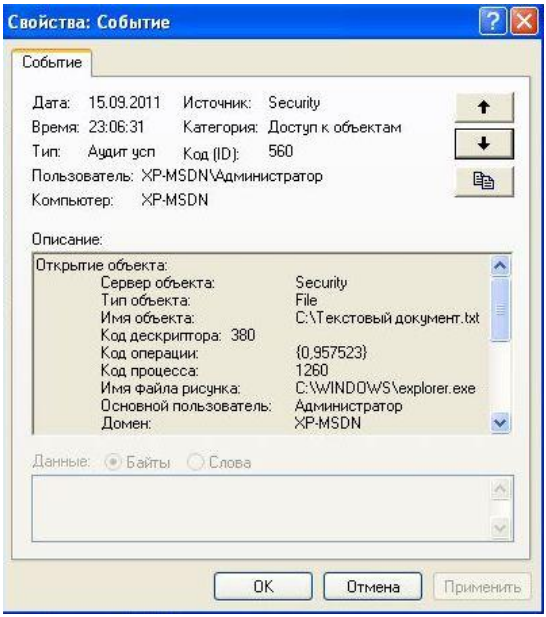

Рисунок 22 – Запись аудита о доступе к объекту для изменении прав доступа

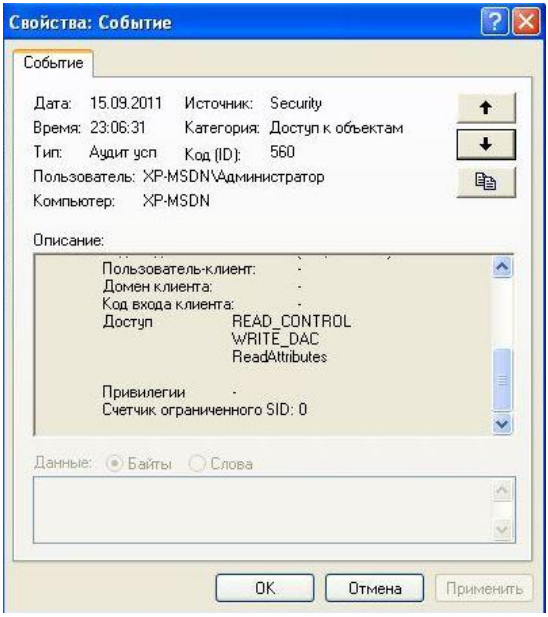

Рисунок 23 – Запись аудита о доступе к объекту для изменении прав доступа (окончание)

Войдите под учётной записью «user». Попытайтесь удалить созданный файл, попытайтесь изменить разрешения на доступ к файлу.

Войдите под учётной записью «Администратор». Откройте записи журнала «Безопасность» категории «Доступ к объекту» с кодом 560, произведённой от имени учётной записи «user». Одна из записей содержит информацию о неуспешной (Аудит отказов) попытке удаления файла (тип доступа – DELETE, рис. 24). Другая запись содержит информацию о неуспешной (Аудит отказов) попытке изменения разрешений на доступ к файлу (рис. 25).

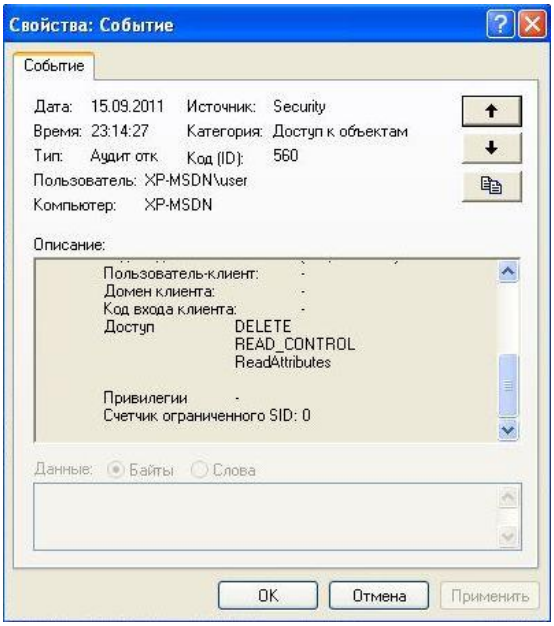

Рисунок 24 – Запись аудита о неуспешной попытке доступа к объекту для его удаления

Откройте «Свойства» принтера doPDF («Пуск – Настройка – Принтеры и факсы»). Для принтеров возможен аудит следующих специфичных действий: печать, управление принтерами, управление документами.

Включите тип аудита «Успех» типа доступа «Управление документами» принтера doPDF для пользователя «Администратор» (применить «Для этого принтера и докуентов», рис.26). Напечатайте текстовый документ.

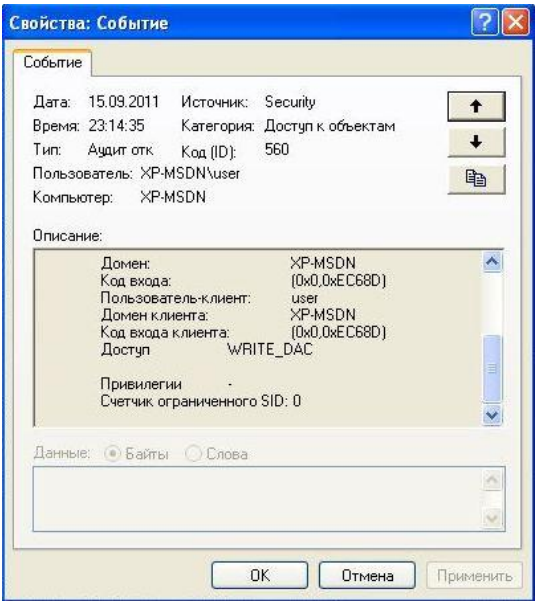

Рисунок 25 – Запись аудита о неуспешной попытке доступа к объекту для изменения прав доступа к нему

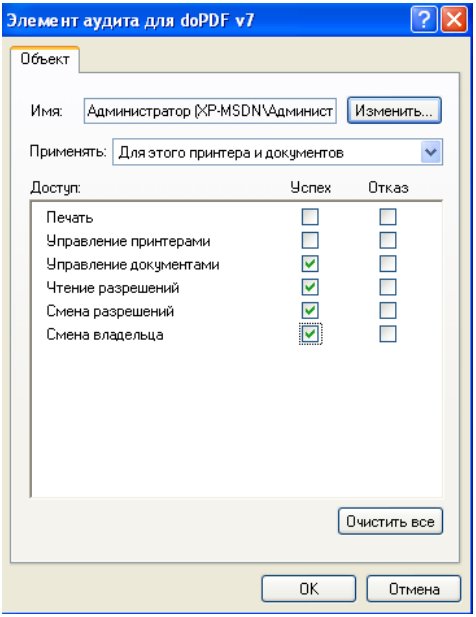

Рисунок 26 – Параметры аудита доступа к принтеру

Просмотрите записи категории «Доступ к объекту» с кодом 560. К печати документа имеют отношение записи с типом объекта Printer (рис. 27) и Document (рис. 28). В записи для принтера указан тип доступа «Печать». В записи для документа указано имя напечатанного документа.

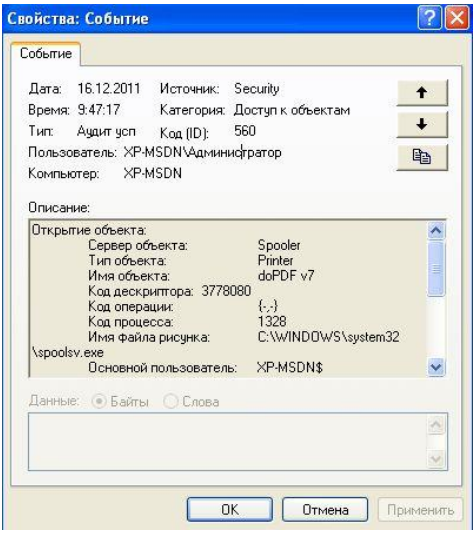

Рисунок 27 – Запись аудита об использовании принтера

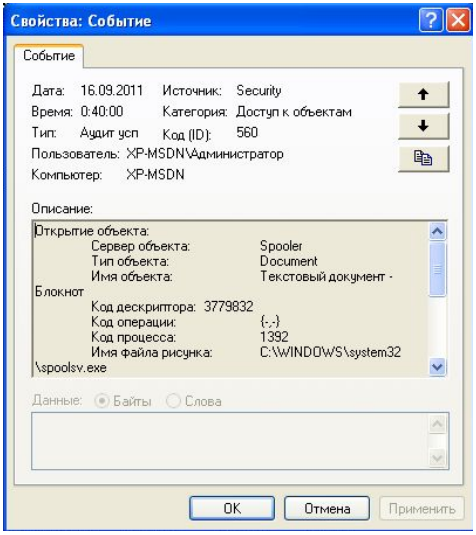

Рисунок 27 – Запись аудита об управлении документом

6. Управление журналом аудита

Войдите под учётной записью «user». Попытайтесь открыть журнал аудита. Группе «Пользователи», в которую входит «user», по умолчанию запрещена работа с журналом аудита, поэтому операционная система сгенерирует ошибку доступа (рис.29).

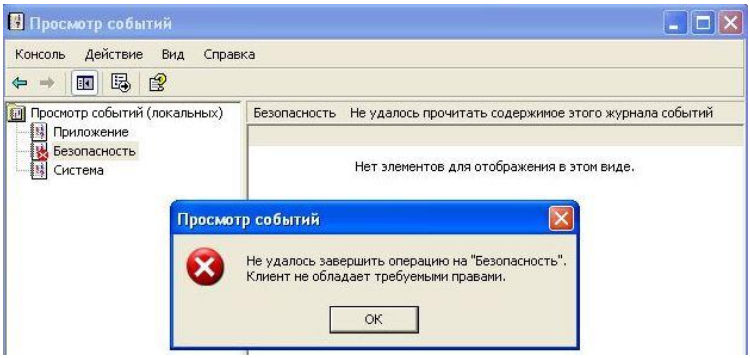

Рисунок 29 – Ошибка доступа к журналу аудита

Запустите от имени учётной записи «Администратор» оснастку «Локальная политика безопасности». Добавьте пользователя «user» в перечень учётных записей параметра «Управление аудитом и журналом безопасности» («Локальные политики – Назначение прав пользователей», рис. 30). Под учётной записью «user» проверьте наличие прав для работы с журналом аудита.

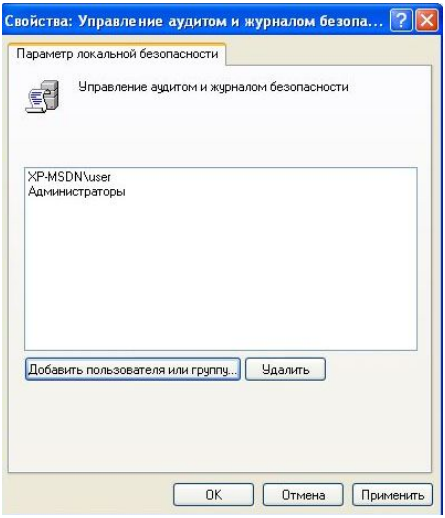

Рисунок 30 – Параметр управления доступом к журналу безопасности

Войдите под учётной записью «Администратор». В меню журнала аудита выберите «Вид» – «Фильтр». Настройте фильтр в соответствии с рис. 31. После применения фильтра в журнале останутся записи только об удачных и неудачных попытках входа под учётной записью «user».

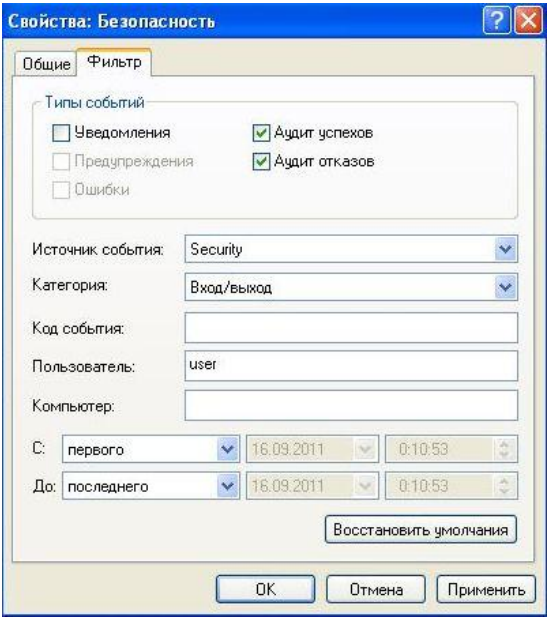

Рисунок 31 – Настройка фильтрации записей журнала безопасности

При поиске объекта с известным именем лучше использовать функцию поиска: «Вид» – «Найти» (рис. 32), введя имя (часть имени) файла.

В контекстном меню журнала «Безопасность» выберите «Свойства». В появившейся вкладке можно установить максимальный размер журнала и действия в случае его переполнения (рис. 33).

Установите размер журнала в минимально возможное значение – 64 КБ. Включите все возможные виды аудита.

Рисунок 32 – Настройка поиска записей журнала безопасности

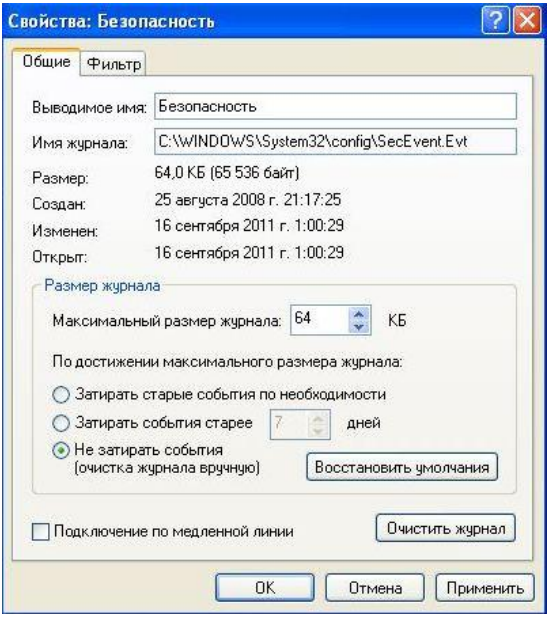

Рисунок 33 – Настройка работы журнала безопасности

Для установки запрета работы пользователя в случае переполнении журнала необходимо включить параметр «Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности» в разделе «Параметры безопасности» локальной групповой политики (рис. 34).

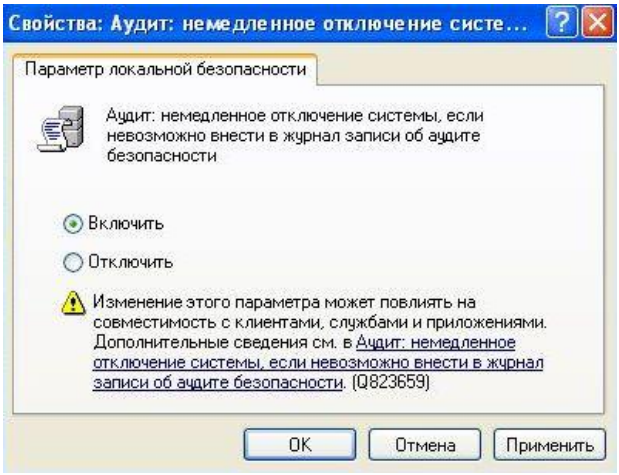

Рисунок 34 – Настройка действий при переполнении журнала безопасности

Перезагрузите операционную систему. Войдите под учётной записью «Администратор». Генерируйте новые записи аудита до тех пор, пока не произойдёт заполнение журнала и перезагрузка системы. После этого войдите в систему под учётной записью «Администратор» (рис. 35), сохраните журнал (рис. 36) и очистите его.

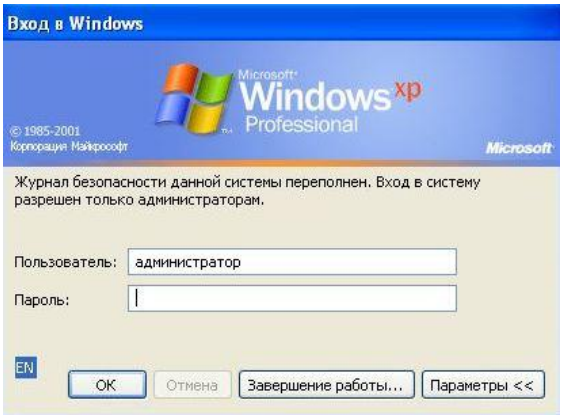

Рисунок 35 – Окно входа в систему при переполнении журнала безопасности

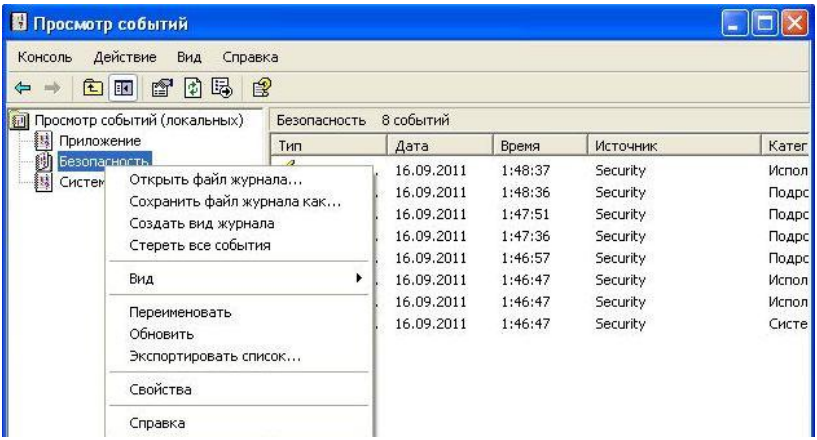

Рисунок 36 – Сохранение журнала безопасности

Просмотр сохранённых журналов безопасности осуществляется при помощи функции «Открыть файл журнала» контекстного меню журнала безопасности.

Задание

Импортируйте журнал безопасности в соответствии со своим вариантом. Проанализируйте журнал безопасности согласно распределению вариантов и определите виновных. Параметры аудита, использовавшиеся при фиксации событий, перечислены в табл. 2. Также включен параметр «Аудит прав на архивацию и восстановление». Правом управлять аудитом и журналом безопасности могут только «Администратор» и пользователь «Анатолий». Сведения об учётных записях перечислены в табл. 3.

Таблица 2 - Параметры политик аудита

Название параметра	Успех	Отказ
Аудит событий входа в систему	+	+
Аудит управления учётными записями	+	+
Аудит доступа к службе каталогов	-	-
Аудит входа в систему	+	+
Аудит доступа к объектам	+	+
Аудит изменения политики	+	+
Аудит использования привилегий	-	+
Аудит отслеживания процессов	-	-
Аудит системных событий	+	+

Таблица 3 - Учётные записи

Имя учетной записи	Должность, группа
Дмитрий	стажёр, пользователь
Геннадий	финансовый менеджер, пользователь
Василий	оператор пульта видеонаблюдения, пользователь
Администратор	технический консультант, администратор системы
Валерий	директор, оператор архива
Людмила	бухгалтер, пользователь
Татьяна	секретарь, пользователь
Артур	помощник технического консультанта, пользователь
Анатолий	администратор безопасности, администратор системы
ДАВЫДОВ	руководитель отдела разработки, пользователь

Вариант 1

Администратор безопасности Анатолий предоставил полный доступ к материалам по безопасности отдела только стажеру Дмитрий. Эти материалы были размещены на сетевом ресурсе «Ресурсы предприятия\Обмен\Дмитрию», к которому был заранее выставлен аудит чтения, записи, удаления, а также смены владельца. При утилизации документации Анатолий обнаружил распечатанные копии этих материалов. Стажер утверждает свою непричастность к распечатанным копиям важных документов. Докажите или опровергните причастность Дмитрия к распечатанным документам.

Вариант 2

На предприятии есть сетевой ресурс «Ресурсы предприятия\Конкурентоспособность основного продукта», в котором находились два документа «Продукты конкурентов.doc» и «Стратегия развития основного продукта.doc». Доступ на запись и чтение имели только следующие пользователи: «Геннадий» и «ДАВЫДОВ». Администратор безопасности Анатолий ранее настроил для этого ресурса аудит успехов и отказов удаления, чтения, записи, смены разрешений и смены владельца. Вскоре финансовый менеджер и руководитель отдела разработки сообщили об исчезновении этих документов. Выясните, кто причастен к удалению этих документов?

Вариант 3

Администратор системы неоднократно сообщал о действиях в системе, выполняемых кем-то под его учетной записью, включая смену паролей пользователей. Администратор безопасности посчитал необходимым настроить полный аудит ветви реестра, хранящий учетные записи и их пароли в неявном виде. Ветвь реестра, хранящая базу данных учетных записей, имеет следующий путь: «HKEY_LOCAL_MACHINE\SAM\SAM». Выясните, кто и какой программой получает доступ к базе данных учетных записей.

Вариант 4

Из организации, по собственному желанию, уволился системный администратор, не проработав и одной рабочей недели. По прошествии нескольких дней оператор пульта видеонаблюдения сообщил о странном поведении компьютера: «Компьютер самопроизвольно заблокировался, отобразив окно блокировки пользователем MS_Support_tech567». Выясните причину блокировки.

Вариант 5

В сетевых ресурсах предприятия дополнительной мерой защиты при обмене значимыми электронными документами между сотрудниками является установка пароля. Секретарь оповестила администратора безопасности о недейственности таких мер защиты, приведя в пример редактированный документ «Отчет деятельности сотрудников на апрель.doc» по сравнению с сохранившимся оригиналом. Администратор безопасности настроил аудит чтения на сетевой ресурс «C:\Ресурсы предприятия\Обмен» с применением наследования параметров аудита для создаваемых в нем файловых объектов. Проведите аудит файловых объектов этого ресурса на факт подбора пароля к ним.

Вариант 6

В предприятии имеется доступ к сети интернет, настроенный только для работы с почтовыми серверами. Приходящие счета за предоставления доступа к сети интернет не соизмеримы с объемом трафика, получаемого по почтовым протоколам. Директор потребовал администратора безопасности выяснить причину таких затрат. Проведите аудит запущенных пользователями программ, которые могли получать большой объем данных из сети интернет.

Вариант 7

Администратор безопасности ответственен за лицензионное ПО, используемое в компьютерах организации. Поэтому он должен отслеживать доступ к информации, приводящий к краже закрытой

информации лицензионного ПО, такой как 25-тизначный ключ продукта Windows. Большинство такой информации хранится в ветвях реестра, к которым применим аудит чтения. Проведите аудит журнала безопасности на факт чтения значений ветвей реестра лицензионных программ, а также используемые программы.

Вариант 8

Директор организации использует встроенные средства резервирования для файла «База данных заказов.doc», архив которого он сохраняет в папку «C:\АРХИВ\backup», к которому только он имеет доступ. Служба внутренней безопасности организации сообщила об отфильтрованном электронном письме с поддельным адресом отправителя, не значившимся в списке разрешенных отправителей. Текст письма содержал предложение о продаже информации и список электронных документов, в число которых входил архивируемый директором файл. Администратору безопасности было поручено разобраться проблемами утечки информации, в число которых входит вопрос выявления способа получения ограниченных в доступе файлов. Выясните, кто и как получил ограниченный в доступе файл.

Вариант 9

Администратор безопасности посчитал необходимым провести аудит неблагонадежных сотрудников организации. Для этого он открыл доступ к документу «зарплата сотрудников на 30.04.09.doc», назначив аудит чтения и записи. Выявите неблагонадежных пользователей, которые редактировали этот файл.

Вариант 10

Администратор пожаловался на наличие в компьютерах организации нежелательного ПО (компьютерные игры), которое регулярно появляются вновь, включая то, которые требуют для установки права локального администратора. Проведите аудит, чтобы выяснить пользователей, обладающих паролем локального администратора.

Контрольные вопросы

1. Какие данные фиксируются при аудите входа/выхода в систему?
2. Чем отличается аудит входа в систему от аудита событий входа в систему?
3. Какие данные фиксируются при аудите управления учётными записями?
4. Какие данные фиксируются при аудите изменения политики?
5. Какие данные фиксируются при аудите использования прав?
6. Какие данные фиксируются при аудите системных событий?

7. Какие данные фиксируются при аудите отслеживания процессов?

8. Какие типы объектов могут подвергаться фиксации при аудите доступа к объектам? Какие при этом фиксируются данные?

9. Каким образом происходит настройка аудита доступа к объектам?

10. Какие существуют настройки политики безопасности, связанные с аудитом?

ЛАБОРАТОРНАЯ РАБОТА №8

АНАЛИЗ И НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Целью данной работы является ознакомление с встроенными в операционную систему Windows XP возможностями по оценке текущего состояния подсистемы безопасности и контролю целостности настроек безопасности.

Оценка текущего состояния проводится на основе сравнения текущих значений параметров безопасности с эталонными. Применение эталона позволяет автоматизировать настройку безопасности операционной системы и дальнейший контроль установленного уровня безопасности.

В операционной системе Windows XP для работы с текущими и эталонными настройками безопасности предназначены оснастки «Шаблоны безопасности» и «Анализ и настройка безопасности».

Ход работы

Войдите в операционную систему под учётной записью «Администратор». Откройте Microsoft Management Console («Пуск – Выполнить» и введите команду «mmc») и добавьте оснастки «Анализ и настройка безопасности» и «Шаблоны безопасности».

1. Структура шаблона безопасности

Шаблон безопасности – набор эталонных настроек операционной системы, влияющих на информационную безопасность. В Windows XP существует набор встроенных шаблонов безопасности. По умолчанию встроенные шаблоны безопасности расположены в каталоге C:\Windows\security\templates\. Просмотр и редактирование настроек, входящих в шаблон, осуществляется через оснастку «Шаблоны безопасности» (рис. 1).

Ниже приведён перечень встроенных шаблонов безопасности и их краткое описание.

а). Безопасность по умолчанию (Setup security.inf) – содержит параметры безопасности, которые применяются по умолчанию во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. Этот шаблон можно использовать полностью или частично в целях аварийного восстановления.

б). Совместимый (Compatws.inf) – содержит разрешения по умолчанию для рабочих станций и серверов (не контроллеров домена). Учитывается иерархия прав локальных групп: "Администраторы", "Опытные пользователи" и "Пользователи".

в). Защита (Securews.inf и Securedc.inf) – шаблоны для настройки рабочих станций (ws – workstations) и контроллеров домена (dc – domain controllers). В них определяются параметры повышенной безопасности: определяются параметры надёжных паролей, блокировки и аудита; правила работы с протоколом NTLM; определяются дополнительные ограничения для анонимных пользователей.

г). Повышенная защита (Hisecws.inf и Hisecdc.inf) – шаблоны повышенной защиты для рабочих станций и контроллеров домена, налагающие дополнительные ограничения на уровни кодировки и подписи, необходимые для проверки подлинности и для данных, передаваемых по безопасным каналам между клиентами SMB и серверами.

д). Безопасность системного корневого каталога (Rootsec.inf) – включает разрешения, по умолчанию применяемые для корневого каталога системного диска.

Каждый шаблон состоит из следующих разделов (рис. 1):

- Политики учётных записей;
- Локальные политики;
- Журнал событий;
- Группы с ограниченным доступом;
- Системные службы;
- Реестр;
- Файловая система.

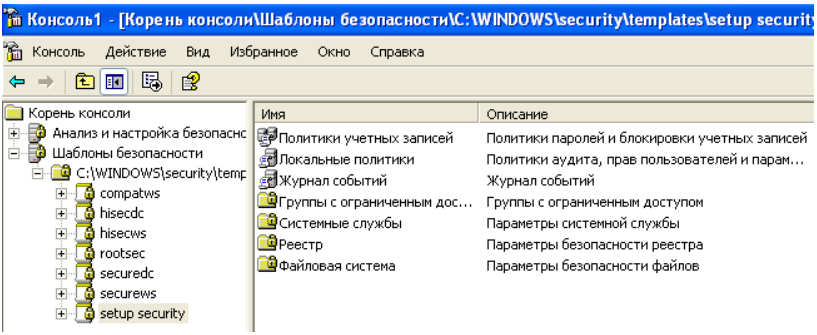

Рисунок 1 – Структура шаблона безопасности

Дальнейшее рассмотрение структуры шаблона и изменение его настроек осуществляется на основе встроенного шаблона «setup security».

Разделы «Политики учётных записей» и «Локальные политики» включают в себя все параметры аналогичных разделов «Групповой политики». Измените значение минимальной длины пароля на 6

символов в разделе «Политики учётных записей» – «Политика паролей» (рис. 2). Добавьте группу «Пользователи» в параметре «Управление аудитом и журналом безопасности» раздела «Локальные политики» – «Назначение прав пользователя» (рис. 3).

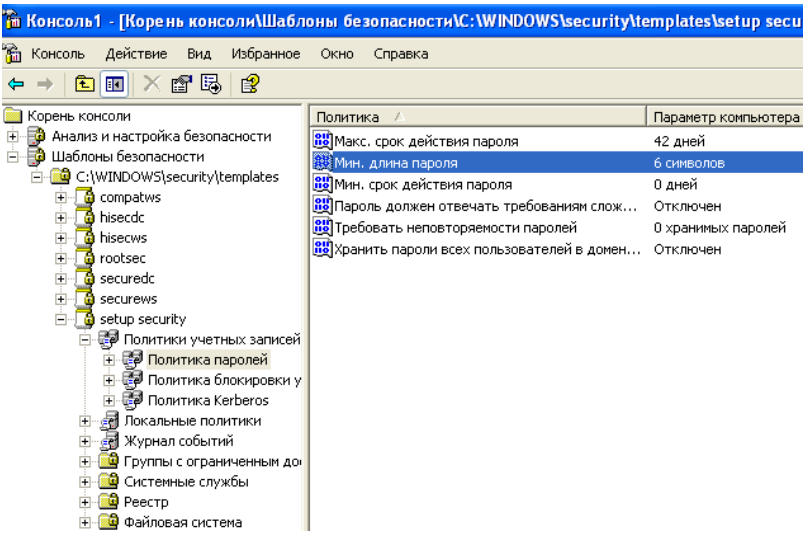

Рисунок 2 – Изменение параметра в разделе «Политики учётных записей»

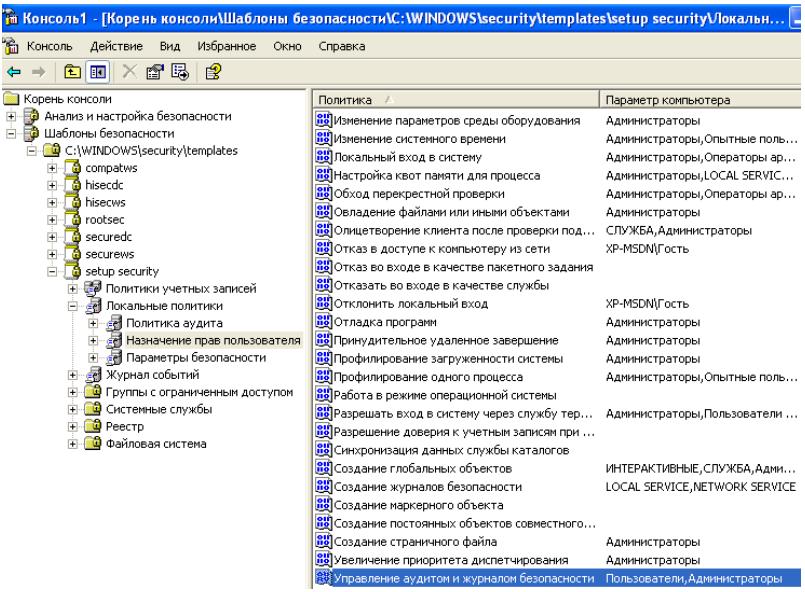

Рисунок 3 – Изменение параметра в разделе «Локальные политики»

Раздел «Журнал событий» включает настройки правил работы с журналами аудита. Разрешите доступ локальной группе гостей к журналу безопасности (рис. 4).

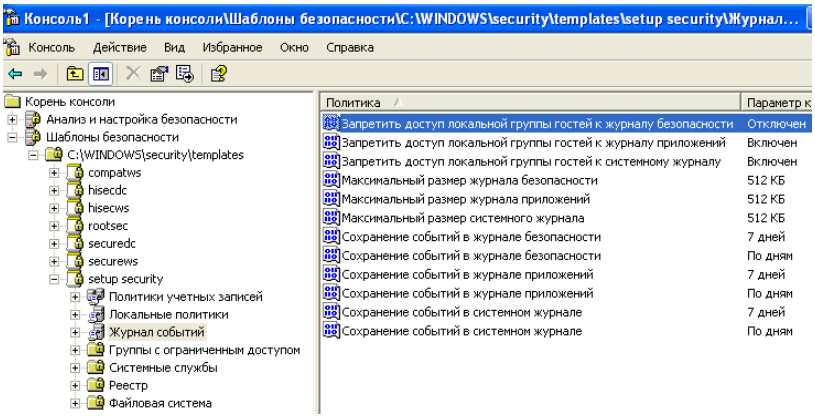

Рисунок 4 – Изменение параметра в разделе «Журнал событий»

Раздел «Группы с ограниченным доступом» позволяет настраивать состав групп пользователей. При помощи контекстного меню добавьте в список группу «Администраторы» и в качестве члена группы добавьте пользователя «user» (рис. 5).

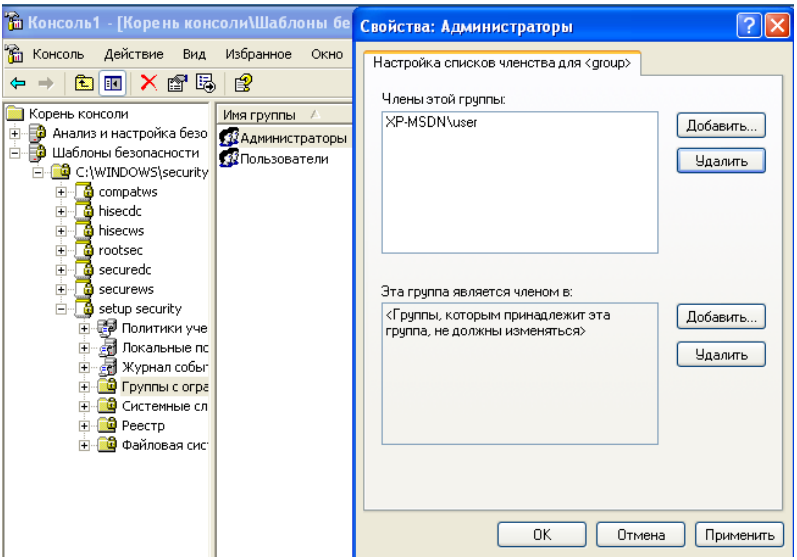

Рисунок 5 – Изменение параметра в разделе «Группы с ограниченным доступом»

Раздел «Системные службы» содержит настройки по запуску служб и разграничению доступа к управлению ими. Запретите запуск службы «Диспетчер очереди печати» (рис. 6). Эта служба запускается как процесс с именем spoolsv.exe.

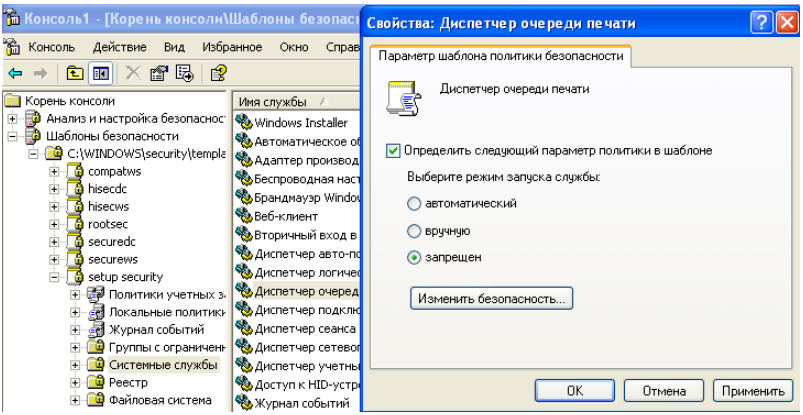

Рисунок 6 – Изменение параметра в разделе «Системные службы»

Раздел «Реестр» содержит правила разграничения доступа к основным ветвям реестра: software, system, users. Настройте доступ к разделу HKEY_LOCAL_MACHINE\SOFTWARE (рис. 7), разрешив полный доступ к нему группе «Опытные пользователи» (рис. 8).

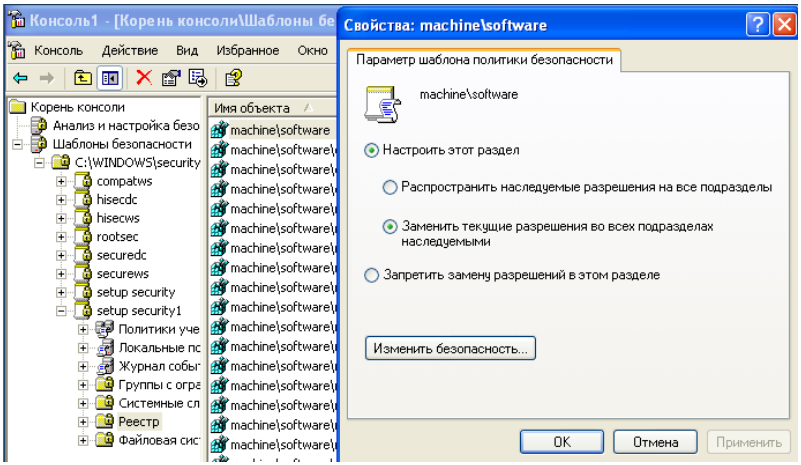

Рисунок 7 – Изменение параметра в разделе «Реестр»

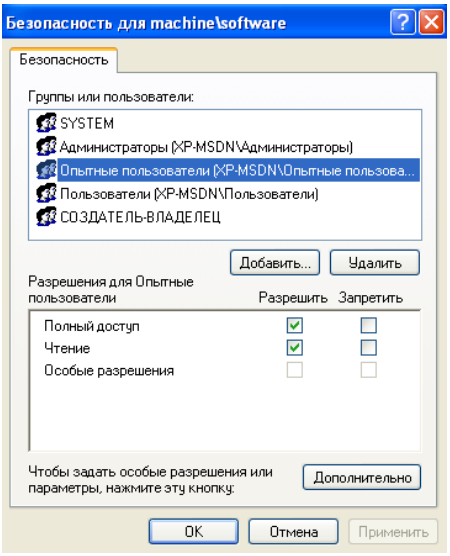

Рисунок 8 – Установка прав доступа к разделу реестра

Раздел «Файловая система» содержит правила разграничения доступа к каталогам на системном диске. Запретите всем пользователям доступ к «Косынке» («C:\WINDOWS\system32\sol.exe», рис. 9-10).

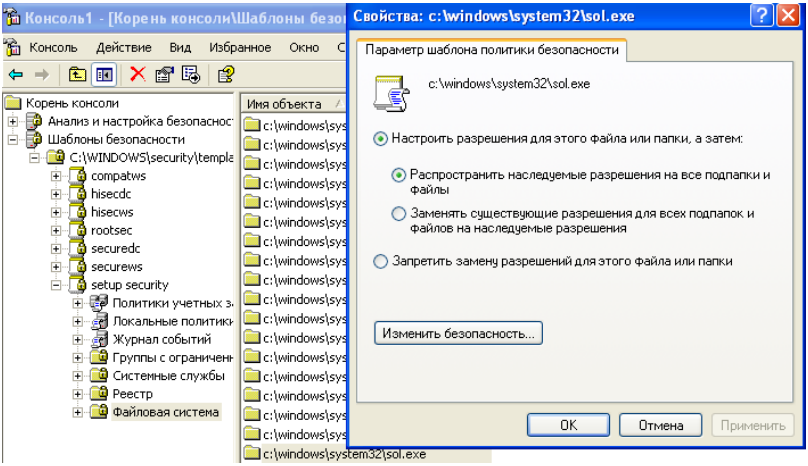

Рисунок 9 – Изменение параметра в разделе «Файловая система»

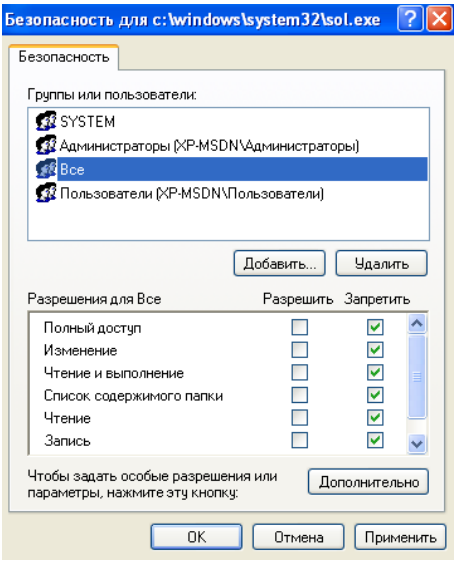

Рисунок 10 – Установка прав доступа к файлу

2. Управление шаблонами безопасности

В оснастке «Шаблоны безопасности» существует возможность создавать собственные шаблоны. Создать новый шаблон можно через контекстное меню каталога, содержащего шаблоны (рис. 11). При этом будет создан шаблон, у которого все параметры будут иметь значение «Не определено».

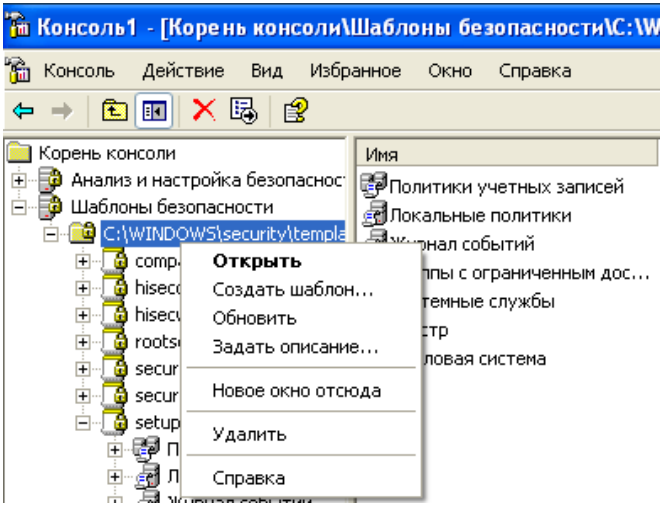

Рисунок 11 – Создание нового шаблона безопасности

Кроме того, собственный шаблон можно создать на основе существующего. Вызовите контекстное меню шаблона «setup security», выберите «Сохранить как…» (рис. 12) и сохраните шаблон под новым именем (например, «test»). При этом будет создан новый шаблон, включающий все сделанные ранее изменения значений параметров.

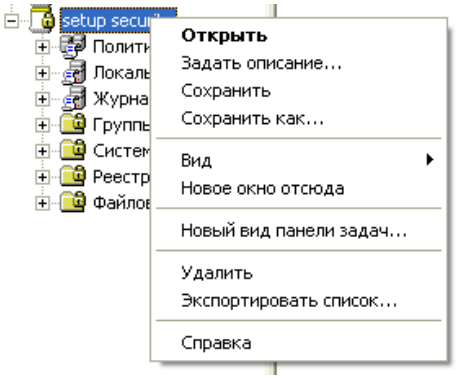

Рисунок 12 – Сохранение изменённого шаблона

3. Анализ параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» (рис. 13), выберите пункт «Открыть базу данных…». Задайте имя для создаваемой базы данных эталонных настроек. После этого необходимо занести в базу значения параметров из интересующего шаблона. Выберите созданный шаблон (рис. 14).

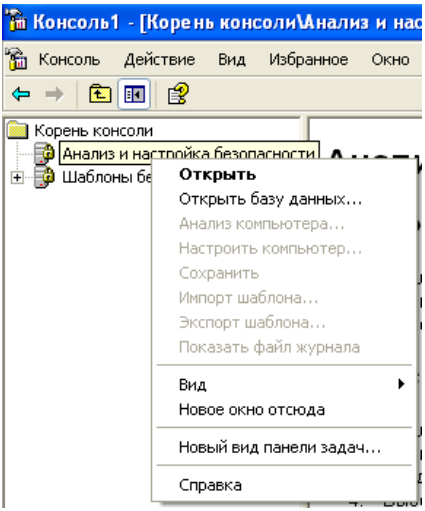

Рисунок 13 – Создание базы данных настроек безопасности

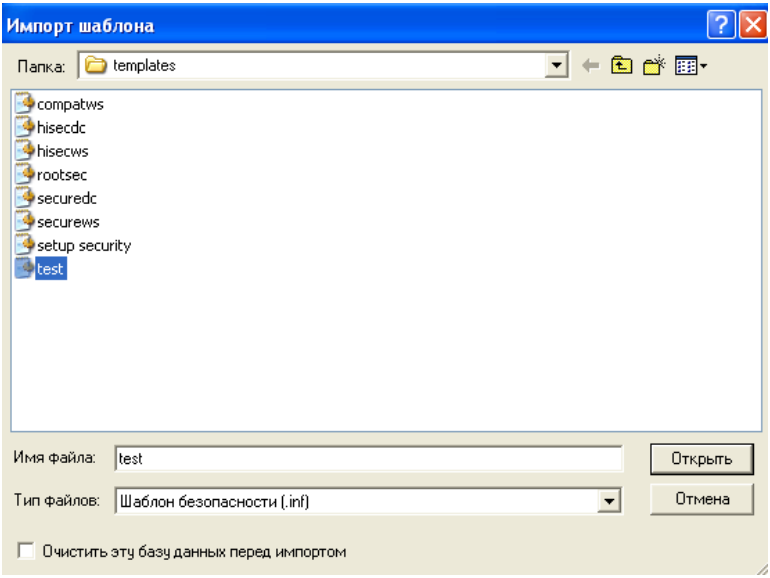

Рисунок 14 – Выбор шаблона для импорта в базу данных

Занесение в базу настроек из другого шаблона возможно через команду контекстного меню «Импорт шаблона» (рис. 15).

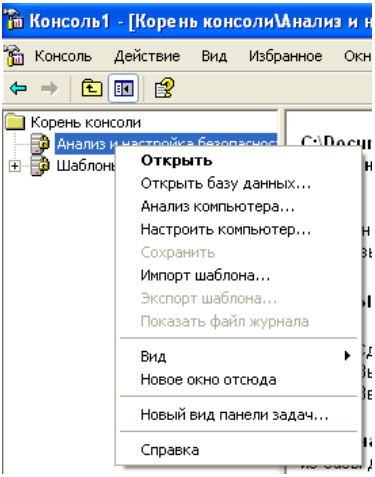

Рисунок 15 – Импорт шаблона

Выберите в контекстном меню оснастки пункт «Анализ компьютера…» и подтвердите предложенный путь к лог-файлу. После

этого начнётся анализ текущих настроек безопасности операционной системы (рис. 16). Результатом анализа является сравнение текущих (Параметр компьютера) и эталонных (Параметр базы данных) значений параметров безопасности. Структура представления результатов совпадает со структурой шаблона (рис. 17).

Результаты сравнения значений параметров представляются в виде специальных пиктограмм, находящихся рядом с названием каждого параметра (табл. 1).

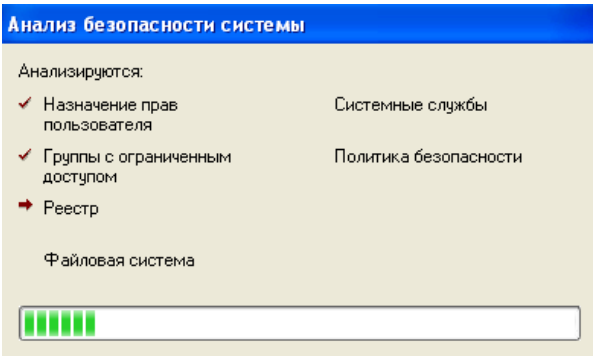

Рисунок 16 – Анализ настроек безопасности операционной системы

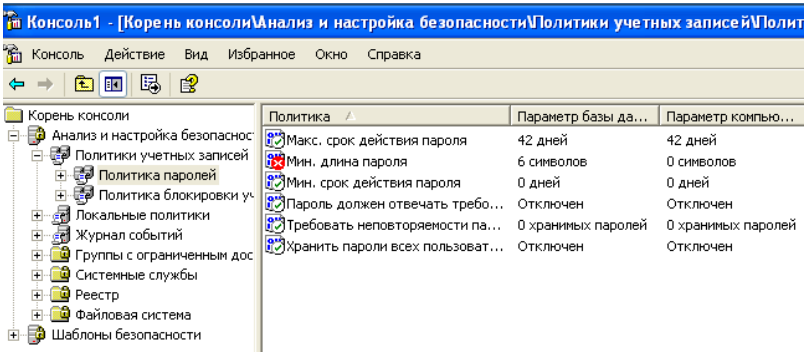

Рисунок 17 – Результат анализа безопасности операционной системы

Таблица 1 – Описание пиктограмм результатов анализа

Пиктограмма	Описание
	Элемент определён в базе данных анализа и в системе, но значения параметров безопасности не совпадают.
	Элемент определён в базе данных анализа и в системе; значения параметров безопасности совпадают.

	Элемент не анализировался. Возможно, он не был определён в базе данных анализа или пользователь, выполняющий анализ, не имеет достаточных разрешений на анализ данного объекта или области
	Элемент определён в базе данных анализа, однако, не существует в текущей конфигурации системы. Например, может существовать группа с ограниченным доступом, определённая в базе данных анализа и не существующая в анализируемой системе
	Элемент не определён в базе данных анализа или в системе

Удостоверьтесь, что в результате проведенного анализа изменённые параметры безопасности отмечены как несовпадающие.

Если какая-нибудь из текущих настроек системы предпочтительнее эталонной, то её можно занести в базу (рис. 18). Изменённую базу можно сохранить в качестве шаблона из контекстного меню оснастки, сохранив базу и выбрав пункт «Экспорт шаблона».

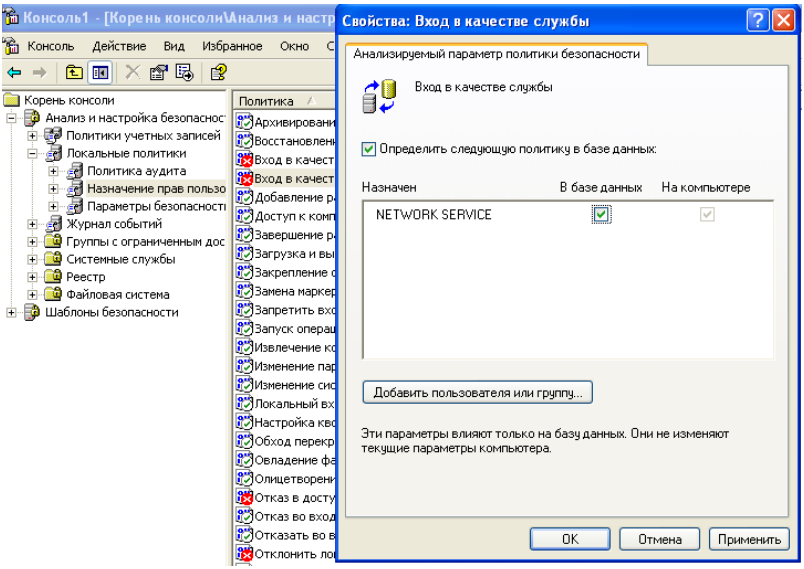

Рисунок 18 – Изменение настроек в базе данных

В итоге, был создан шаблон, в котором запрещён доступ к «Косынке», запрещён запуск службы «Диспетчер очереди печати» и пользователь с учётной записью «user» является членом группы «Администраторы». Проверьте текущее состояние этих настроек:

возможность запуска «Косынки», наличие запущенного процесса spoolsv.exe в «Диспетчере задач» и отсутствие пользователя «user» в группе «Администраторы».

4. Настройка параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» и выберите пункт «Настроить компьютер…». После подтверждения пути к лог-файлу начнётся настройка операционной системы в соответствии со значениями параметров, указанных в базе данных (рис. 19).

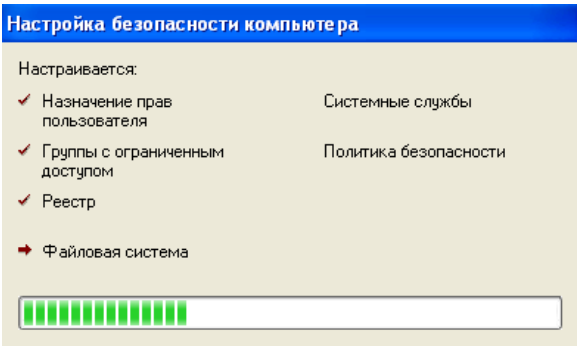

Рисунок 19 – Настройка параметров безопасности операционной системы

Проведите повторный анализ системы для проверки изменения несовпадавших параметров (рис. 20).

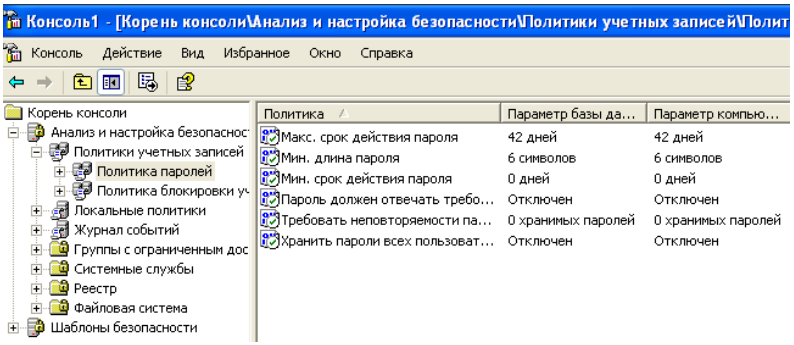

Рисунок 20 – Результат настройки параметров операционной системы

Удостоверьтесь в применении настроек, установленных в изменённом шаблоне: попытайтесь запустить «Косынку», проверьте отсутствие процесса spoolsv.exe в «Диспетчере задач» и наличие учётной записи «user» в группе «Администраторы».

Задание

Создайте шаблон безопасности в соответствии с Вашим вариантом и настройте операционную систему, используя созданный шаблон.

Вариант 1

Политики учётных записей	Политики учётных записей	Локальные политики
Минимальная длина пароля – 10 символов	Пороговое значение блокировки – 3 ошибки входа	Включите аудит отказов входа в систему

Вариант 2

Локальные политики	Журнал событий	Группы с ограниченным доступом
Запретите группе «Операторы архива» восстановление архивных файлов	Сохранение событий в журнале безопасности – вручную	Включите учётную запись «user» в группу «Операторы архива»

Вариант 3

Локальные политики	Журнал событий	Файловая система
Включите аудит доступа к объектам (успех и отказ)	Сохранение событий в журнале безопасности – 30 дней	Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Вариант 4

Локальные политики	Локальные политики	Системные службы
Запретите отображение имени последнего пользователя при входе в систему	Включите обязательное нажатие Ctrl-Alt-Del при входе в систему	Автозапуск службы «Центр обеспечения безопасности»

Вариант 5

Локальные политики	Журнал событий	Группы с ограниченным доступом
Разрешите учётной записи «user» работу с журналом аудита	Максимальный размер журнала безопасности – 2 МБ	Включите учётную запись «user» в группу «Опытные пользователи»

Вариант 6

Политики учётных записей	Локальные политики	Системные службы
Включите применение требований к сложности паролей	Включите аудит управления учётными записями	Автозапуск службы «Автоматическое обновление»

Вариант 7

Локальные политики	Группы с ограниченным доступом	Файловая система
Запретите группе «Пользователи» завершение работы системы	В группу «Пользователи» добавьте пользователя «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к редактору реестра группе «Пользователи»

Вариант 8

Политики учётных записей	Локальные политики	Системные службы
Срок действия пароля – 90 дней	Запретите учётной записи «user» доступ к компьютеру из сети	Запретить запуск службы «Диспетчер сеанса справки для удалённого рабочего стола»

Вариант 9

Локальные политики	Группы с ограниченным доступом	Файловая система
Включите очистку файла подкачки при завершении работы системы	В группу «Пользователи» добавьте учётную запись «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к оснастке «Службы» (services.msc) группе «Пользователи»

Вариант 10

Локальные политики	Локальные политики	Файловая система
Запретите изменение системного времени группе «Опытные пользователи»	Включите аудит системных событий (успех и отказ)	Запретите учётной записи «user» доступ к оснастке «Просмотр событий» (eventvwr.msc)

Контрольные вопросы

1. Каким образом при помощи встроенных средств операционной системы Windows XP можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?
2. Каким образом при помощи встроенных средств Windows XP можно автоматизировать настройку операционной системы в соответствии с требуемыми параметрами безопасности?
3. Что такое «Шаблон безопасности»?
4. Для чего предназначена оснастка «Шаблоны безопасности»?
5. Какие группы настроек входят в шаблон безопасности?
6. Для чего предназначена оснастка «Анализ и настройка безопасности»?
7. Опишите последовательность действий администратора при проведении анализа настроек безопасности операционной системы.
8. Опишите последовательность действий администратора при настройке безопасности операционной системы.
9. Приведите возможные типы результатов анализа параметров безопасности операционной системы.
10. Каким образом можно внести в шаблон текущие настройки безопасности операционной системы?