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 объекта3
ЛАБОРАТОРНАЯ РАБОТА №2. Двухфакторная аутентификация в программном обеспечении на основе технологии SSO17
ЛАБОРАТОРНАЯ РАБОТА №3. Дискреционный механизм разграничения доступа к файловым объектам
ЛАБОРАТОРНАЯ РАБОТА №4. Мандатный механизм разграничения доступа к файловым объектам
ЛАБОРАТОРНАЯ РАБОТА №5. Разграничение доступа к устройствам
ЛАБОРАТОРНАЯ РАБОТА №6. Ограниченное использование программ
ЛАБОРАТОРНАЯ РАБОТА №7. Аудит событий безопасности операционной системы90
ЛАБОРАТОРНАЯ РАБОТА №8. Анализ и настройка параметров безопасности операционной системы

ЛАБОРАТОРНАЯ РАБОТА №1 АУТЕНТИФИКАЦИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ ПРИ ПОМОЩИ ФИЗИЧЕСКОГО ОБЪЕКТА

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

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-кол: «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).

🖻 Изменить пароль: eToken	×
изменить пароль eToken	
Текущий пароль для eToken:	
Новый пароль для eToken: ••••••• Подтверждение: •••••• Пароль должен отвечать требованиям к сложности пароля, заданным для устройства.	
Текущий язык: EN	_
ОК Отмена	

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.

😑 Пе ре име новать	eToken	
	Переименовать eToken	eloken
Новое имя	a eToken: User	
Использо	овать это имя для идентификац	ии eToken
	ок	Отмена

Рисунок 3 – Переименование eToken

🖴 eToken PKI Client Properties			
eToken	YOUR KEY TO *SECURITY	💁 i ? 😫	e 32
	🕺 🖡 🐺 🛅 绪 🤫 🌶		
the set of	Имя —	eloken	^
eToken PKI Client	Категория eToken	Физическое	
🖃 🚘 устроиства	Имя устройства считывания	AKS irdh 0	
	Серийный номер	0x4d43a014	
Пастроики	Общий объем памяти	32768	
— 💁 настроики етокеп PKI Client	Свободное место на смарт-карте eToken	27777	
	Версия оборудования	1.2	1
	Версия встроенного ПО	0.4	
	ID смарт-карты	26 20 be 18 16 1e	
	Название продукта	eToken PRO	
	Модель	Token P0514 F4.2.5.4	
	Тип смарт-карты	Card OS	
	Версия ОС	CardOS/M4.01 (C) Siemens AG 1994-2001	
	Mask version	Неприменимо	
	Цвет	Синий	
	Поддерживаемый размер ключа	1024	~
		-	
	SECURING THE GLOBAL VILLAGE	Aladd	lin

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.

	Качество пароля	Дополнительно					
	Минимальная длина	пароля (символов)		6	5	-	
😑 - eToken PKI Client	Максимальный перио	д использования (д	ней)	C)	\$	
🖨 🚔 Устройства	Минимальный перио,	д использования (дн	ей)	C)	\$	
🖻 🖘 User	Период уведомления	ю об истечении срока	а действия пароля (дней	i) ()	\$	
Настройки eToken PKI Client	Размер истории паро	лей		1	10	\$	
	Число повторов			3	3	\$	
	Пароль должен отве	чать требованиям к	сложности пароля	4	Активный	\$	
	Установка сло	жности вручную					
	Цифры			F	азрешить	÷	
	Прописные буквы			F	разрешить	-	
	Строчные буквы			F	азрешить	\$	
	Специальные симе	олы		F	разрешить	\$	
		_					
			Установить по умолчанию	Сохранит	гь	Сброс	

Рисунок 5 – Настройка параметров качества PIN-кода eToken

3. Администрирование eToken

В режиме «Подробный вид» выберите подключенный еТокеп и на панели инструментов выберите «Инициализировать еТокеп». В окне «Параметры инициализации еТокеп» (рис. 6) установите PIN-код еТокеп или требование к обязательной смене пароля при первом использовании (если оставите PIN-код по умолчанию), а также PINкод администратора еТокеп. Также можно установить максимальное количество ошибок ввода соответствующих PIN-кодов и имя еТокеп. Отформатируйте еТокеп. 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.

2 Инициализировать eToken	×
Параметры инициализации eToken	
Иня eToken: User	
 ✓ Пароль пользователя: ●●●●●●● Максимальное число ошибок при входе: 15 	\$
✓ Пароль администратора: ●●●●●●● Максимальное число ошибок при входе: 15 Подтверждение: ●●●●●●● входе: 15	*
Примечание: для разблокировки устройства введите пароль администратора.	
Дополнительные настройки	
При первом входе необходимо изменить пароль Дополнительно	
Текущий язык: EN	
Запуск Закрыть	

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.

🖴 Вход: User	
Вход с правами адм	инистратора на еТокеп еТокеп
Введите пароль а	дминистратора eToken
Имя eToken:	User
пароль.	Текущий язык: EN
	ОК Отмена

Рисунок 7 – Ввод пароля администратора

Настройки интерфейса утилиты «Свойства eToken» можно изменять через «Групповые политики», используя соответствующий административный шаблон. Откройте ochactky 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».

🚡 Групповая политика		
Консоль Действие Вид Справ	жа	
← → 🖻 🗷 🛱 🚱 🔮	Свойства: Access Control	? 🛛
Contrinue Toxanisheir Korehsorer Kordprypaus Inporpare Change Token KCI General Settings Cartificate Store Se Monitor Settings Cartificate Store Se Monitor Settings Corto Corto	Пераметр Объяснение Access Control He sagan Ø Brunoven O Trunoven ChangePassword 1 * Warner O Trunoven ChargePassword 1 * UnlockEtoken 1 * UnlockEtoken 1 * OpenAdvanced/lew 0 * OpenAdvanced/lew 0 * Предыдуший параметр	
	ОК Отмена Пр	оименить
	Расширенный / Стандартный /	

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».

🂐 eToken Network Logon Prot	file Wizard 5.1	\mathbf{X}
Logon Information		Aladdin
Enter a user name and domain for the	new profile.	
User name:	User	
Log on to:	XP-MSDN (this computer)	~

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.

Domain Password for Profile	Aladdi
Use current domain password	
Current password:	1
Confirm password:	
🔿 Create new domain password	
Current domain password:	
	Read current domain password from eToken
O Manual password	
New password:	
Confirm password:	
🔘 Random password	
Random password length:	
Update domain password in directory	

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 OC. После входа в OC отключите eToken – в этом случае сеанс пользователя блокируется. Подключите eToken и разблокируйте ceaнс.

Вход в Windows	
eToken Your key to esecurity	
	SECURING THE GLOBAL VILLAGE
_	
Пользователь: User	<u>•</u>
Token password:	
I forgot my eToken Password	
Create Profile on Token	
EN ОК Отмена Завершение раб	оты Параметры <<

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 еТокеп для записи на него нового пароля.

Смена пароля	
	securing the global village
Пользователь:	User
Вход в:	
Новый пароль:	
Подтверждение:	
Token password:	Г Архивация ОК Отмена

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 OC («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.

💐 eToken Network Logon Profile Wizard 5.1		
Profile Selection		Aladdin
Select a profile: O Add a new profile		
 Select an existing profile Update the existing profile Remove the existing profile 	User - XP-MSDN	~

Рисунок 13 – Выбор существующего на eToken профиля

Domain Password for Profile	Aladdi
O Use current domain password	
Current password:	
Confirm password:	
Oreate new domain password	
Current domain password;	******
Manual password	Read current domain password from eToken
New password:	•••••
Confirm password:	•••••
O Random password	12 DECIS
Random password length:	
Undate domain password in directory	

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.

zard 5.1	
	Aladdin
User - XP-MSDN	×
	card 5.1 User - XP-MSDN

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 еТокеп, 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.

Jomain Password for Profile	Aladdi
O Use current domain password	
Current password:	
Confirm password:	
Oreate new domain password	
Current domain password:	•••••
	Read current domain password from eToken
O Manual password	
New password:	
Confirm password:	
Random password	
Random password length:	14 🗘
Undate domain password in directory	

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.

Смена пароля	
	RITY Aladdin SECURING THE GLOBAL VILLAGE
Пользователь: Вход в:	user
Token password:	<u> </u>
EN	Архивация ОК Отмена

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 «С:\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.

🚡 Групповая политика	
Консоль Действие Вид Справ	жа
	Свойства: Allow Standard Windows Logon 🛛 ? 🔀
 Политика "Локальный компьютера Конфикурация компьютера Конфикурация програми Конфикурация Windows Конфикурация Windows Сокстема Сокстема Сокстема Сокстема Конфикурация пользователя Конфикурация пользователя Конфикурация пользователя Конфикурация ильзователя Конфикурация Windows Адиинистративные шаблс 	Параметр Объяснение Allow Standard Windows Logon Не задан Включен Отключен Allow Standard Windows Logon © Предыдущий параметр Следующий параметр ОК Отмена Применить
	\ Расширенный / Стандартный /

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).

Вход в Windows	
eToken	
Пользователь:	user
Token password:	
	I forgot my eToken Password
	Create Profile on Token
EN	Отмена Завершение работы Параметры <<

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.

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

Таблица 1 – Варианты заданий

8	Макс. срок действия пароля – 30 дней. За сколько дней пользователь должен быть предупреждён о смене пароля – 3 лня	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).

						_
	1.72			~		
and the second s	Формат архива:	7z	~	Режим изменения:		
	Уровень сжатия:	Нормальный	~	Добавить и заменить		
	Метод сжатия:	LZMA	~	Опции		
- ·	Размер словаря:	16 MB	~	Сжимать открытые для за	лиси файлы	
New Form	Размер слова:	32	~	Шифрование		
Drag and drop the hand icon to an application window to add it.	Размер блока:	2 GB	~	Введите пароль:		
Alternative form handling	Число потоков:	1	/1	Повторите пародь:		
	Объем памяти для упак	овкис	186 MB			_
	Объем памяти для расп	таковки:	18 MB	Показать пароль		
	Разбить на тома размером (в байтах):		Метод шифрования:	AES-256	~	
			~	Шифровать имена файлов		
	Параметры:					

Рисунок 2 – Выбор окна для создания шаблона

Template List	Добавить к архиву Profile Settin	igs 👂
Personal Folders Password	Password Po	olicy 👂
Windows Live Messenger - S	Добавить к архиву	
Под*Добавитькархиву	Form name Advanced	a D
	Добавить к архиву	
	Default form settings	
	☑ Automatic data submission	
	Enforce	
	Always display the eToken SSO window on top when processing this form	
	Custom submit button definition	
	Use custom submit button	
	Submit button caption:	
	Field information	
	Display Name Script Field Default Data	
	Delete Add Add Virtual Edit p	
New Open Save Save As Delete	Add Form Delete Form	

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».

Добавить к архиву			×
Архив:			
1.7z		*]
Формат архива:	7z 💌	Режим изменения:	
Уровень сжатия:	Нормальный 🗸	Добавить и заменить	~
Метод сжатия:	LZMA 💌	Опции	
Размер словаря:	12 MB	🗌 Сжимать открытые для записи файлы	
Размер слова:	New Field	Вание	
Размер блока:	Drag the hand icon, and drop the application field to be add	piton ded. те пароль:	-
Число потоков:		онте пароды:	
Объем памяти для упаковк	и: 148 MB		
Объем памяти для распако	вки: 14 МВ	🗌 Показать пароль	
Разбить на тома размером	(в байтах):	Метод шифрования: AES-256	~
	~	📃 Шифровать имена файлов	

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).

Добавить к архиву	Profile Settings 👂	Field display name	
	Password Policy D	Field2	
Добавить к архиву		Field type	
Form name	Advanced N	Password	
Добавить к архиву		Field role	
Default form settings Automatic data submission Enforce Always display the eToken SSO window on top when proc Custom submit button definition Use custom submit button	essing this form	Password General Password New Password Confirm Password Confi	le
Field information Display Name Script Field Delete Add Add Virtual	► Edit ►	More	

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.

Добавить к архиву	Profile Settings 👂	Field display name	
	Password Policy N	Повторите пароль	
Добавить к архиву		Field type	
Form name	Advanced N	rassword	
Добавить к архиву		Field role	
Default form settings		Password	
Automatic data submission		Data value is visible	
Enforce		Lock visibility	
Always display the eToken SSO window on top when proce	ssing this form	 Field is visible during profile creation Allow data entry during profile creat 	tion
Custom submit button definition		Allow data modification when editing a	profile
Use custom submit button Submit button caption:		Generate random value	fore 🤝
Field information			
Display Name Script Field Default Data			
Введите пароль s_Field1			
повторите пар 5_петод			
Dalata Add Add Mitral			2
		1	

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.

Добавить к архи	ву	\mathbf{X}
Архив:		
1.7z	😫 e Token SSO - New Profile 🛛 🛛 🔀	✓ …
Формат архива:	eToken your key to esecurity	
Уровень сжатия:	Profile Name: Добавить к архивч	
Метод сжатия:		
Размер словаря:	Enter values for the following fields.	и файлы
Размер слова:	Введите пароль	
Размер блока:	Повторите пароль	
Число потоков:		
Объем памяти для	Automatio submit	
Объем памяти для	 Automatic submit Set as default for application 	
Разбить на тома р	Verify site identity Domain name without server	S-256 💌
	O Exact domain name	
Параметры:	OK Cancel	
	ОК Отмена	Помощь

Рисунок 10 – Создание профиля на eToken для окна приложения

Созданные профили отображаются в основном окне утилиты еToken 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).

🕌 eToken SSO 5.1							X
eToken your	KEY TO	esecui	RITY				
9 8 S S	51	8	()	61	S	ĩ	»
Profile Name		l	.ast Modi	fied			
🐘 eToken Network Logon - XP-MSDN	I\User						
💼 📴 Добавить к архиву			1/9/2010) 1:55 PM			
🗐 📴 Извлечь		1	1/9/2010) 1:55 PM			
					M	lore Deta	ails
					_		_

Рисунок 11 – Список профилей, сохранённых на eToken

🕌 eToken SSC) - More Det	tails							
eToker	r	YOU	RKE	Y ТО	ese(EURIT	ΓY		
Profile Name	Добавить к	архиву							
Form	Добавить к	архиву							*
Field Values-									
Введите парол	пь	•••••							
Повторите пар	роль	•••••							
Show unlock	ted values								
Automatic su Set as defaul	lt								
Use advance	ed Fill & Submit	t mode							
🔲 Verify site ide	entity								
🔿 Domain	name without :	server							
🔘 Exact de	omain name								
							_		
								ок	Cancel

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.

💐 eToken SSO Template Editor			
eToken	YOUR KEY TO esecurity		SECURING THE GLOBAL VILLAGE Aladdin
Template List	КИБЭВС - Комплексная Информацион Ра Ра	ofile Settings 🕨	Template name КИБЭВС - Комплексная Информа
 Windows Live Messenger - S Добавить к архиву Изалечь КИБЭВС - Комплексная И 	КИБЭВС - Комплексная Form name КИБЭВС - Комплексная Информационная	Advanced D	Display profile details Enable profile editing Enable profile edietion Creation officst profile is mandatory
	Default form settings Automatic data submission		Enforce logon Maximum number of profiles on token:
	Enforce Aways display the eToken SSO window on top when processing Custom submit button definition	this form	More 🛡
	Use custom submit button Submit button Field information		
	Display Name Script Field Default Data login s_login password s_password		
	Delete Add Add Virtual	Edit	2
New Open Save Save As Delete	Add Form Delete Form		

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 еToken. 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

🚢 eToken SSO - New Pro	file 🔀	
eToken	YOUR KEY TO eSECURITY	
Profile Name: тронно-Выч	ислительных Систем, НОВОСТИ	C
Enter values for the following fie	elds.	
login	kaa2	KUNDAR
password	•••••	<u>6</u> Q ⊠
8	введите запрос	
Automatic submit		Авторизация.
Set as default for application		Пожалийста ввелите:
 Venity site identity Domain name without site 	erver tusur.ru	Логин: каа?
 Exact domain name 	keva.tusur.ru	Пароль:
	OK Cancel	Войти

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.

🚡 Групповая политика	Свойства: Profile Quota	×
Консоль Действие Вид Справ Справ Политика "Локальный компьютер Конфигурация компьютерани Конфигурация молькотерани Конфигурация Windows Административные шаблс Скотема Система Система Система Система Конфигурация пользователя Конфигурация пользователя Конфигурация пользователя Конфигурация пользователя Конфигурация пользователя Конфигурация пользователя Конфигурация пользователя Административные шаблс	Параметр Объяснение Profile Quota Не задан Включен Отключен Profile Quota True 4	
	Предьидущий параметр Следующий параметр ОК Отмена Примени	ть
Рисунок 16 – Ограничение	Profile Quota Show / Set the 'Show migration prompt when SSO Client starts' О Template Folder Path Максимального количества профилей сохраняем	1е за, 1е за, 1е за, 1е за, (БІХ

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

Залание

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

* – для демонстрации войдите под учётной записью «User» и запустите какую-либо оснастку ММС 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 е Token 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 webсайтов 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).

бшие Е	ид	Типы файл	юв	Автономны	е файлы	
		1	222201			
Предс	тавле	ние папок				
) H	1ожно приме апример, "Та	нить абли	ь вид, выбран іца'' или ''Плі	ный для этой папки итка", ко всем папки	I, BM.
	(Применить к	ю во	сем папкам	Сброс для всех п	апок
Дополн	лель	ные парамет	ры:			
Φ	йлы і	и папки				~
	Авто	матический і	поис	ск сетевых п	апок и принтеров	
	Boco	танавливать	пре	жние окна п	апок при входе в си	стем
	Выв	одить полный	й пут	ъ в панели а	дреса	
	Выв	одить полный	й пут	ъ в строке з	аголовка	
	Испо	ользовать пр	осто	ой общий дос	ту <mark>п к ф</mark> айлам (реког	иендуе
	Нек	эшировать э	скиз	зы		
	Откр	ывать кажду	јю па	апку в отдел	ьном окне	
	Отоб	і́ражать "Па⊦	юль	управления'	' в папке "Мой комп	ьют
	Отоб	і́ражать опис	ани	е для папок і	и элементов рабочег	TO C1
V	Отоб	і́ражать прос	той	вид папок в	списке папок "Пров	одні 🞽
<						>
				-		
					Восстановить умол	чания
				-		

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).

безопасност Типы объектов
Размещение
Проверить имена
· · · · · · · · · · · · · · · · · · ·
1

Рисунок 2 – Добавление нового пользователя

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



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).

войства: Изменение	? 🔀	Свойства: Запись	? 🛛
Общие Доступ Безопасность Настройка		Общие Доступ Безопасность	Настройка
Группы или пользователи:		Группы или пользователи:	
SYSTEM		SYSTEM	
g user (XP-MSDN\user)		user (XP-MSDN\user)	
🖸 Администратор (XP-MSDN\Администратор)		🖸 Администратор (XP-MSDN\A	дминистратор)
🕵 Администраторы (XP-MSDN\Администраторы)		🗖 Администраторы (XP-MSDN)	Администраторы)
🕵 создатель-владелец		🕵 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	
Добавить	Удалить		Добавить Удалить
Разрешения для user Разрешить	Запретить	Разрешения для user	Разрешить Запретить
Полный доступ		Полный доступ	
Изменить		Изменить	
Чтение и выполнение		Чтение и выполнение	
Список содержимого папки		Список содержимого папки	
Чтение		Чтение	
Запись		Запись	
		Doofe to poopourousia	— — <u> </u>
Чтобы задать особые разрешения или Доп параметры, нажмите эту кнопку:	олнительно	Чтобы задать особые разрешени параметры, нажмите эту кнопку:	я или Дополнительно
ОК Отмена	применить	UK	Отмена Применить
Duounou 5 Votonopu		Duornor 6	Voteriopro

Рисунок 5 – Установка разрешения «Изменить»

разрешения «Запись»

уппы или пользователи.			Груп	пы или польз	юватели:		
SYSTEM	SYSTEM user (XP-MSDN\user)						
🖸 user (XP-MSDN\user)							
🖸 Администратор (XP-MSDN\Администратор)				🙎 Администратор (XP-MSDN\Администратор)			
🕼 Администраторы (XP-MSDN	1	🙀 Администраторы (XP-MSDN\Администраторы)					
🗊 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ			G	СОЗДАТЕЛЬ	-ВЛАДЕЛЕЦ		
	Добавить	Удалить				Добавить	Удалить
азрешения для user	Разрешить З	апретить	Pasp	ешения для	user	Разрешить	Запретить
Полный доступ			По	олный достуг	ě.		
Изменить			Из	зменить			
Чтение и выполнение			Чт	гение и выпо	пнение	V	
Список содержимого папки			Cr	писок содерж	имого папки		
Чтение	V		Чт	гение		V	
Запись			3a	апись			
		- M	1.0-		00000		
гобы задать особые разрешен	ия или Допо	лнительно	Чтоб	ы задать ос	бые разрешения	или До	полнительно
раметры, нажмите эту кнопку	; C		napa	метры, нажм	ите эту кнопку:	-	

Рисунок / – 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.

бщие везопасность Свод	ка	
Группы или пользователи:		
SYSTEM		
😰 user (XP-MSDN\user)		
🕵 Администратор (XP-MSD	N\Aдминистратор)	
Парминистраторы (XP-M9)	DNVAдминистратор	ы
		11
	Дооавить	эдалить
Разрешения для SYSTEM	Разрешить	Запретить
Полный доступ	×	
Изменить	1	
Чтение и выполнение	1	
Чтение	V	
Запись	1	
Особые разрешения		
	A REPORT OF A R	
Чтобы задать особые разреи	иения или Дог	толнительн

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.

Цля просмі снопку "Из Элементы р	пра свед ченить". назрешен	цений об особ иий:	ых разрешениях вы	іберите элемент ра	зрешения и нажмите
Тип	Имя		Разрешение	Унаследован	Применять к
Paspe	SYSTEM		Полный доступ	D:N	Для этой папки, ее
Paspe	аминис	граторы (Х	Полный доступ	D:V	Для этой папки, ее
Paspe	Адменнис	гратор (ХР	Полный доступ	D:\	Только для этой пап
Paspe	СОЗДАТІ	ЕЛЬ-ВЛАД	Полный доступ	D:\	Только для подпапо
Добави	ъ	Изменить	. Удалить		
Добави Наследо добавля	ть вать от р я их к яв	Изменить родительского но заданным	. Удалить о объекта примени в этом окне.	мые к дочерним об	ьектам разрешения,
Добави Наследо добавля Замения примени	ты вать от р я их к яв ть разрец мыми к ;	Изменить родительского но заданным цения для все дочерним объ	. Удалить о объекта примени в этом окне. х дочерних объекто ектам.	мые к дочерним об	ьектам разрешения, > разрешениями,

Рисунок 14 – Дополнительные параметры безопасности

Имя: user (XP-MSDN\user) Изменить	Имя: user (XP-MSDN\user) Изменить
Трименять: Для этой папки и ее подпапок 🛛 👻	Применять: Для этой папки, ее подпапок и файлов
Разрешения: Разрешить Запретить	Разрешения: Разрешить Запретить
Полный доступ Обзор папок / Выполнение Файлов Осаержание папки / Чтение данных Чтение атрибутов Чтение дополнительных атрибутов Создание Файлов / Запись данных Запись атрибутов Запись дополнительных атрибутов Даление Чтение разрешений Vаление Применять эти разрешения к объектам и контейнеран только внярти этого контейнера	Полный доступ Обазор папок / Выполнение файлов Содержание папки / Чтение даннык Чтение дополнительных атрибутов Чтение дополнительных атрибутов Создание файлов / Запись данных Запись атолог / Дозапись данных Запись дополнительных атрибутов Зались дополнительных атрибутов Зались атрибутов Заление Чтение разрешения к объектам Колтейнерам только внутри этого колтейнерам только внутри этого

Рисунок 15 – Элементы разрешений для «Списка содержимого папки»

Рисунок 16 – Элементы разрешений для «Чтения»



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).

Имя: user (XP-MSDN\u	iser)	Изменит	ъ	Имя: user (XP-MSDN\us	(re	Изменить
Применять: Для этой па	пки, ее подпапок и фа	айлов	~	Применять: Для этой пап	ки, ее подпапок и ф	айлов 😽 😽
Разрешения:	Разрешит	ь Запрети	гь	Разрешения:	Разрешит	ъ Запретить
Полный доступ			~	Полный доступ		
Обзор папок / Выполн	ение файлов 🔽			Обзор папок. / Выполнен	ие файлов 📃	
Содержание папки / Ч	гение данных 🔽			Содержание папки / Чте	ние данных 🔽	
Чтение атрибитов				Чтение атрибутов		
Чтение дополнительнь	их атрибитов	Ē		Чтение дополнительных	атрибитов	
Создание файлов / Заг	пись данных 🔽			Создание файлов / Запи	сь данных 🔲	
Создание папок / Доз	апись данных 🔽			Создание папок / Дозаг	ись данных	
Запись атрибутов		Π		Запись атрибутов		Ē
Запись дополнительны	их атрибутов 🔽			Запись дополнительных	атрибутов	
Удаление подпапок и с	райлов			Улаление поллалок и фа	айлов 🗌	
Удаление			- -	Чладение		- H -
Чтение разрешений			-	Чтение разрешений		Ē.
C			~	C		
Применять эти разре. и контейнерам только контейнера	иения к объектам внутри этого	Очистить	все	Применять эти разреше и контейнерам только в	ния к объектам нутри этого	Очистить все

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).

азрешения владелец	Действующие разрешения	
Вы можете стать владе	льцем объекта, если вы имеете соответствующие разрешения.	
Текущий владелец этог	о элемента:	
user (XP-MSDN\user)		
Изменить владельца на	£	
Имя		
🗌 Заменить владельца	а субконтейнеров и объектов	

Рисунок 25 - Вкладка «Владелец»

растро	ика
руппы или пользователи:	
SYSTEM	
🔮 user (XP-MSDN\user)	
🖸 user1 (XP-MSDN\user1)	
🕵 Администраторы (XP-MSD)	N\Администраторы)
🕵 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	
	Лобавить Члалить
	Horsen C.
азрешения для user1	Разрешить Запретить
азрешения для user1 Полный доступ	Разрешить Запретить
'азрешения для user1 Полный доступ Изменить	Разрешить Запретить
Разрешения для user1 Полный доступ Изменить Чтение и выполнение	Разрешить Запретить
азрешения для user1 Полный доступ Изменить Чтение и выполнение Список содержимого папки	Разрешить Запретить
Разрешения для user1 Полный доступ Изменить Чтение и выполнение Список содержимого папки Чтение	Разрешить Запретить

Рисунок 26 - Предоставление прав пользователю «user1»

Войдите под учётной записью «user1».

Попытайтесь перейти в каталог «D:\Изменениe\test» при помощи иерархического представления каталогов в «Проводнике». Переход невозможен, потому что у пользователя «userl» 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 «userl» 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

Имя: Администраторы (XP-MSD)	₩₩Админи	Измени	гь
Трименять: только для этого объе	жта		×
разрешения:	Разрешить	» Запрети	ть
Полный доступ Обзор папок / Выполнение файл Содержание папки / Чтение данн Чтение атрибутов Чтение дополнительных атрибуто Создание файлов / Запись данн Создание папок / Дозапись данн Запись атрибутов Запись дополнительных атрибуто Удаление Чтение разрешений Смена разрешений	ао мана мана мана мана мана мана мана ма	<u>.</u>	
Применять эти разрешения к об и контейнерам только внутри эт	љектам (Гл Очистить	все

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).

Разрешения	Владелец	Действующие разрешения	
Вы можете Текуший вл	стать владе наделец этог	льцем объекта, если вы имеете соответствующие разрешения. ю элемента:	
user1 (XP-M	ISDN\user1)		
Изменить в	ладельца на	a:	
Имя			

Рисунок 29 – Смена владельца файла

Безопас	сность
i)	У вас есть разрешение только на просмотр текущего владельца для Новый том (D:). ОК

Рисунок 30 – Ошибка смены владельца файла

Разрешения	Аудит	Владелец	Действующие разрешения	
Вы можете	стать вл	адельцем о	бъекта, если вы имеете соответствующие разреш	шения.
Текущий вл	аделецз	этого элеме	нта:	
Администр	аторы (Х	P-MSDN \Ag	иминистраторы)	
Изменить в	падельц	a Ha:		
NMR				
Имя	истратор	o (XP∙MSDN'	Vадминистратор)	
Имя	истратор истратор	» (XP-MSDN ры (XP-MSD)	Чадминистратор) NЧадминистраторы)	
Имя Д. Админи Д. Админи	истратор истратор	» (XP-MSDN ры (XP-MSD)	Фдминистратор) N\Администраторы)	
Имя Д Админа Д Админа	истратор истратор	о (XP-MSDN ры (XP-MSDI	Фдиненстратор) МФдиненстраторы)	
Имя Админи Админи Админи	истратор истратор	ы (XP-MSDN) вы (XP-MSDI	Чадиевистратор) NAдиевистраторы)	
Имя В Админи Мамини	«стратор «стратор	ы (XP-MSDN' ры (XP-MSDI	Чадненистратор) NЧарьянистраторы)	
Имя 😰 Админи 🚮 Админи	кстратор	р (XP-MSDN' ры (XP-MSDI	Чадненктратор) NNАрыявистраторы)	
Имя 😰 Админи 🚮 Админи	истратор истратор	D (XP-MSDN)	Чадненотратор) NVАднеенотраторы)	
Имя இ Админи М Админи	кстратор) (XP-MSDN ры (XP-MSDI	Чадненистратор) NNарьевистраторы)	

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

тарамет	р локальной безопасности
F	Овладение файлами или иными объектами
Админ	истраторы
Добав	ить пользователя или группу] Удалить
Добав	ить пользователя или группу) Удалить

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 Откройте «Разрешения» вложенного объекта. вкладку в лополнительных 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».

5-52-56-56-56-56-56-56-56-56-56-56-56-56-56-	Аудит	Владелец	Действующие разр	ешения	
(ля просм нопку "Из лементы	отра свед «менить".	цений об осо(иий:	бых разрешениях вь	іберите элемент ра:	зрешения и нажмите
Тип	имя	ии.	Разрешение	Унаследован	Применять к
Paspe Paspe Paspe Paspe Paspe	user (XP-n SYSTEM Админист Админист СОЗДАТІ	изоручизет) граторы (Х гратор (ХР ЕЛЬ-ВЛАД	чтение Полный доступ Полный доступ Полный доступ Полный доступ	<не унаследов <не унаследов <не унаследов <не унаследов <не унаследов	для этой папки, ее Для этой папки, ее Для этой папки, ее Только для этой пап Только для подпапо
Добави	ть (овать от р яя их к яві	Изменить. юдительског ю заданным	Удалить ю объекта примени в этом окне.	мые к дочерним объ	ьектам разрешения,

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 запись объектам». Улалите учётную «user» ИЗ чиспа санкционированных пользователей каталога «Чтение1». B 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.

	Аудит Владелец	Действующие разр	ешения	
Для просмі кнопку "Изі Элементы г	этра сведений об особ менить". разрешений:	ых разрешениях вы	иберите элемент ра	зрешения и нажмите
Тип	Имя	Разрешение	Унаследован	Применять к
Paspe Paspe Paspe Paspe	SYSTEM Администраторы (Х Администратор (ХР СОЗДАТЕЛЬ-ВЛАД	Полный доступ Полный доступ Полный доступ Полный доступ	D:X D:X D:X D:X	Для этой папки, ее Для этой папки, ее Только для этой пап Только для подпапо
Добави Наследо добавля	гь Изменить звать от родительского я их к явно заданным гь разрешения для все		мые к дочерним обя ов заданными здесь	ьектам разрешения, » разрешениями,

Рисунок 35 – Включение принудительного наследования

бщие везопасность	Сводка
руппы или пользовате	ели:
SYSTEM	
user (XP-MSDN\us	er)
Администратор (×	P-MSDN\Aдминистратор)
Администраторы	(XP-MSDN\Администраторы)
🕵 Пользователи (ХР	-MSDN\Пользователи)
	Добавить 9далить
^р азрешения для	Разрешить Запретить
Полный доступ	
Изменить	
Чтение и выполнени	
Чтение	
Запись	
Особые разрешения	
нторы задать осорые зараметры, нажмите з	разрешения или Дополнительн
	r g raioring.

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.

^р азрешения	Аудит	Владелец	Действующие разрешен	ия		
В списке от на основе в Группа или г	ображаю сех имен пользова	лтся разреш ощихся разр атель:	ения, которые будут даны ешений.	выбранной гр	уппе или пользователю	6
user					Выбрать.	
Действующи	ие разре	шения:				
Полный	ароступ					
🔲 Обзор г	папок / В	ыполнение	файлов			
Содерж	ание па	пки / Чтение	данных			
🔲 Чтение	атрибут	ов				
🔲 Чтение	дополни	пельных атр	рибутов			
🔲 Создан	ие файл	ов / Запись.	данных			
🔲 Создан	ие папок	/ Дозапись	данных			
🔲 Запись	атрибут	ов				
🔲 Запись	дополни	пельных атр	оибутов			
🔲 Удален	ие					
🔲 Чтение	разреши	ений				
🔲 Смена	разреше	ний				
🔲 Смена і	владелы	ца				
						_
			_			
					Отмена Примен	HULL

Рисунок 37 – Действующие разрешения пользователя

Разрешения	Аудит	Владелец	Действующие разрешения	
В списке от на основе в	ображак сех имен	отся разреш ощихся разр	ения, которые будут даны выбранной гр ешений.	уппе или пользователю,
группа или г	тользов	атель:		
user				Выбрать
Пействиющи	ue paspe	шения.		
Полині	й постип			
	лапок / Е	вполнение	daŭ nos	
Conep*	ание па	пки / Чтение	анных	
И Чтение	атрибит	OB		
✓ Чтение	дополны	пельных ато	рибитов	
🔲 Создан	ие файл	ов / Запись	данных	
🔲 Создан	ие папон	. / Дозапись	данных	
🔲 Запись	атрибут	OB		
🔲 Запись	дополны	ательных атр	рибутов	
🔲 Удален	ие			
🗹 Чтение	разреш	ений		
🔲 Смена ј	разреше	ний		
🔲 Смена і	владель	ца		

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.

Имя: user		Азменить
Применять: Только для п	одпапок	~
Разрешения:	Разрешить 3	Запретить
Полный доступ Обзор папок / Выполнен Содержание папки / Чта Чтение априбутов Чтение дополнительных Создание файлов / Запи Создание папок / Дозап Запись атрибутов Запись дополнительных	иие файлов ние данных атрибутов ись данных иись данных атрибутов	
Удаление подпапок и Ф Удаление Чтение разрешений Применять эти разреши ✓ и контейнерам только в контейнера	айлов	чистить все

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).

бщие	Доступ	Порты	Дополнительно	Управление цветом	Безопасность	About
8	Для ра необхо Windov	зрешения димо, что из для обы	а общего доступа і бы администратор цего доступа к фа	к этому принтеру 5 настроил брандмаузр йлам и принтерам.	2	
۲	Нет обще	го доступ	а к данному принт	еру		
-01	Общий до	ступ к да	нюму принтеру —			
Cer	евое имя					
с Д В В В В В В В В В В В В В В В В В В В	райверы сли этот ерсиями ополните је искать	принтер д Windows, льные др драйверь	оступен компьют рекомендуется ус айверы, что позво принтера.	ерам с различными становить для него лит пользователям		
			Дополните	льные драйверы]		

Рисунок 40 – Свойства принтера

doPDF v7 Свойства	?
Общие Доступ Порты Дополнительно Управление	цветом Безопасность About
Группы или пользователи:	
🕵 Администраторы (XP-MSDN \Администраторы)	
🕵 Boe	
🕼 Опытные пользователи (ХР-MSDN\Опытные польз 🕼 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	ователи)
Разрешения пля Все	Добавить Удалить Разпешить Запретить
Печать	
Управление принтерами	
Управление документами	
Особые разрешения	
Чтобы задать особые разрешения или параметры, нажмите эту кнопку:	Дополнительно
ОК	Отмена Применить Справка

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				
Cyoberth	Общедоступно	Конфиденциально	Принтер		
Админи- стратор	Полный доступ	Чтение	Полный доступ		
user	Чтение	Изменить, кроме удаления	Печать Управление документами		
user1	Изменить	Нет доступа	Печать		

Вариант 2

<u>.</u>					
CVGLERTH	Объекты				
Субысты	Общедоступно Конфиденциально		Принтер		
Админи-	Полный доступ	Чтение и	Полный доступ		
стратор		выполнение			
user	Изменить	Чтение	Печать		
user1	Чтение и	Изменить	Печать		
	выполнение		Управление		
			документами		

Вариант 3

1					
	Объекты				
Субъекты	Общедоступно	Конфиден-	Текстовый файл в		
	_	циально	«Конфиденциально»		
Админи-	Полный доступ	Список	Нет доступа		
стратор		содержимого			
user	Чтение	Изменить,	Изменить		
		кроме			
		удаления			
user1	Изменить	Нет доступа	Нет доступа		

Вариант 4			
	Объекты		
Субъекты	Общедоступно	Конфиден- циально	Текстовый файл в «Конфиденциально»
Админи- стратор	Изменить	Чтение и выполнение	Нет доступа
user	Чтение	Изменить	Запрет удаления
user1	Полный доступ, кроме смены владельца	Запись	Нет доступа

Вариант 5

1				
~ ~	Объекты			
Субъекты	Общедоступно	Конфиден-	Исполняемый файл в	
		циально	«Конфиденциально»	
Админи-	Полный доступ	Список	Выполнение	
стратор		содержимого		
user	Чтение	Чтение и	Выполнение, запрет	
		удаление	удаления	
user1	Изменить,	Запись	Нет доступа	
	кроме			
	удаления			

Вариант 6

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

Вариант 7

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

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

Вариант 8

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

Вариант 9

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

Вариант 10

1			
	Объекты		
Субъекты	Общедоступно	Конфиден-	Исполняемый файл в
		циально	«Конфиденциально»
Админи-	Чтение	Полный	Изменить
стратор		доступ	
user	Список	Чтение и	Выполнение
	содержимого	удаление	
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.

()	Полномочное управление доступом: Названия уровней конфиденциальности	
Низший	Общедоступно	
Средний	Конфиденциально	
Высший	Секретно	
	Вернуть исходные	
Параметр ог каталогов и конфиденци Лоя возврат	пределяет названия категорий конфиденциальности файлов и уровней допуска пользователей к альной информации. га к названиям, принятым по умолчанию, нажмите кнопки	*

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».

ювый пользоват	ель	<u>?</u> ×
Пользователь:	онфиденциальный	
Полное имя:		
Описание:		
Пароль:	••••	
Подтверждение:	•••••	
Г Потребовать с	чену пароля при следующем і	входе в систему
🔲 Запретить сме	ну пароля пользователем	
🔽 Срок действия	пароля не ограничен	
🔲 Отключить учет	ную запись	
		š
	Созда	ать Закрыть

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 ceanca.

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).

Измене	ние категории конфиденциальности	×
2	При изменении категории конфиденциальности могут быть выполнены дополнительные действия:	
	Присвоение категории конфиденциальности всем вложенным каталогам	
	🔽 присвоение категории конфиденциальности всем файлам в каталоге	
	присвоение категории конфиденциальности скрытым и системным файлам	1000
	ОК]

Рисунок 7 – Изменение категории конфиденциальности вложенных каталогов и файлов

Изменение категории конфиденциальности файла производится аналогично.

Пользователю разрешается доступ к файлу, если уровень допуска категории конфиденциальности файла. пользователя не ниже 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\Koнф.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



Не удается создать файл "Текстовый документ.txt" Отказано в доступе.
ОК

Рисунок 11 - Ошибка создания файла в конфиденциальном каталоге

Войдите под учётной записью «Секретный». Попытайтесь открыть файл «D:\temp\Koнф.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\Koнф.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\Koнф.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.

Конф.txt У вас нет прав на сохранение файлов в этой папке. Для получения разрешения обратитесь к администратору.
Хотите выполнить сохранение в папке "Мои документы" вместо этого



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\Kohф.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 17). Несмотря (рис. на потерю конфиденциальности, копирование будет разрешено, т.к. пользователю было предоставлено конфиденциальной вывода информации на сменные носители (рис. 4).

Secret M	Net 5
<u>.</u>	Это Ваш первый вход на данный компьютер. Для обеспечения нормальной работы операционной системы во время этого сеанса не может производиться работа с конфиденциальными ресурсами. Возможность выбора уровня конфиденциальности сеанса будет предоставлена Вам при следующем входе в систему.
	Рисунок 16 – Первый вход в операционную систему

Вывод файла Р	:\temp\Конф	.txt на внешний но	ситель.
Категория кон	фиденциалы	ности файла будет	г потеряна
the second s			
Разрешить выг	полнение опе	ерации?	(2820)
Разрешить выг	полнение опе	ации?	
Разрешить выг	полнение опе	ации?	

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.

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

Таблица 1 – Варианты заданий

3	D:\Докумен- тация\Отчёты	D:\Документация\ Приёмные документы	D:\Документация\ Информация о сотрудниках
4	D:\Подразде- ления\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:\Подразде- ления\Отдел кадров	D:\Подразделения\ Финансовый отдел	D:\Подразделения \Отдел сбыта
9	D:\Файлы\ Опытные пользователи	D:\Файлы\ Пользователи	D:\Файлы\ Администраторы
10	D:\Документа- ция\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 ceanca?

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 «ММС», 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)



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.

ILISISTEM Dire-RSDMAllow_Access_to_CDRom Dire-RSDMAllow_Excess_to_CDROM Dire-RSDMAllow_Exce	U = 2 = 4	 U = 12 = 14 = 16	= 18 = 20 = 22 =
2 ХР-М50М(user Выделин С Администраторы понедел	ъвсе		
Понедел			
	ыник		
вторн	ик		
Добавить Удалить По умолчанию сред	a		
Сновные четре	pr		
Чтение Запись пятни	ца		
суббо	та		
воскрес	енье		

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 USBпорту 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.

Пользователи	4		+			3
2 XP-MSDN(user	0 = 2 =	4 # 6 !	8 = 10 = 12	14 = 16 = 18	= 20 = 22 =	• 0
<u>Fisce</u>	Выделить все					
	понедельник					
Andrews Vacante Da management	вторник					
Права пользователя Вазрешено	среда					
	четверг					
Запись	пятница					
Извлечение	суббота					
	воскресенье					
	Настройки безопасност	арешенное ги) Белый	время 🔳 - Запре і список USB	щенное время		

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.

🗟 Настройки безопасности 🔹 💽
Управлять доступом к USB HID (нышь, клавиатура, и т.д.) Управлять доступом к USB-принтерам Управлять доступом к USB-сканерам и устройствам обработки изображен Управлять доступом к USB Bluetooth-адаптерам Управлять доступом к устройствам хранения USB Управлять доступом к сетевым картам USB и FireWire
ОК Отмена

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».

🗟 Белый список USB-устрої	іств		? 🛛
База данных USB-устройств			
Описание	ID-устройства Ти	n	
Добавить База данных USE	-устройств	О <u>т</u> ображать	все типы 👻
Белый список USB-устройств			
Пользователи	Устройства		
Пользователи	Описание	ID-устройства	Переинициали Контр
Arfanan Varmen			2
Дооавить	Удалить Редактировать		<u>рагрузить</u> <u>С</u> охранить
		ОК	Отмена Применить

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).

Ē	в База данных USB-устройств					? 🗙
		Доступные USB-устро	йства (Локальный ко	мпьютер):		
	Описание	ID-устройства	Подключено			
	🖃 ᡩ Запоминающее устройство	. USB\VID_0457&PID_0151				
	Запоминающее устройст.	USB\VID_04578PID_0151	Да			
	Добавить Раскрыть все Свер	онуть все	Удаленный ко	мпьютер Показать	все устройства Об	новить
		База данны	ах USB-устройств:			
	Описание	ID-устройства	Тип			
	Папоминающее устройство для	USB\VID_0457&PID_0151	Уникальное ус			
	Удалить Редактировать	0	тображать: Все тип	ы 💙	Загрузить Сох	ранить
				ОК	Отмена При	менить

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).

Описание	ID-устройства	Тип				
≫Запоминающее устройство дл	я USB\VID_0457&PID_015	1 Уникальное	ус			
обавить База данных USB-ус	тройств		Отображ	ать: Все т	илы	
лый список USB-устройств						
Іользователи	Устройства					
Тользователи Пользователи	Устройства Описание		ID-устройства	Перея	инициали Ко	нтр
Ioльзователи Пользователи	Устройства Описание Эапоминающее ус	тройство для	ID-устройства USB(VID_0457&PID_01	Перея 51	инициали Ко V	-17
ользователи Пользователи 🕅 XP-MSDM(user	Устройства Описание Ф Запонинающее ус	тройство для	ID-устройства USB(VID_0457&PID_01	Пере 51	инициали Ко V	-1T >

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, FireWireпорт, 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.

🖉 DeviceLock Management Console							
Консоль Действие Вид Справка							
I DeviceLock	Тип	Дата/Время 💎	Тип устр	Действие	Имя	Информация	Поль:
🖻 🏫 Сервис DeviceLock	🔍 Успех	12.02.2009 15:16:08	Removable	Open	Е:\Зима.jpg	Read	XP-MS
Настройки сервиса	🔍 Успех	12.02.2009 15:16:06	Removable	Open	Е:\Голубые холмы.jpg	Read	XP-MS
Устройства	🔍 Успех	12.02.2009 15:16:06	Removable	Open	Е:\Водяные лилии.jpg	Read	XP-MS
С Разрешения	🔍 Успех	12.02.2009 15:16:06	Removable	Overwrite/Create	Е:\Закат.jpg	Read Write Del	XP-MS
тору Аудит и теневое ко	🔍 Успех	12.02.2009 15:16:06	Removable	Create New	Е:\Зима.jpg	Read Write Del	XP-MS
Болын список обо-у т. К. Белый список ногизанием	🔍 Успех	12.02.2009 15:16:04	Removable	Create New	Е:\Закат.jpg	Read Write Del	XP-MS
Настройки безопас	🔍 Успех	12.02.2009 15:16:03	Removable	Create New	Е:\Голубые холмы.jpg	Read Write Del	XP-M:
🖃 Просмотрщик журнала	Sycnex 9	12.02.2009 15:16:03	Removable	Create New	Е:\Водяные лилии.jpg	Read Write Del	XP-MS
🙀 Просмотрщик журнала	Sycnex 9	12.02.2009 15:16:03	Removable	Open	E:\	DirList	XP-MS
🗄 🌆 DeviceLock Enterprise Serve	Sycnex 9	12.02.2009 15:16:03	Removable	Create New	E:\	DirCreate Write	XP-M:
	Sycnex 9	12.02.2009 15:15:52	Removable	Open	Е:\Закат.jpg	Read	XP-M:
	Sycnex .	12.02.2009 15:15:48	Removable	Open	E:\	DirList	XP-MS
	Screx 9	12.02.2009 13:35:43	USB port	Set Permissions		XP-MSDN	XP-MS
٢	1						>
			and a				
всего: 13							

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).

🚡 Консоль1 - [Корень кон	соли\Просмотр соб	іытий (локал	ьных)\Devic	eLock Log]			- 7 🛛
🚡 Консоль Действие Вид	Избранное Окно	Справка					_ & ×
← → 🗈 📧 🗗 🗟							
🧰 Корень консоли	Тип	Дата	Время	Источник	Категория	Co6	Пользователь
🖻 🛐 Просмотр событий (лока)	🥑 Аудит успехов	12.02.2009	15:16:08	DeviceLock Audit	Отсутствует	4	user
Приложение	💞 Аудит успехов	12.02.2009	15:16:06	DeviceLock Audit	Отсутствует	5	user
B DeviceLock Log	💞 Аудит успехов	12.02.2009	15:16:06	DeviceLock Audit	Отсутствует	4	user
Везопасность	🛃 Аудит успехов	12.02.2009	15:16:06	DeviceLock Audit	Отсутствует	4	user
та система	🛃 Аудит успехов	12.02.2009	15:16:06	DeviceLock Audit	Отсутствует	7	user
	🥑 Аудит успехов	12.02.2009	15:16:04	DeviceLock Audit	Отсутствует	5	user
	🥑 Аудит успехов	12.02.2009	15:16:03	DeviceLock Audit	Отсутствует	5	user
	🥑 Аудит успехов	12.02.2009	15:16:03	DeviceLock Audit	Отсутствует	5	user
	🥑 Аудит успехов	12.02.2009	15:16:03	DeviceLock Audit	Отсутствует	4	user
	🥑 Аудит успехов	12.02.2009	15:16:03	DeviceLock Audit	Отсутствует	5	user
	🥑 Аудит успехов	12.02.2009	15:15:52	DeviceLock Audit	Отсутствует	4	user
	🥑 Аудит успехов	12.02.2009	15:15:48	DeviceLock Audit	Отсутствует	4	user
	🥑 Аудит успехов	12.02.2009	13:35:43	DeviceLock Audit	Отсутствует	22	Администратс
< >	<						>

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).

💐 DeviceLock Management Console (XP-MSDN\Администратор)						
Консоль Действие Вид Справка						
← → 🗈 🖬 🖧 😫 🖓 🕶	-0					
I DeviceLock	Статус	Дата/Время 🗸	Тип устройства	Действие	Имя файла	
🖻 🍰 Сервис DeviceLock	S Vcnex	01.12.2010 10:49:26	Съемные устрой	Запись	Е:\Закат.jpg	
🕀 🍓 Настройки сервиса	<u> </u>					
🖃 🌉 Устройства						
😪 Разрешения						
- 😽 Аудит и теневое копирован						
😥 📄 Белый список USB-устройст						
🕀 國 Белый список носителей						
🕀 🎑 Контентно-зависимые прав						
🔣 Настройки безопасности						
— 📑 Просмотрщик журнала аудита						
🙀 Просмотрщик журнала теневог						
🕀 🌆 DeviceLock Enterprise Server						
🗄 🝈 DeviceLock Content Security Server						

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	Доступ по будням.	Полный доступ.
один носитель в белый	Аудит печати и	Аудит чтения и
список. Полный доступ к	запретов доступа	записи
виртуальным приводам		

Вариант 2

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

Вариант 3

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

1		
Параллельный	Жёсткий диск	Съёмные устройства
порт		
Запрет доступа.	Доступ по будням с 8	Чтение и извлечение.
	до 20 часов.	Аудит всех событий.

Вариант 6

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

Вариант 7

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

Вариант 8

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

Вариант 9

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

Вариант 10

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

🔯 Локальные параметры безопасности		
Консоль Действие Вид ⊆правка ⇐ ⇒ 🗈 🗟 😭		
 Паранетры безопасности Политики учетных записей Политики учетных записей Политики опкрытого ключа Политики опкрытого ключа Политики опкрытого ключа Политики опкрытого ключа Дополнитики опкрытока Дополнительные правила Политики безопасности IP на "Локальный конпьютер" 	Тип объекта Уровни безопасности Дополнительные правила ВП/Понудительный ВП/Пони	

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 «С», чтобы его изменить дважды кликните на уровень безопасности и выберите пункт «По умолчанию». Установите уровень «Неограниченный», в качестве уровня безопасности по умолчанию.

🗊 Локальные параметры безопасности		
Консоль Действие Вид Справка 🗢 🔿 💼 📴 😭		
 Поринтры безолазости Полячку учетак: закой Полячку учетак: закой Полячку учетак: закой Полячку отрантог ключа Полячку безолозости № 1% Полячку кляча, теря 	Иня Э Не разрешено Неограниченный	Списачие Поогранное обеспечнике зипускаться не будат, вне закносности от прав доступе пользователя. Доступ програми к ресурсаи определяется правани пользователя.

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, «ехе». Таким образом, добавляются новые типы файлов, которые учитываются в правиле для пути.

юйства: Принудительный	2
Общие	
Применять политики ограниченного использования:	
🛞 ко всем файлам программ, кроме библиотек. (т	akuk Kak DLL)
🚫 ко всем Файлам программ	
Принечание: Если уровень по унолнанию установлен то приненение политик, ограниченного использования библиктекан потребует установить правила для всех использоваться этой програмной, прежде чем ею стан воспользоваться.	"запрещено", програни к библиотек, ет возможно
Приниенять политики ограниченного использования п следующих пользователей:	рогранен для
Эля всех пользователей	
О Для всех пользователей, кроме локальных ади	венстраторов
ОК Отмена	Понент

Рисунок 3 - Настройка дополнительных параметров

Свойства: Назначе	енные типы файлов	? 🛛		
Общие				
Перечисленные ни исполняемым кодо программным типа Назначенные типы	же типы файлов определяют, что счи м. Они являются дополнением к ста м файлов, таким, как EXE, DLL и VB файлов:	пается індартным iS.		
Расширение	Тип файла	^		
PIF PREG SCR SHS URL VB SWSC C	Ярлык к программе MS-DDS Файл реестра Программа-заставка Фрагмент Ярлык Интернета Файл "VB" Windows Script Component			
Удалить Чтобы добавить тип файла, введите его расширение и щелкните кнопку "Добавить". Расширение: Добавить				
	ОК Отмена	Применить		

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.

Создание правила для хеша 🔹 🕐	×
Общие	
Чтобы перекрыть уровень безопасности по умолчанию, используйте правила. Чтобы выбрать файл, для которого нужно создать хеш, щелкитие "Обзор". Поля атрибутов файла, например, его размер, дата и время создания, заполняются автоматически.	
∠ешируемый файл:	
e3013175d75cb6abbb55f61fdfef7f50:177152:32771	
Информация файла:	
utorrent.exe 174 K5 17.02.2009 14:00:05	
Безопасность: Не разрешено	
Опидание:	
Нежелательное ПО	
ОК Отмена Применить	5

Рисунок 6 - Создание правила для хеша

C:\Docum	nents and Settings\Rustam\Paбочий стол\utorrent.exe
8	C:\Documents and Settings\Rustam\Pa6oчий стол\utorrent.exe Невозможно открыть данную программу из-за политики ограничения применения программного обеспечения. За дополительной информацией обратитесь к системному администратору или откройте "Проснотр событий".

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 нужно ограничивать, например: которыми «%programfiles%\Messenger» и выберите уровень безопасности «Не разрешено». Путь можно указывать и к конкретному файлу, а так же использовать подстановочные знаки «*» и «?», например: $(c:\langle downloads \rangle^*, *)$

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%».

Создание правила для пути 🔹 🔀
Общие
Чтобы перекрыть уровень безопасности по умолчанию, используйте правила.
Путь:
al Settings\Application Data\Microsoft\Outlook\ 0630p
Уровень безопасности:
Не разрешено
Описание:
ОК Отмена Применить

Рисунок 8 - Создание правила для пути

Попоненное	Rupuputo
переменная	эпачение
TEMP TMP	C:\Documents and Settings\Bato\Local C:\Documents and Settings\Bato\Local
	Создать Изменить Удалить
іс <u>т</u> емные перем	<u>Создать Изменить Удалита</u> енные
іс <u>т</u> емные перем Переменная	
истемные перем Переменная Сомбреа Баммар - снож	
ICTENHUE ПЕРЕМ Переменная ComSpec DEVMGR_SHOW FP NO HOST C	<u>создать</u> <u>Изменить</u> <u>Удалит</u> енные Значение C:\WINDOWS\system32\cmd.exe 1 NO
ICTEMHЫE ПЕРЕМ Переменная ComSpec DEVMGR_SHOW FP_NO_HOST_C NUMBER_OF_P.	<u>Создать</u> <u>Изменить</u> <u>Удалит</u> енные Значение С:\WINDOWS\system32\cmd.exe 1 NO . 1
ICTEMHЫE ПЕРЕМ Переменная ComSpec DEVMGR_SHOW P_NO_HOST_C UUMBER_OF_P, DS	<u>Создать</u> <u>Изменить</u> <u>Удалита</u> енные С:\WINDOWS\system32\cmd.exe . 1 NO . 1 Windows_NT

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).

Свойств	a: bootvis 1.3	3.37.msi		? 🛛
Общие	Цифровые под	писи Особые Св	одка	
_Спи	сок подписей —			
И	ия подписав	Электронная п	Штамп времени	
M	crosoft Corpor	Нет данных	25 июня 2003 г. 23:.	
			<u>С</u> ведения	
		ОК	Отмена При	менить

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.

Состав цифровой по	дписи	? 🛛
Общие Дополнительн	ю	
Сведения Эта цифров	о цифровой подпи ая подпись действи	кси тельна.
Информация о подг	исавшем	
Имя:	Microsoft Corporat	tion
Электронная почт	а: Нет данных	
Время подписания:	25 июня 2003 г. 2	23:06:52
		Просмотр сертификата
Подписи других сто	орон	
Имя подписав	Электронная	Штамп времени
VeriSign Time St	Нет данных	25 июня 2003 г. 23:
		Сведения
		ОК

Рисунок 11 - Состав цифровой подписи файла

Сертификат		?×
Общие Состав Путь сертифик	ации	
<u>П</u> оказать: 	~	
Поле	Значение	
Версия Серийный нокер Алгорити подписи Поставшик Действителен с Действителен по Субъект Открытый ключ	V3 61071143000000000034 sha1RSA Microsoft Code Signing PCA, C., 25 мая 2002 г. 7:55:48 25 моября 2003 г. 8:05:48 Microsoft Corporation, Copyri RSA (2048 Bits)	· •
Geo	йства	йл
		ок

Рисунок 12 – Сертификат

Свойства: Microsoft Corporation
Общие
Правило для сертификата
Имя субъекта сертификата:
Microsoft Corporation O6sop
Чтобы просмотреть выбранный сертификат подробнее, щелкните кнопку "Подробнее". Уровень безопасности:
Неограниченный
Описание:
Изменено: 15 мая 2009 г. 1:32:14
ОК Отмена Применить

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

Гаолиг	ца 1 — Распределение задании
Номер варианта	Задания
1	сапод
2	с б по е
3	с в по ж
4	сгпоз
5	с д по и
6	сепок
7	с ж по л
8	с з по м
9	скпоо
10	с л по п

Таблица 1 – Распределение заданий по вариантам

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

a) 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;

e) 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).

🧊 Локальные параметры	безопасности	
Консоль Действие Вид С	правка	
📴 Параметры безопасности	Политика /	Параметр безопас
🕀 🧾 Политики учетных запис	👪 Аудит входа в систему	Нет аудита
🖻 🛄 Локальные политики	🕮 Аудит доступа к объектам	Нет аудита
🕒 🛄 Политика аудита	👪 Аудит доступа к службе катало	Нет аудита
Hазначение прав полі Політичние прав полі	В Аудит изменения политики	Нет аудита
нараметры безопасно	👪 Аудит использования привилегий	Нет аудита
	В Аудит отслеживания процессов	Нет аудита
Политики безопасности І	В Аудит системных событий	Нет аудита
	🕮 Аудит событий входа в систему	Нет аудита
	🕮 Аудит управления учетными за	Нет аудита

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.

Свойства: Аудит входа в систему	? 🛛
Параметр локальной безопасности	
Аудит входа в систему	
Вести аудит следующих попыток доступа:	
ОК Отме	на Применить

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).

📕 Управление компьютером							ĺ.	. 🗗 🗙
📕 Консоль Действие Вид Окн	ю Справка							_8×
)							
💻 Управление компьютером (локаль	Тип	Дата	Время	Источ	Категория	Соб	Пользователь	Компьют
🖃 🌇 Служебные программы	<i>З</i> Аудит успехов	14.09.2011	11:31:12	Security	Вход/выход	538	Администратор	XP-MSDN
🖃 🔝 Просмотр событий	💰 Аудит успехов	14.09.2011	11:30:24	Security	Использование	576	Администратор	XP-MSDN
Приложение	🕜 Аудит успехов	14.09.2011	11:30:24	Security	Вход/выход	528	Администратор	XP-MSDN
Безопасность	🕜 Аудит успехов	14.09.2011	11:30:24	Security	Вход учетной за	680	SYSTEM	XP-MSDN
СИСТЕМА	🔒 Аудит отказов	14.09.2011	11:30:18	Security	Вход/выход	529	SYSTEM	XP-MSDN
	🔒 Аудит отказов	14.09.2011	11:30:18	Security	Вход учетной за	680	SYSTEM	XP-MSDN
	💰 Аудит успехов	14.09.2011	11:30:11	Security	Вход/выход	551	Администратор	XP-MSDN
Диспетчер устройств	💰 Аудит успехов	14.09.2011	11:30:04	Security	Изменение поли	612	Администратор	XP-MSDN
 Эапоминающие устройства 	🕜 Аудит успехов	14.09.2011	11:29:58	Security	Изменение поли	612	Администратор	XP-MSDN

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.

OODIT NC				
Дата:	14.09.2011	Источник:	Security	+
Время:	11:30:18	Категория:	Вход/выход	
Тип:	Аудит отк	Код (ID):	529	+
Пользов	ватель: NT A	\UTHORITY\	SYSTEM	
Компью	лер: ХР-М	ISDN		
Описани	ие:			
Отказ в пароль	входа в систе Причина: н	ему: неизвестное і	имя пользователя ил	и неверный
Пароль	входа в систи Причина: н Пользоват Домен: Тип входа Процесс в Пакет про Рабочая с	эму: неизвестное і ХР-№ 2 хода: User верки: Neg ганция: ХР-№	имя пользователя ил инистратор ISDN 32 otiate ISDN	и неверный
Штказ е пароль Данные	входа в систи Причина: н Пользовал Домен: Тип входа Процесс в Пакет про Рабочая с	ему: неизвестное і тель: Адм ХР-№ : 2 хода: User верки: Neg ганция: ХР-№	имя пользователя ил инистратор ASDN 32 otiate ASDN	и неверный

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.

обытие				
Дата: 14.09.2011	Источник:	Security		•
Время: 11:30:24	Категория:	Вход/выход 529		F
Пользователь: XP-1	код (ID): ISDN VAдмин	истратор		
Компьютер: ХР-М	ISDN	9990 BJB (BB)		3
0				
Процесс в Пакет про Рабочая с {00000000	жода: Üser верки: Negi танция: XP-N -0000-0000-00	32 otiate 4SDN K 000-00000000000	юд GUID: 00}%	
Данные: 🍥 Байты	О Слова			
				~
				Y
				-

Рисунок 5 – Запись аудита об успешном входе в операционную систему

	,	Габлица 1 – Описание типов входа в систему
Тип	Название типа	Описациа
входа	входа	Описание
		Локальный вход пользователя на
2	иптерактивный	компьютер.
3		Пользователь вошёл на данный
5	ССТВ	компьютер через сеть.
4	Пакетный	Пакетный тип входа используется
-	Пакстный	пакетными серверами.
5	Спужба	Служба запущена Service Control
5	Служоа	Manager.
7	Разблокирование	Эта рабочая станция
/	тазолокирование	разблокирована.
		Пользователь вошёл на данный
8	NetworkCleartext	компьютер через сеть. Пароль
0	NetworkClearlext	пользователя передан в
		нехэшированной форме.
		Посетитель клонировал свой
9	NewCradentials	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.

Свойства: Событие	? 🔀	Свойства: Событие	? 🔀
Событие		Событие	
Дата: 12.1222011 Источник: Security Время: 15:40:48 Категория: Вход учетной записи Тип: Аудит отк. Код (ID): 680	↑ ↓	Дата: 14.09.2011 Источник: Security Время: 11:30:24 Категория: Вход учетной записи Тип: Ачдит чсп Кол (Л): 680	↑ ↓
Пользователь: NT AUTHORITY\SYSTEM Компьютер: XP-MSDN		Пользователь: NT AUTHORITY\SYSTEM Компьютер: XP-MSDN	
Описание:		Описание:	
МІСЛОЗОГТ, АЦТНЕНТІСАТІОН, РАСКАВЕ, V1_0 Четена запись вжода Аленичетратор Исходная рабочая станция: XP-MSDN Код ошибки: 0xC000006A		MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Четена заянось входа: Администратор Исходиная рабочел станция: XPMSDN Код ошибии: 0x0	
Данные: 🖲 Байты 🔘 Слова		Данные: 💿 Байты 🔿 Слова	
			~
ОК Отмена Г	Трименить	ОК Отмена	Применить

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»).

Событие				
Дата: 15.09.2011	Источник:	Security		+
Время: 12:44:01	Категория:	Учетные за	аписи	1
Тип: Аудитусп	Код (ID):	628		
Компьютер: ХР-1	изом учадмин ИSDN	истрагор		
Компьютер. Агн	13014			
Описание:				
Исполнит Домен ис Код входа	эль: Адм толнителя: исполнителя	инистратор XP-MSI : (0x0,0x	DN 5E12B)	
Данные: 💿 Байты	О Слова			
				~

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.

войства	: Событие			?
Событие	1			
Дата: Время: Тип:	15.09.2011 12:44:21	Источник: Категория: Каз (ID):	Security Учетные записи 626	+
Пользо Компью	ватель: XP-1 тер: XP-1	КОД (ID). ISDN \Админ ISDN	истратор	
Включе	ние учетной Имя коне Конечный Код конеч Исполнит Домен ис Код входа	записи поль нюй записи: домен: XP-N ной записи: эль: Адм полнителя: исполнителя	зователя: user1 ASDN XP-MSDN\user1 инистратор XP-MSDN x (0x0,0x6E12B)	
Данные	: 💽 Байты	() Слова		~
			ОК Отмена) Применить

Рисунок 9 – Запись аудита о включении учётной записи

	а: Событие					?
Событие						
Дата: Время: Тип: Пользо Компьк	15.09.2011 12:44:21 Аудит усп ватель: ХР-М отер: ХР-М	Источник: Категория: Код (ID): SDN\Админ SDN	Security Учетны 636 истратор	е записи	Ē	↑ ↓
Добав безопа	ление члена л асностью: Имя члена: Код члена: Имя конечн Конечный д Код конечн Домен испол Код конечн	жальной гр 	уппы с в ISDN\us записи: n BUI инистрат XP-1	ключенна er1 Пол LTIN\Пол op MSDN No.cc120	й њзователи њзователи	
Данны	е: 💽 Байты	О Слова	. (540	, onor 120	,	-

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).

юйства: Событие	?
Событие	
Дата: 15.09.2011 Источник: Security Время: 13:28:09 Категория: Изменение политики Тип: Аудит усп Код (ID): 608 Пользователь: XP-MSDN\Администратор Компьютер: XP-MSDN	↑ + ₽
Присвоение прав пользователя: Право: SeBackupPrivilege Присвоеню: XP-MSDN\user Исполнитель: Пользователь: Администратор Домен: XP-MSDN Код входа: (0x0,0xAD15)	
Данные: 💿 Байты 🔿 Слова	<u>^</u>
	Прежения

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».

ойства:	Событие			?
Событие				
Дата: Время: 1 Тип: 4 Пользов- Компьют Описания	5.09.2011 3:30:23 Аудит усп атель: ХР-М ер: ХР-М	Источник: Категория: Код (ID): SDN\Админ SDN	Security Изменение политики 622 истратор	+ + B
Доступ н	безопасної Доступ уда Изменен: Удален: Пользова Домен: Код входа	сти системы лен: Seln XP-М гель: Адмі XP-М : (0x0,	идален: teractiveLogonRight ISDN/Гость инистратор ISDN 0xAD15)	
Данные	🖲 Байты	() Слова		
		(_ r	КПтмена	Примени

Рисунок 12 – Запись аудита об удалении прав у пользователя

ойства: Событи	9		?
Событие			
Дата: 15.09.2011	Источ	ник: Security	+
Время: 22:22:25	Катего	рия: Изменение политики	
Тип: Аудит усп	Код (ІС) <u>;</u> 612	+
Пользователь: ХР	MSDN A	дминистратор	Ba
Компьютер: ХР	MSDN		-3
Описание:			
Изменение полити	ки аудита	3:	^
Новая политика:			
Yonex	Отказ	Dura da una	
		Востип к объектем	
	~	Использование прав	
		Управление учетными записями	
+	-	Изменение политики	
1.5		Системные события	
1	1	Подробное слежение	×
Панные: П Байт	. 000	083	
Addition Or Or Departy		000	11/20
			2
			120
	ſ		-

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.

Событие				
Дата: Время: Тип: Пользо Компьк	15.09.2011 22:07:02 Аудит усп ватель: ХР-М отер: ХР-М	Источник: Категория: Код (ID): ISDN \Админи ISDN	Security Использование прав 577 истратор	↑ ↓ ₽
Вызов	привилегиро Сервер: S Служба: Основной I Домен: Код входа: Пользоват Домен кли Код входа Привилеги	ванной служб ;ecurity пользователь ;ель-клиент: ;ента: клиента: и:	iы: - Администратор XP-MSDN (0x0.0x521FF) Администратор XP-MSDN (0x0.0x521FF) Se5ystemtimePrivilege	
Данные	: 💽 Байты	О Слова		^ ~

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).

ойства	: Событие			?
Событие				
Дата: Время: Тип: Пользо	15.09.2011 22:16:16 Аудит усп ватель: ХР-М	Источник: Категория: Код (ID): ISDN\Админ	Security Использование прав 576 истратор	+ + 1
Описан	ие: рение специа Пользовал Домен:	льных прав д гель:	(ля нового сеанса входа:	
	Код входа: Привилеги	(0x0. ки: SeCi SeB SeR SeD	0xA69A7) hangeNotifyPrivilege ackupPrivilege estorePrivilege ebugPrivilege	
Данные	: 💿 Байты	() Слова		<u>~</u>
			IK Птмена	Применит

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

Дата:	15.09.2011	Источник:	Security	t
Время:	22:16:44	Категория:	Использование прав	1
Тип:	Аудитусп	Код (ID):	578	
Компьк Описан	вагель. АРч отер: ХР-М ие:	ISDN ALMAH	истратор	B
Опера	ция с привили Сервер об Дескрипти Код проце	егированным љекта: ор объекта: сса:	объектом: EventLog 9791536 664	^
	Основной Домен: Код входа Пользова	пользовател : гель-клиент:	 XP-MSDN\$ WORKGROUP (0x0,0x3E7) Администратор 	
	Домен кл Код входа	иента: клиента:	XP-MSDN (0x0,0xA69A7)	~
Данные	е 💿 Байты	О Слова		
				~

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.

Дата: 👖	09.2011	Источник:	Security		+
Время: 21	:36:40	Категория:	Системное о	событие	1
Тип: А <u>ч</u> Пользоват Компьюте	дитусп гель: NT / p: XP-N	Kog (ID): AUTHORITY\! ISDN	ST7 SYSTEM		Ē
Очистка и	курнала ау Основной Домен: Код входа: Пользоват Домен клі Код входа	дита пользовател тель-клиент: чента: клиента:	»: SYSTEM NT AUTI (0x0,0x3 Админи XP-MSD (0x0,0x8	t HORITY E7) stpatop N 95C)	
Данные:	🖲 Байты	О Слова			

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.

обытие				(111)
Цата: 15 Пата: 21	.09.2011	Источник:	Security	+
время:∠і Тип∵∆и	:33:37 aumuch	Категория: Код (ID):	системное сооытие 520	+
Пользоват Компьютер	ель:NT/ c:XP-M	AUTHORITYN AUTHORITYN ASDN	SYSTEM	B
Системно Код проци Имя проц WMwareS Основной Основной	е время и есса: 1 ecca: (ervice.exe пользов домен: \ код вход	зменено. 608 C:\Program File aтель: XP-M VORKGROUF a: (0x0, ент: XP-M	es\VMware\VMware Tools ISDN\$ 0.033E7) ISDN\$	
Пользова	пель-клие	JODVCDOUL		
Основной Пользова Домен кл Код входа	пель-кли пиента: \ аклиента:	VORKGROUF (0x0,	, .0x3E7)	~

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».

обытие	
Дата: 15.09.2011 Источник: Sr Время: 22:25:44 Категория: По Тип: Аудит усп Код.([D): 55 Пользователь: XP-MSDN Хаминист Компьютер: XP-MSDN	есипіту здробное отслеживан 32 гратор 🖹
Создание процесса: Код нового процесса: Имя файла образа: Notepad.exe Код создателя процесса: Пользователь: Домен: Код входа:	1868 C:\WINDOWS\system32 232 Администратор XP-MSDN (0x0.0x6C2A8)
	 A V

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

ойства: Событие			2
Дата: 15.09.2011 Время: 22:25:46 Тип: Аудит усп Пользователь: ХР-М Компьютер: ХР-М	Источник: Sec Категория: Под Код (ID): 593 ISDN \Администр. ISDN	чићу кробное отслеживан к атор	↑
Выход из процесса: Код проце Имя файл \notepad.exe Пользоват Домен: Код входа	сса: 1868 а рисунка: :ель: Админист XP-MSDN (0x0,0x6C	C:\WINDOWS\systei тратор ↓ 248)	m32
Данные: 💿 Байты	О Слова		() () () () () () () () () () () () () (
	ОК	Отмена	Примения

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».

азрешени	я Аудит	Владелец	Действун	ощие разрешения	
Для прос кнопки "И	мотра свел Ізменить".	дений об осс	бых элеме	ентах аудита выбери	ите элемент аудита и нажмите
- Элементь	наудита:				
Тип	Имя			Доступ	Унаследовано от
Отказ	user (XP-I	MSDN\user)		Полный доступ	<не унаследовано>
Yonex	Админис	тратор (ХР-М	ISDN\Aa	Смена разреш	<не унаследовано>
Добае	ить	Изменить		Удалить	
Добає Янасле добав	чить (довать от р ляя их к яв	Изменить родительско но заданным		Удалить а применимые к доч кне.	ерним объектам элементы аудита,
Добав Добав.	ить (довать от (ляя их к яв	Изменить родительско но заданныю	 го объект. и в этом о	Удалить а применимые к доч кне.	ерним объектам элементы аудита,
Добає У Насле добав.	чить) довать от р ляя их к яв	Изменить родительско но заданным		Удалить а применимые к доч кне.	юрным объектам элементы аудита,
Добағ Расле добав	ить (довать от р ляя их к яв	Изменить родительско но заданным	 го объект. и в этом о	Удалить а применимые к доч кне.	юрним объектам элементы аудита,

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.

Пата	15.09.2011	Источник	Securitu	-
Дата: 15.09.2011 Источник: 5 Время: 23:06:31 Категория: Д Тип: Аудит усп Код ([D]: 5 Пользователь: XP-MSDN \4дминис Компьютер: XP-MSDN		Источник. Категория: Kog (ID): MSDN\Админ MSDN	Зесиліу Цоступ к объектам 560 ч	
Описан Откры	иие: Сервер об Тип объек Имя объек Код дескрр Код опера Код проце Имя файл Основной Домен:	њекта: ,та: иптора: 380 ции: сса: а рисунка: пользователі	Security File C:\Teкcтовый документ.txt (0.957523) 1260 C:\WINDOWS\explorer.exe s: Администратор XP-MSDN	
Данны	е: 🛞 Байты	Слова		< >

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

войства: Событи	19	?
Событие		
Дата: 15.09.201 Время: 23:06:31 Тип: Аудит усп Пользователь: XF Компьютер: XF	I Источник: Security Категория: Доступ к объектам Код (ID): 560 ⁹ -MSDN \Администратор ⁹ -MSDN	+ + =
Описание: Пользов Домен н Код вход Доступ	затель клиент: лиента: a клиента: READ_CONTROL WRITE_DAC ReadAttributes	<u>*</u>
Привиле Счетчик	егии ограниченного SID: 0	~
Данные: 💿 Байт	ъ 🔘 Слова	
		~
	ОК Отмена	Примени

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).

15.09.2011 23:14:27 Аудит отк ватель: ХР-1 итер: ХР-1	Источник: Категория: Код (ID): ISDN\user ISDN	Security Доступ к объектам 560	 ↑ ↓ □
Пользова Доменкл Код входа Доступ	гель-клиент: иента: клиента: DELI REA Read	ETE D_CONTROL JAttributes	~
Привилегі Счетчик о	ии - раниченного	SID: 0	~
: 💽 Байты	О Слова		
			< 3
	15.09.2011 23.14:27 Аудит отк ватель: ХР-№ ие: Пользоват Лользоват Лользоват Лользоват Доступ Привилеги Счетчик ог	15.09.2011 Источник: 23:14:27 Категория: Аудит отк Код (ID): ватель: XP-MSDN vuser лер: XP-MSDN ие: Пользователь-клиента: Домен клиента: Домен клиента: Домен клиента: Доступ DELL Код входа клиента: Доступ DELL Счетчик ограниченного	15.09.2011 Источник: Security 23.14:27 Категория: Доступ к объектам Аудит отк Код (ID): 560 ватель: XP-MSDN изег лер: XP-MSDN ие: Пользователь-клиент: Домен клиента: Домен клиента: Домен клиента: Домен клиента: Доступ DELETE READ_CONTROL ReadAttributes Привилегии Счетчик ограниченного SID: 0

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.

сооршие					
Дата: 15	.09.2011	Источник:	Security	+	
Время: 23	:14:35	Категория:	Доступ к объект	лам	
Тип: Ау	дит отк	Код (ID):	560		-
Пользоват	ель: ХР-М	ISDN/user		Ē₽.	
Компьюте	p: XP-M	ISDN			
Описание:					
	Домен: Код входа: Пользоват Домен кли Код входа Доступ Привилеги Счетчик ог	ель-клиент: іента: клиента: WRI и - раниченного	XP-MSDN (0x0,0xEC68 user XP-MSDN (0x0,0xEC68 TE_DAC SID: 0	D)	
Данные:	🖲 Байты	О Слова			
				2	5
					<u> </u>

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

Элемент аудита для doPDF v7	? 🛛
Объект	
Имя: Администратор (XP-MSDN	Идминист Изменить
Доступ:	успех Отказ
Печать Управление принтерами Управление документами Чтение разрешений Смена разрешений Смена владельца	
	Очистить все
	ОК Отмена

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.

Дата:	16.12.2011	Источник:	Security	+
Время:	9:47:17	Категория:	Доступ к объектам	
Тип:	Аудит усп	Код (ID):	560	•
Пользов	затель: ХР-М	ИSDN\Админ	ифгратор	6
Компью	тер: ХР-М	ISDN		
Описани	4e:			
Открып	ие объекта:			~
	Сервер об	ъекта:	Spooler	
	Имя объек	ita: Ktar	doPDE v7	
	Код дескр	иптора: 3778	080	
	Код опера	ции: сол:	{-,-} 1229	
	Имя файл	сса. а рисунка:	C:\WINDOWS\system32	
\spoolsv	/.exe			
ļ	Основнои	пользовател	E: XP-MSDN\$	~
Данные	🔅 💿 Байты	О Слова		
				2

Рисунок 27 – Запись аудита об использовании принтера

Пата: 1	£ 09 2011	Истонник	Security	
дага. г Впема: Г	0.03.2011	Категория:	Постип к объектам	ा
Тип: А	Ачдит чсп	Kog (ID):	560	+
Пользов	атель: ХР-М	ISDN\Админ	истратор	80
Компьют	ep: XP-M	ISDN	-	
Описани				
Открыти	le объекта:			
	Сервер об	ъекта:	Spooler	
	Имя объек	.та: <та:	Document Текстовый документ -	
Блокнот	Koalaeoro	umona: 2779	1022	
	Код опера	ции:	{-,-}	
	Код проце Има файл	сса: сса:	1392 C:\WINDOWS\sustem32	
\spoolsv.	exe	a priograna.	0. 111110 0 11 0 Injetomoz	
Данные:	🛞 Байты	ОСлова		
	C. D. G. H.D.	0 01000		- 11

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.

Тарамет	р локальной безопасности
đ	Управление аудитом и журналом безопасности
ХР-МSI Админ	DN Vuser истраторы
Добави	ить пользователя или группу) Удалить

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».

Јощие Фильтр					
Типы событий Уведомления Предупрежден Ошибки	ия	✓ Аудит уст ✓ Аудит отк	1ехов .азов		
Источник события:	Security	1			~
Категория:	Вход/выход			~	
Код события:					
Пользователь:	Пользователь: user				
Компьютер:					
С: первого	~	16.09.2011	v	0:10:53	÷
До: последнего	~	16.09.2011	~	0:10:53	*
		E	восста	новить умол'	чания

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.

Уведомления Предупрежден Ошибки	✓ Аудит успехов ия ✓ Аудит отказов	
Источник события:	Security	~
Категория:	(Bce)	~
Код события:		
Пользователь:		
Компьютер:		
Описание:	Текстовый документ	
Направление поис	ka	
О Вверх 💿 Вн	из Найти	далее

Рисунок 32 – Настройка поиска записей журнала безопасности

Общие	Фильтр				
Вывод	имое имя:	Безопасность			
Имя ж	урнала:	C:\WINDOWS\System32\config\SecEvent.Evt			
Размер:		64,0 КБ (65 536 байт)			
Создан	-с	25 августа 2008 г. 21:17:25			
Измен	ен:	16 сентября 2011 г. 1:00:29			
Откры	T:	16 сентября 2011 г. 1:00:29			
Pass	іер журнал	1a			
Mar	симальнь	ий размер журнала: 64 📚 КБ			
Πo,	достижени	и максимального размера журнала:			
0	Затирать с	тарые события по необходимости			
0	Затирать с	обытия старее 🛛 🍵 дней			
0	Не затират очистка ж	гь события урнала вручную) Восстановить умолчания			
Πορ	цключение	по медленной линии Очистить журнал			

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).

Свойства	: Аудит: немедленное отключение систе 😰 🔯
Парамет	р локальной безопасности
Ð	Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности
⊙ E	Зключить
00	тключить
	Изменение этого параметра может повлиять на совместимость с клиентами, службами и приложениями. Дополнительные сведения см. в <u>Ачдит: немедленное</u> отключение системы, если невозможно внести в журнал записи об ачдите безопасности. (Q823659)
	ОК Отмена Применить

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.

2 1985-2001	Professional	
Корторация Майкроссфт		Microso
Журнал безопасно разрешен только а	сти данной системы переполнен. Вход і администраторам.	зсистему
Пользователь: а	дминистратор	

Рисунок 35 – Окно входа в систему при переполнении журнала безопасности

консоль Дей	сооытии іствие Вид Справ	жа				
🗢 🔿 🔁		2				
<u>同</u> Просмотр со	бытий (локальных)	Безопасность	8 событий			
Приложение		Тип	Дата	Время	Источник	Катег
ру Сезолами на Систен	Открыть файл жур Сохранить файл жур Создать вид журна Стереть все событи Вид Переименовать Обновить Экспортировать спи Свойства Справка	нала рнала как ла ня на нок	16.09.2011 16.09.2011 16.09.2011 16.09.2011 16.09.2011 16.09.2011 16.09.2011 16.09.2011	1:48:37 1:48:36 1:47:51 1:47:36 1:46:57 1:46:47 1:46:47 1:46:47	Security Security Security Security Security Security Security Security	Испол Подре Подре Подре Подре Испол Испол Систе

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 Проанализируйте вариантом. журнал безопасности согласно распределению вариантов и определите виновных. Параметры аудита, использовавшиеся при фиксации событий, перечислены в табл. 2. параметр Также включен «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.

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	
Гоннолий	финансовый менеджер,	
т еннадии	пользователь	
Deaurri	оператор пульта	
Басилии	видеонаблюдения, пользователь	
	технический консультант,	
Администратор	администратор системы	
Валерий	директор, оператор архива	
Людмила	бухгалтер, пользователь	
Татьяна	секретарь, пользователь	
A 1977 19	помощник технического	
Артур	консультанта, пользователь	
A	администратор безопасности,	
Анатолии	администратор системы	
	руководитель отдела разработки,	
давідов	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 странном компьютера: «Компьютер 0 поведении отобразив самопроизвольно заблокировался, 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 «С:\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

использует Директор встроенные организации средства резервирования для файла «База данных заказов.doc», архив которого он сохраняет в папку «С:\APXИB\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 Администратору безопасности было поручено директором файл. 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 текуших 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.

🚡 Консоль1 - [Корень консоли	\Шаблоны безопасности\С:\	WINDOWS\security\templates\setup securit
°∰ Консоль Действие Вид Изб ← → 🗈 📧 🗔 🚱	іранное Окно Справка	
Корень консоли Анализ и настройка безопасности Шаблоны безопасности G C:\WINDOWS\security\temp: G C:\WINDOWS\security\temp: G G compatws G G compatws G G hisecdc G G hisecws G G securedc G G securedc G G securess G G secures G G secures	Имя Политики учетных записей Покальные политики В Хурнал событий Сируппы с ограниченным дос Системные службы Феестр Файловая система	Описание Политики паролей и блокировки учетных записей Политики аудита, прав пользователей и парам Журнал событий Группы с ограниченным доступом Параметры системной службы Параметры безопасности реестра Параметры безопасности файлов

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).

🚡 Консоль1 - [Корень консоли\Шабл	оны безопасности\C:\WINDOWS\security\te	emplates\setup secu
📸 Консоль Действие Вид Избранное	Окно Справка	
⇔ → 🗈 📧 🗙 🗗 🔂 😫		
Корень консоли	Политика 🛆	Параметр компьютера
 В Шаблоны безопасности В Сумтирои/Steering with themplates 	щомакс. срок деиствия пароля Мин. длина пароля	42 днеи 6 символов
Criwindoworksecurity (templates	воправля пароля в пароля в пароля пароля пароль должен отвечать требованиям слож	0 дней Отключен
	Пребовать неповторяемости паролей Каранить пароли всех пользователей в домен	0 хранимых паролей Отключен
🗄 📑 setup security 🖻 🖼 Политики учетных записей		
 Политика паролей Политика блокировки х 		
 Политика Kerberos Вогальные политика 		
⊕ локальные политики ⊕ Журнал событий		
⊕ ⊡ Реестр ⊕ ⊡ Файловая система		
Рисунок 2 – Изменение пара	аметра в разделе «Политики учёт	ных записей»

🔓 Консоль1 - [Корень консоли\Шаблоны бе	зопасности\C:\WINDOWS\security\template	s\setup security\Локальн
🚡 Консоль Действие Вид Избранное Окно	Справка	
← → 🖻 📧 🗙 🖀 🖶 😫		
🔁 Корень консоли	Политика 🔺	Параметр компьютера
🗄 🙀 Анализ и настройка безопасности	🔀 Изменение параметров среды оборудования	Администраторы
🖃 🗊 Шаблоны безопасности	изменение системного времени	Администраторы, Опытные поль
C:\WINDOWS\security\templates	📖 Локальный вход в систему	Администраторы,Операторы ар
± G compatws	🔀 Настройка квот памяти для процесса	Администраторы,LOCAL SERVIC
	👪 Обход перекрестной проверки	Администраторы,Операторы ар
H a rootses	🐯 Овладение файлами или иными объектами	Администраторы
E Securedo	🐯 Олицетворение клиента после проверки под	СЛУЖБА, Администраторы
	👪 Отказ в доступе к компьютеру из сети	XP-MSDN\Гость
- a setup security	🐯 Отказ во входе в качестве пакетного задания	
🗄 🛃 Политики учетных записей	🐯 Отказать во входе в качестве службы	
🖃 🛃 Локальные политики	👪 Отклонить локальный вход	XP-MSDN\Гость
🕢 🛃 Политика аудита	🕮 Отладка программ	Администраторы
😥 🛃 Назначение прав пользователя	🕮 Принудительное удаленное завершение	Администраторы
🗄 🚮 Параметры безопасности	👸 Профилирование загруженности системы	Администраторы
🕀 🛃 Журнал событий	🕮 Профилирование одного процесса	Администраторы, Опытные поль
Пруппы с ограниченным доступом	🕮 Работа в режиме операционной системы	
Е Системные службы	👪 Разрешать вход в систему через службу тер	Администраторы,Пользователи
⊡ Пеестр	Разрешение доверия к учетным записям при	
± Файловая система	🐯 Синхронизация данных службы каталогов	
	🔀 Создание глобальных объектов	ИНТЕРАКТИВНЫЕ, СЛУЖБА, Адми
	👪 Создание журналов безопасности	LOCAL SERVICE, NETWORK SERVICE
	😅 Создание маркерного объекта	
	🐯 Создание постоянных объектов совместного	
	👪 Создание страничного файла	Администраторы
	🕮 Увеличение приоритета диспетчирования	Администраторы
	Управление аудитом и журналом безопасности	Пользователи. Администраторы

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).

📸 Консоль1 - [Корень консоли\Шаблоны бе	зопасности\C:\WINDOWS\security\templates\setup security\Ж	урнал [
📸 Консоль Действие Вид Избранное Окно	Справка	
← → 🗈 📧 🗙 🖀 🗟 😫		
Kopethe Konkoonu Image: A particular intervention of the second concern Image: A particular interventinter Image: A partenventinter<	Политика А Запретить доступ локальной группы гостей к журналу безопасности запретить доступ локальной группы гостей к журналу приложений запретить доступ локальной группы гостей к курналу приложений Максимальный размер журнала приложений Максимальный размер журнала приложений Сохранение событий в журнале безопасности Сохранение событий в журнале приложений Сохранение событий в журнале приложений Сохранение событий в журнале приложений Сохранение событий в курнале приложений Сохранение событий в системном журнале в Сохранение событий в системном журнале	Параметр к Отключен Включен Включен 512 КБ 512 КБ 512 КБ 7 дней По дням 7 дней По дням 7 дней По дням
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).

📸 Консоль1 - [Корень консоли\Шаблоны б	Свойства: Администраторы	
 Консоль Действие Вид Избранное Окно Консоль Действие Вид Избранное Окно Корень консоли Корень консоли Алилиз и настройка безо С://WINDOWS/security Балось Балось Совремя Балось Совремя Балили и настройка безо С://WINDOWS/security Балось Совремя Балось Совремя Балось Совремя Балось Совремя <l< td=""><td>Настройка списков членства для (group) Члены этой группы: ХР-MSDN\user Добавить. Удалить Эта группа является членом в: (Группы, которым принадлежит эта группа, не должны изменяться> Добавить. Удалить</td><td></td></l<>	Настройка списков членства для (group) Члены этой группы: ХР-MSDN\user Добавить. Удалить Эта группа является членом в: (Группы, которым принадлежит эта группа, не должны изменяться> Добавить. Удалить	
 	ОК Отмена Примен	нть

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.



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).

🖀 Консоль1 - [Корень кон	соли\Шаблоны бе	Свойства: machine\software
Konconb (Kope His Kohn Konconb Действие Вид Anarus и настройка безо Manus и настройка безо Gonachoctru Gonachoctru	VISipanhoe Okho VISipanhoe Okho S Vina ofsekta / machine(software)	Свойства: machine\software ? Параметр шаблона политики безопасности
ен страна собы: ен страна собы: ен страна сограна ен страна системные сл ен страна системные сл ен страна системные си	machine\software\ machine\software\ machine\software\ machine\software\ machine\software\ machine\software\	ОК Отмена Применить

Рисунок 7 - Изменение параметра в разделе «Реестр»

зопасность		
руппы или пользователи:		
🕵 SYSTEM		
🚮 Администраторы (XP-MS	DN\Aдминистраторы)	
🕵 Опытные пользователи	(XP-MSDN\Опытные польз	ова.
🕵 Пользователи (XP-MSDN	√Пользователи)	
🕵 СОЗДАТЕЛЬ-ВЛАДЕЛЕ	Ц	
	Побавить Члал	UT b
азрешения для Опытные	Добавить Удал	ить
азрешения для Опытные ользователи	Добавить Удал Разрешить Запрет	ить ить
азрешения для Опытные ользователи Полный доступ	Добавить Удали Разрешить Запрет	ить ить
азрешения для Опытные ользователи Полный доступ Чтение	Добавить Удалл Разрешить Запрет	ить
'азрешения для Опытные ользователи Полный доступ Чтение Особые разрешения	Добавить Удал Разрешить Запрет У П	ить

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»

	lsystem32\so	ol.exe ? 🖹
Безопасность		
Группы или пользователи:		
🕵 SYSTEM		
🔢 Администраторы (XP-MSDN	VAдминистрато	ры)
Bce		
🕵 Пользователи (XP-MSDN\П	ользователи)	
Ì	Добавить	Удалить
Processies and Pro-	Baseaurum	2
газрешения для все	газрешить	запретить
- ·		
Полный доступ		
Полный доступ Изменение Итонию и рыто смонию		
Полный доступ Изменение Чтение и выполнение Список содержимого варки		
Полный доступ Изменение Чтение и выполнение Список содержимого папки Чтение		
Полный доступ Изменение Чтение и выполнение Список содержимого папки Чтение Запись		
Полный доступ Изменение Чтение и выполнение Список содержимого папки Чтение Запись Чтобы задать особые разрешени параметры, нажмите эту кнопку	ия или До	

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».

🚡 Консоль1 - [Ко	рень консоли\	Шабло	ны бе	зопасности\C:\W
🛅 Консоль Дейст	вие Вид Избр	анное	Окно	Справка
🗢 🔿 🗈 💽 🕻	X 🖳 😫			
Корень консоли Ф. В Анализ и настр Ф. В Анализ и настр Ф. В Анализ и настр Ф. В С:\WINDO Ф. В C:\WINDO Ф. В C:\WINDO Ф. В C:\WINDO Ф. В Comp	оойка безопаснос пасности WS\security\templa Открыть	Имя Пол Лок Зм	итики у альные онал соб ппы с ог	четных записей политики Бытий граниченным дос
	Создать шаолон Обновить Задать описание	н Э	темные :тр ловая с	службы истема
	Новое окно отск Удалить	ода		
ш	Справка			

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

Импорт шаблона	? 🛛
Папка: 🔁 templates 💽 🔶 🖿	-11 *
compatives insected insecute	
Имя файла: test	Открыты
Тип файлов: Шаблон безопасности (.inf)	Отмена
Г Очистить эту базу данных перед импортом	1

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).

🚡 Консоль1 -	[Корень консоли\Анализ и н
🚡 Консоль 🛛 Д	цействие Вид Избранное Окн
← → 🗈 [☑ 😫
📄 Корень консс	оли
— Фнализ и	Открыть базуданных н Открыть базу данных н Анализ компьютера Настроить компьютер н Сохранить з Импорт шаблона Экспорт шаблона п Показать файл журнала
	Вид ▶ 4 Новое окно отсюда ВЕ
	Новый вид панели задач
	Справка
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).

Анализ безопасности системы	
Анализируются:	
 Назначение прав пользователя 	Системные службы
 Группы с ограниченным доступом 	Политика безопасности
➡ Реестр	
Файловая система	
11111	

Рисунок 16 - Анализ настроек безопасности операционной системы

🗃 Консоль1 - [Корень консоли Мнализ и настройка безопасности Политики учетных записей Полит				
🚡 Консоль Действие Вид Избр	анное Окно Справка			
← → 🖻 🖬 😼 😫				
📄 Корень консоли	Политика 🛆	Параметр базы да	Параметр компью	
🖻 🧊 Анализ и настройка безопаснос	😰 Макс. срок действия пароля	42 дней	42 дней	
🖃 🤯 Политики учетных записей	🐯 Мин. длина пароля	6 символов	0 символов	
Политика паролей	🐯 Мин. срок действия пароля	0 дней	0 дней	
Нолитика блокировки уч	😰 Пароль должен отвечать требо	Отключен	Отключен	
н страници собласти на странити н Странити на странити на стр	😰 Требовать неповторяемости па	0 хранимых паролей	0 хранимых паролей	
но совтии	🐯 Хранить пароли всех пользоват	Отключен	Отключен	
на системные службы				
Файловая система				
🗄 📴 Шаблоны безопасности				

Рисунок 17 – Результат анализа безопасности операционной системы

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

Таблица 1 – Описание пиктограмм результатов анализа

1 1 1	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).

🎦 Консоль1 - [Корень консолиМнализ и настройка безопасностиПолитики учетных записейПолит				
🚡 Консоль Действие Вид Избранное Окно Справка				
🧰 Корень консоли	Политика 🔺	Параметр базы да	Параметр компью	
 Анализ и настройка безопаснос Оплитики учетных записей 	Макс. срок действия пароля Мин. длина пароля	42 дней 6 символов	42 дней 6 символов	
 Политика паролей Политика блокировки уч 	 Мин. срок действия пароля Пароль должен отвечать требо 	0 дней Отключен	0 дней Отключен	
 Запальные политики Запальные политики Запальные событий Покальные событий Покальные событий 	 Требовать неповторяемости па Хранить пароли всех пользоват 	0 хранимых паролей Отключен	0 хранимых паролей Отключен	
 Системные службы Реестр 				
⊕ ⊡ Файловая система ⊕ ⊕ Шаблоны безопасности				

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

Вариант 2

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

Вариант 3

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

Вариант 4

1		
Локальные политики	Локальные политики	Системные службы
Запретите отображение	Включите	Автозапуск службы
имени последнего	обязательное нажатие	«Центр обеспечения
пользователя при	Ctrl-Alt-Del при	безопасности»
входе в систему	входе в систему	

Вариант 5

1		
Локальные	Журнал событий	Группы с ограниченным
политики		доступом
Разрешите	Максимальный	Включите учётную запись
учётной записи	размер журнала	«user» в группу «Опытные
«user» работу с	безопасности – 2 МБ	пользователи»
журналом аудита		

Вариант 6

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

Вариант 7

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

Вариант 8

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

Вариант 9

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

Вариант 10

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