

Обеспечение безопасности ПОЧТОВЫХ КЛИЕНТОВ

Защита клиентов электронной почты

Операционные системы клиентских компьютеров должны быть:

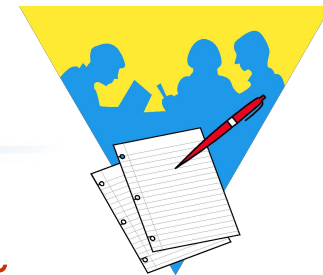
- ❑ Обновлены до наиболее безопасного уровня;
- ❑ Сконфигурированы так, чтобы доступ к локально хранимым сообщениям и конфигурационным файлам почтового клиента имели только соответствующие пользователи (обычно владельцы);
- ❑ На компьютерах под управлением Windows необходимо безопасно сконфигурировать Windows Scripting Host (WSH):
 - Удалить WSH или разрешить доступ только администратору
 - Сменить установки по умолчанию для автоматического запуска приложений обработки в зависимости от типов (расширений имен) файлов
- ❑ На компьютерах под управлением Windows обеспечить такое конфигурирование ОС, чтобы отображались полные имена файлов со всеми расширениями

Защита клиентов электронной почты

Безопасность операционных систем клиентских компьютеров:

- ❑ Установите антивирусные программы и настройте их на автоматическое сканирование всех входящих сообщений и любых вложений при их открытии;
- ❑ Обеспечьте, чтобы ОС принуждала к присвоению минимальных привилегий пользователям и службам (демонам), потому что вредоносный код исполняется в контексте безопасности пользователя, от имени которого запущено приложение или служба (то есть с правами доступа для данного пользователя);
- ❑ Обеспечьте защиту критичных компонент ОС от проникновения воздействия вредоносного кода;
- ❑ Используйте программы шифрования файлов для защиты локальной почты на жестком диске компьютера пользователя (это особенно важно для ноутбуков, которые легче украсть);
- ❑ Настройте ОС на автоматическую блокировку компьютера по истечении установленного времени неактивности пользователя

Настройка безопасности ОС почтового клиента



Практическая работа:

Проверка правильного отображения типов файлов

По умолчанию Windows не показывает расширения файлов известных типов. Поскольку .VBS является известным типом файлов, вирус

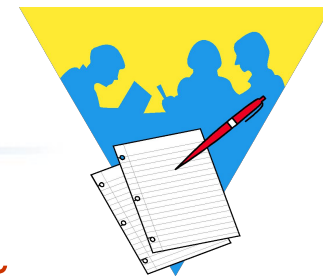
ANNAKOURNIKOVA.JPEG.VBS

отображается как

ANNAKOURNIKOVA.JPEG

1. Пользуясь утилитой TELNET, установить соединение с сервером IMAP.
2. Выбрать START / SETTINGS / FOLDER OPTIONS (Пуск / Настройки / Свойства папки)
3. Нажать VIEW (Вид)
4. В подкаталоге FILES AND FOLDERS (Файлы и папки) найти HIDE FILE EXTENSIONS FOR KNOWN FILE TYPES (Не показывать расширения для зарегистрированных типов файлов).

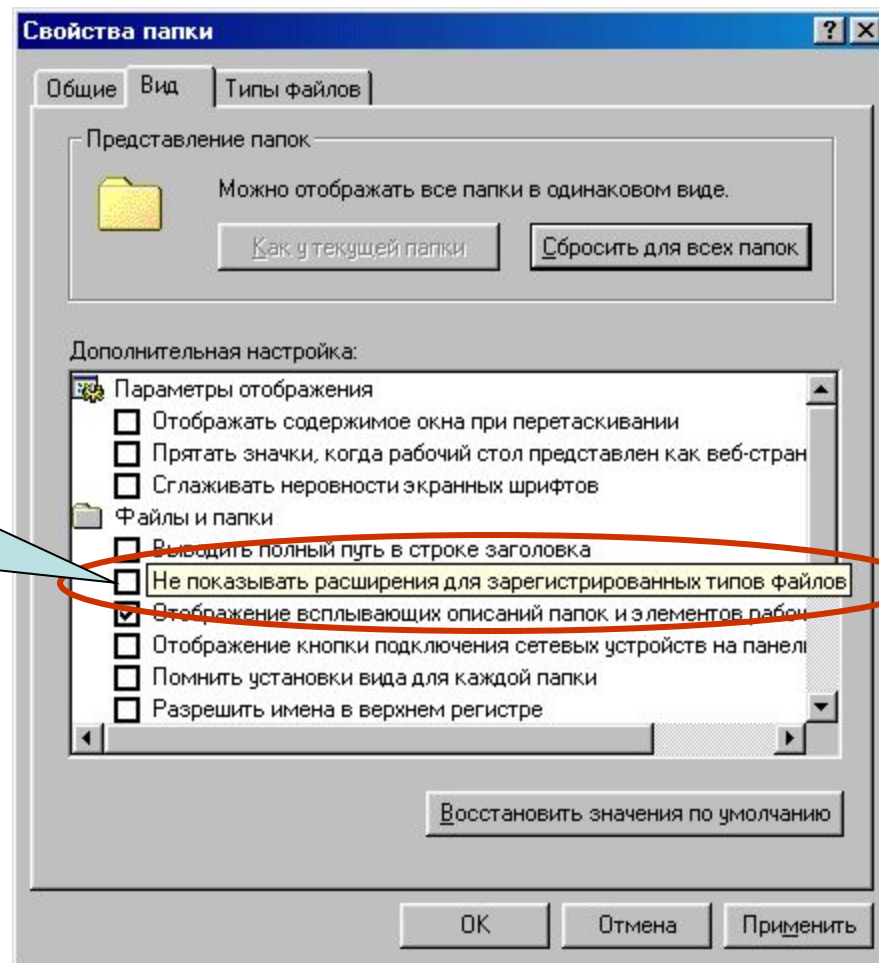
Настройка безопасности ОС почтового клиента



Практическая работа:

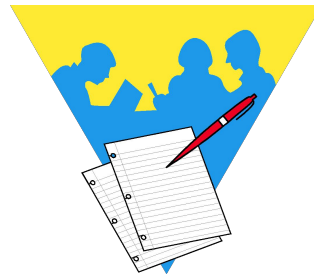
Проверка правильного отображения типов файлов

Если в
прямоугольнике
стоит отметка,
удалить ее
и нажать ОК

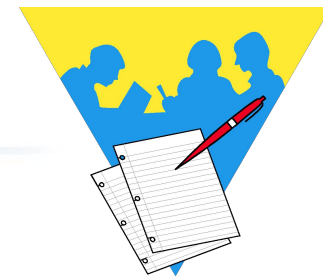


Практическая работа № 13

Настройка безопасности ОС ПОЧТОВОГО



Настройка безопасности ОС почтового клиента

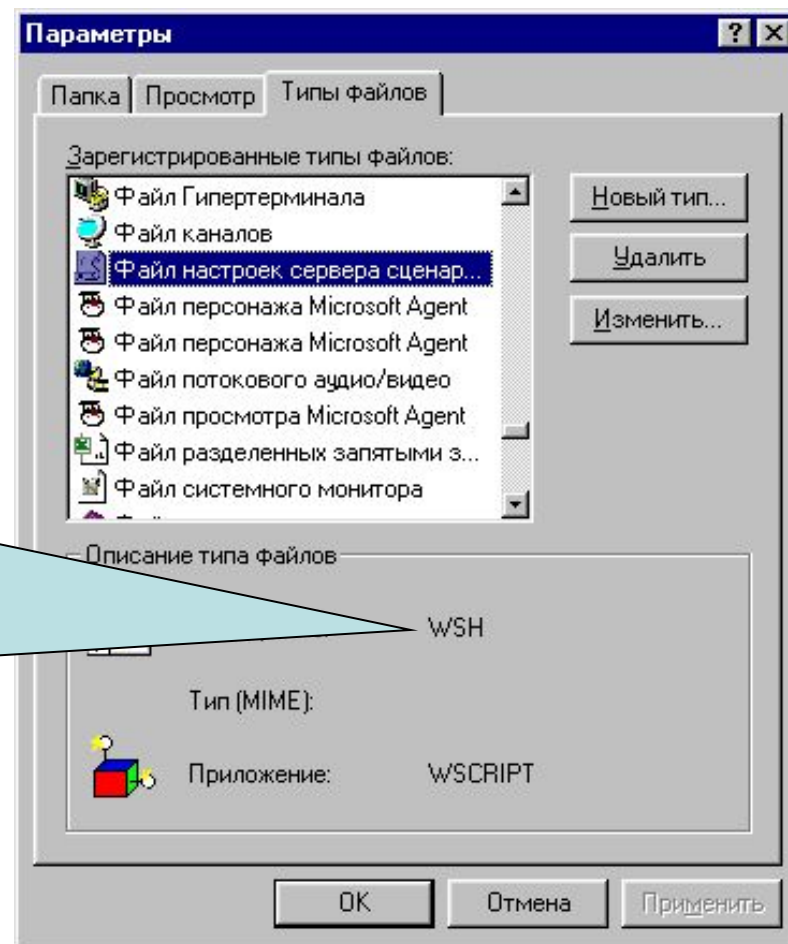


Практическая работа:

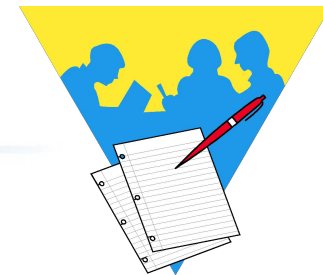
Замена установок по умолчанию для
автоматического запуска приложений

Сменить установки
по умолчанию для
расширений:

- WSC
- WSH
- WS
- WSF
- VBS
- VBE
- JS
- JSE



Настройка безопасности почтового клиента



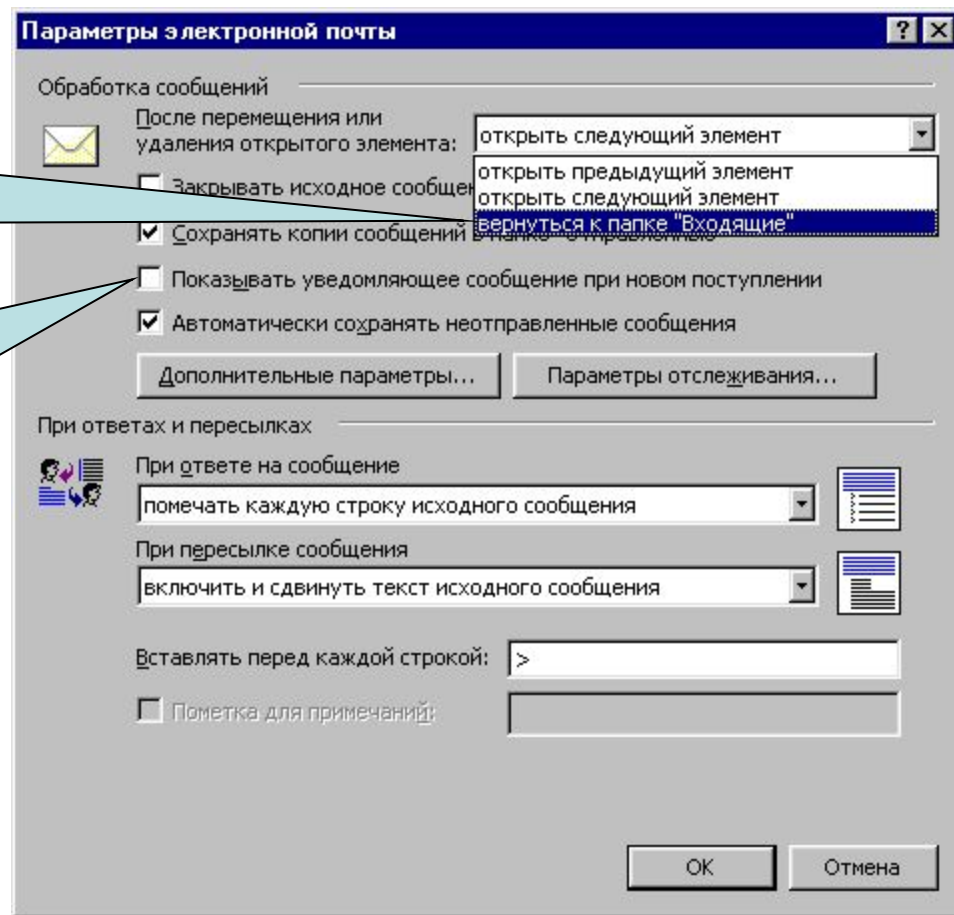
Практическая работа:

Изменение настроек, предусматривающих автоматическое открытие следующего/предыдущего или нового письма

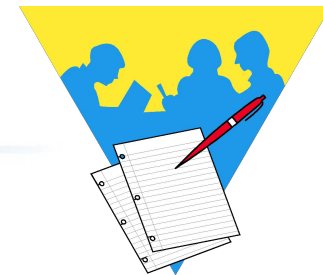
Щелкнуть по стрелке вниз и выбрать RETURN TO THE INBOX (Вернуться к папке «Входящие»)

Убрать «галочку» в строке DISPLAY A NOTIFICATION MESSAGE WHEN NEW MAIL ARRIVES (показывать уведомляющее сообщение при новом поступлении)

Нажать ОК дважды для возврата в Outlook.



Настройка безопасности почтового клиента

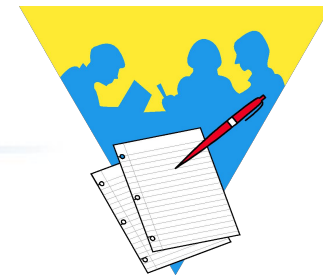


Практическая работа:

Изменение настроек, предусматривающих
автоматическое открытие следующего/предыдущего
или нового письма

1. Открыть Outlook
2. В строке инструментов найти и выбрать TOOLS (Сервис).
3. В выпадающем меню найти и выбрать OPTIONS (Параметры). В диалоге OPTIONS выбрать PREFERENCES (Настройки).
4. Нажать кнопку E-MAIL OPTIONS (Параметры почты)
5. В MESSAGE HANDLING (Обработка сообщений) ниже строки After moving ... (После перемещения ...) необходимо внести изменения.

Настройка безопасности почтового клиента



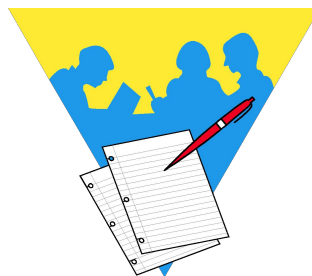
Практическая работа:

Отключение области предварительного просмотра письма

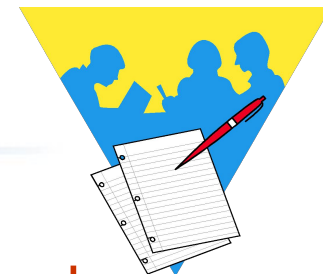
1. Открыть Outlook
2. Найти VIEW (Вид) на панели инструментов
3. В выпадающем меню выбрать
PREVIEW PANE (Область просмотра) и
AUTO PREVIEW (Автопросмотр)
4. Отключить обе возможности.
(Если какая-либо одна или сразу обе возможности включены,
соответствующие иконки будут «утоплены»)

Практическая работа № 14

Защита от VBS Email Worms



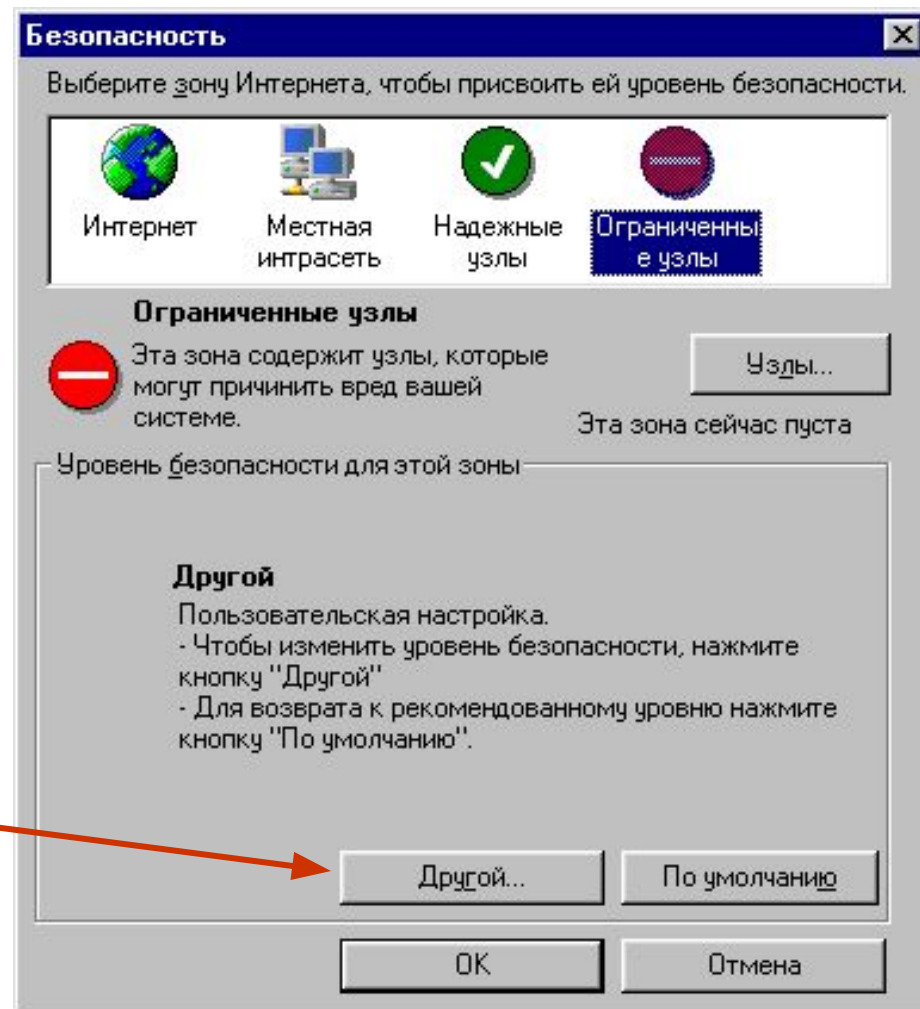
Настройка безопасности почтового клиента



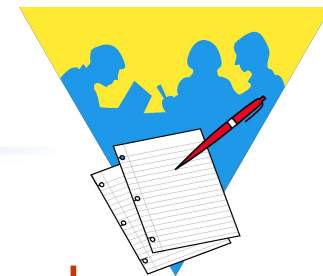
Практическая работа:

Конфигурирование зон безопасности для Outlook

1. Запустить Outlook
2. В строке инструментов найти и выбрать TOOLS (Сервис)
3. В выпадающем меню найти и выбрать OPTIONS (Параметры)
4. В диалоге OPTIONS выбрать SECURITY (Безопасность)
5. Нажать кнопку Настройки зоны
6. Для зоны Restricted Zone (Ограниченные узлы) выбрать «Custom Level» (Другой)

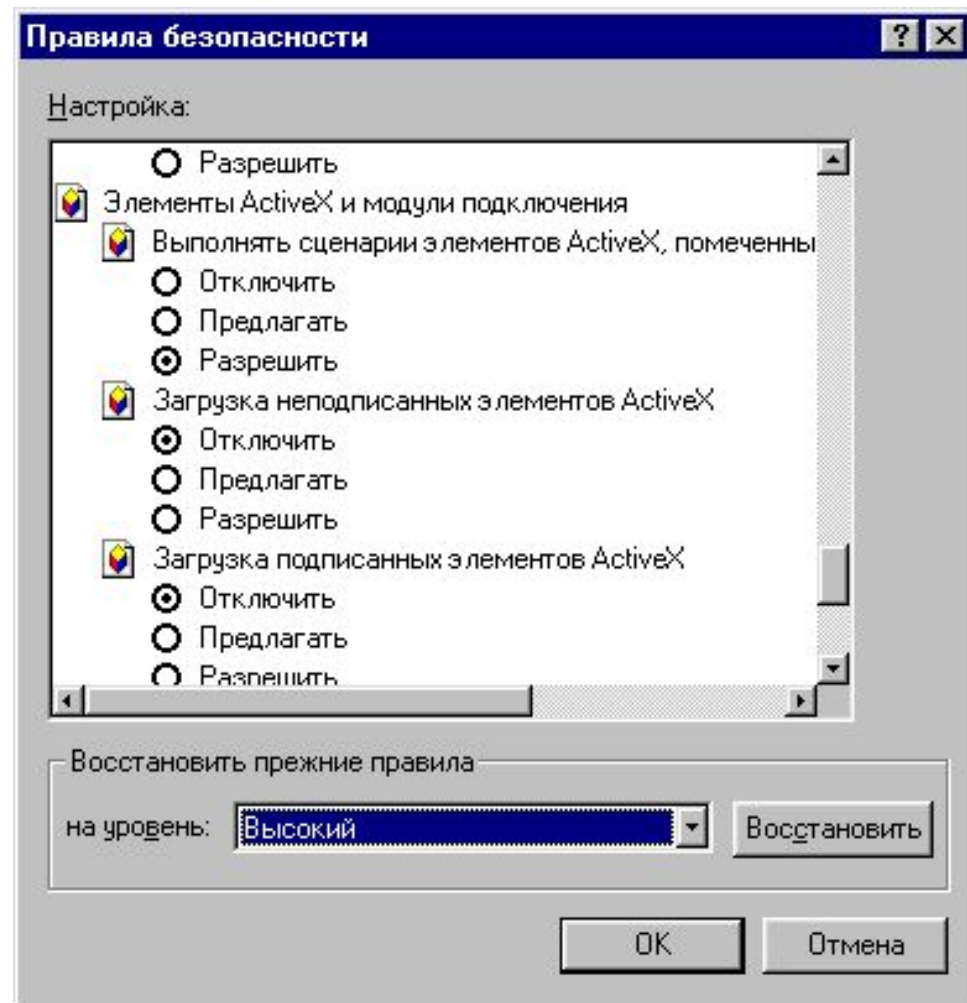


Настройка безопасности почтового клиента

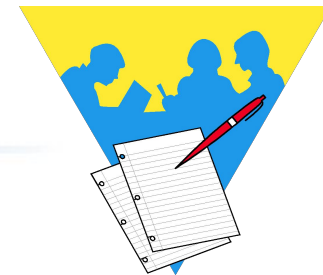


Практическая работа: Конфигурирование зон безопасности для Outlook

7. Установить следующие значения:
 - Запрет обработки загруженных подписанных ЭЦП ActiveX компонент
 - Запрет обработки загруженных не подписанных ЭЦП ActiveX компонент
 - Запрет выполнения Java компонент
 - Запрет запуска программ с IFRAME
 - Запрет выполнения активных скриптов
 - Запрет исполнения Java апплетов



Настройка безопасности почтового клиента



Практическая работа: Настройка чтения HTML сообщения в виде текста

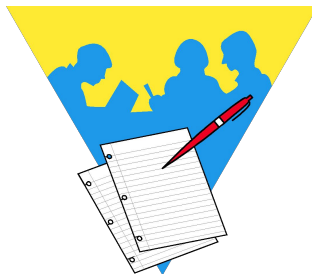
Для исключения угроз, связанных с представлением сообщений в виде HTML необходимо задать следующий ключ реестра

Key:
[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail]
Value Name: ReadAsPlain
Data Type: REG_DWORD
Value Data: 1

Проверить правильность работы установленного параметра

Практическая работа № 15

Конфигурирование зон безопасности для Outlook

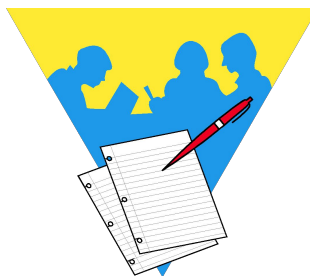


Разграничение прав доступа к общим папкам

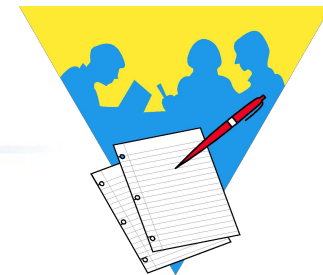
-
- Свойства папки "CERT"**
- Общие Web-страница Управление **Формы** Разрешения
- Имя: Роль:
- | | |
|---------------------|-------------|
| По умолчанию | Автор |
| NT User:S-1-5-21... | Владелец |
| Admin (Charlie R... | Владелец |
| Dmitry V. Ershov | Владелец |
| Анонимные | Нет доступа |
- Добавить...
Удалить
Свойства...
- Разрешения**
- Роли: Автор
- ☒ Соз Ответственный редактор
 - ☒ Изм Редактор
 - ☐ Соз Ответственный автор
 - ☐ Автор
 - ☐ Автор без прав редактора
 - ☐ Читатель
- Права:
- | | |
|---|---|
| ☐ не разрешена | ☐ не разрешено |
| ☒ только своих | ☒ только своих |
| ☐ всех | ☐ всех |
- ОК Отмена Применить Справка

Практическая работа № 16

Разграничение прав доступа к общим папкам



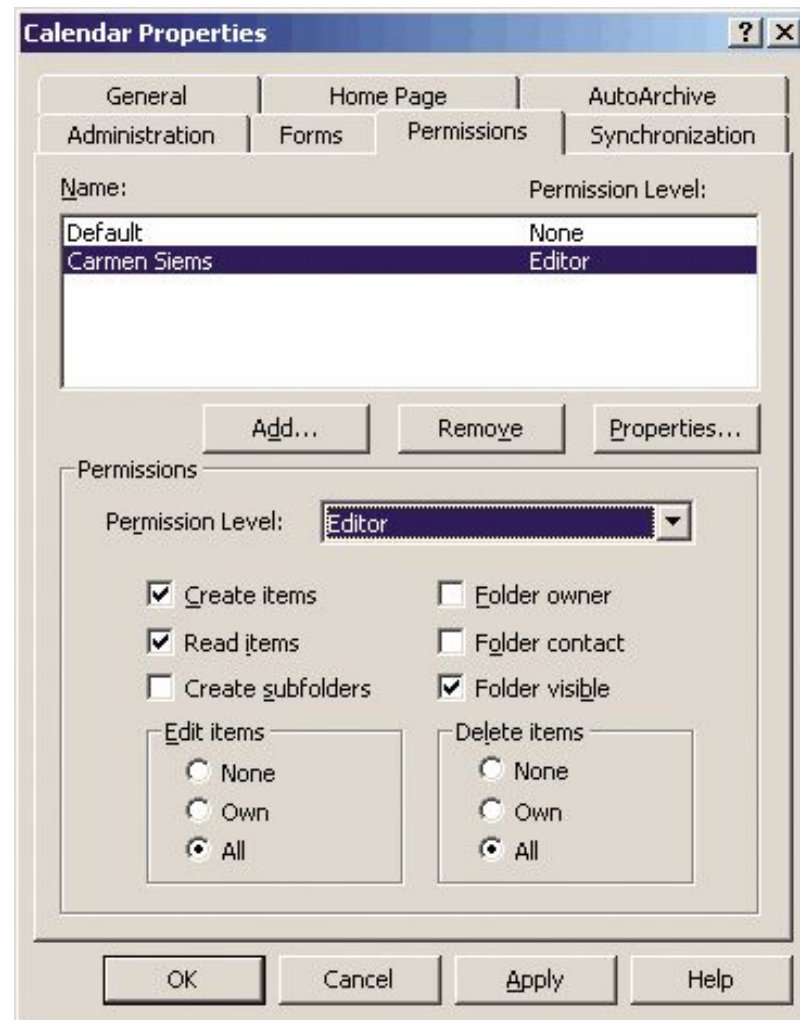
Настройка безопасности почтового клиента



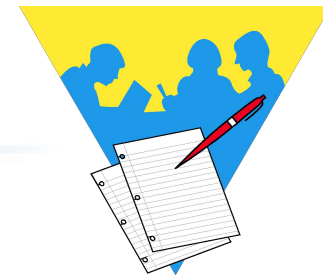
Практическая работа: Разграничение доступа к почтовому ящику

1. Запустить Outlook
2. Щёлкнуть правой кнопкой мыши на папке Inbox в своём почтовом ящике, выбрать пункт свойств Properties
3. В раскрывшемся окне перейти на закладку Permissions
4. Предоставить пользователю соседнего узла доступ на чтение

(в следующей части работы будет возможность проверить правильность назначения прав доступа)



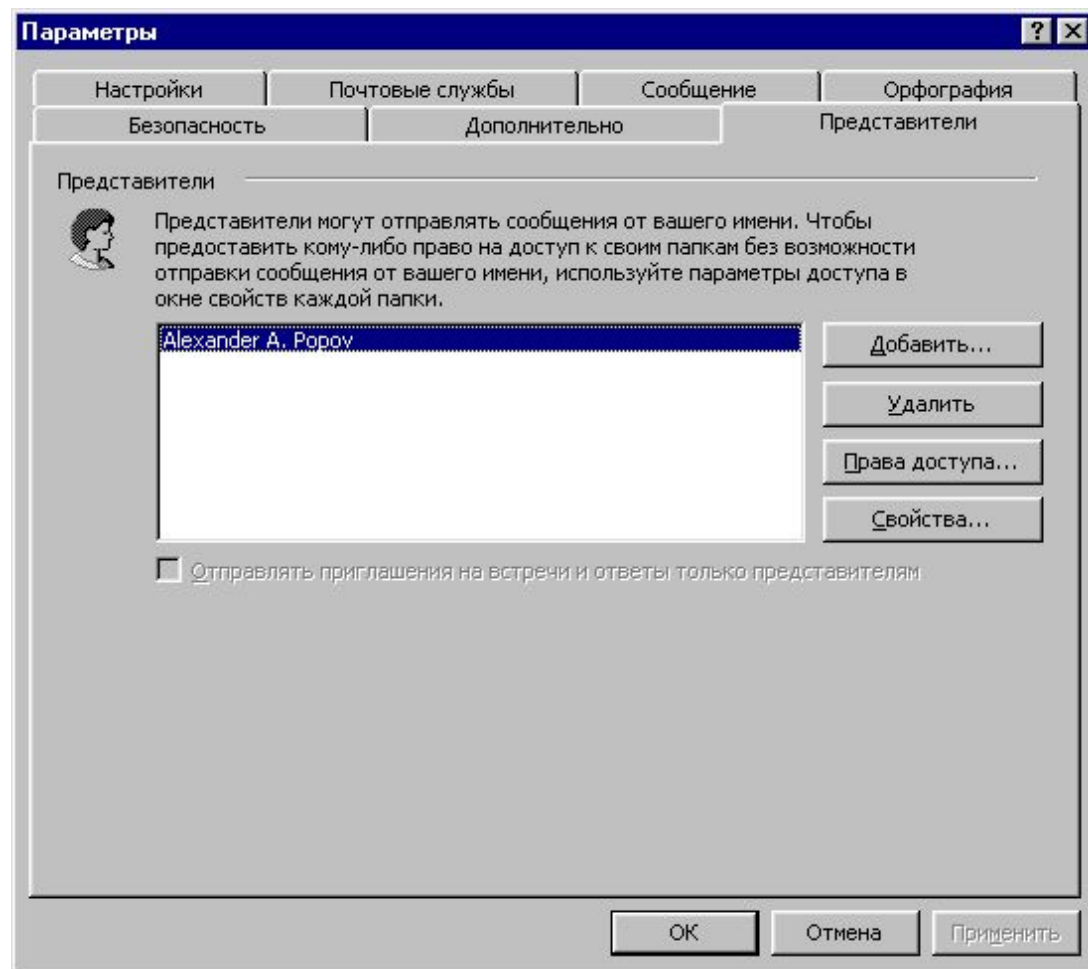
Настройка безопасности почтового клиента



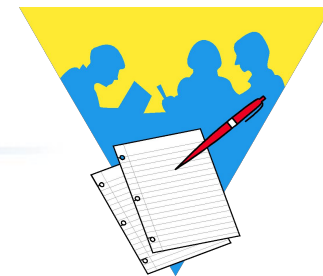
Практическая работа:

Назначение (делегирование) прав доступа к личным папкам

1. Запустить Outlook
2. Выбрать меню Tools, пункт Options, в раскрывшемся окне выбрать закладку Delegates. (Сервис, Параметры, Представители)
3. Щёлкнуть по кнопке Add (Добавить), двойным щелчком выбрать из адресной книги имя пользователя (на соседнем узле)
4. Нажать на кнопку Ok.

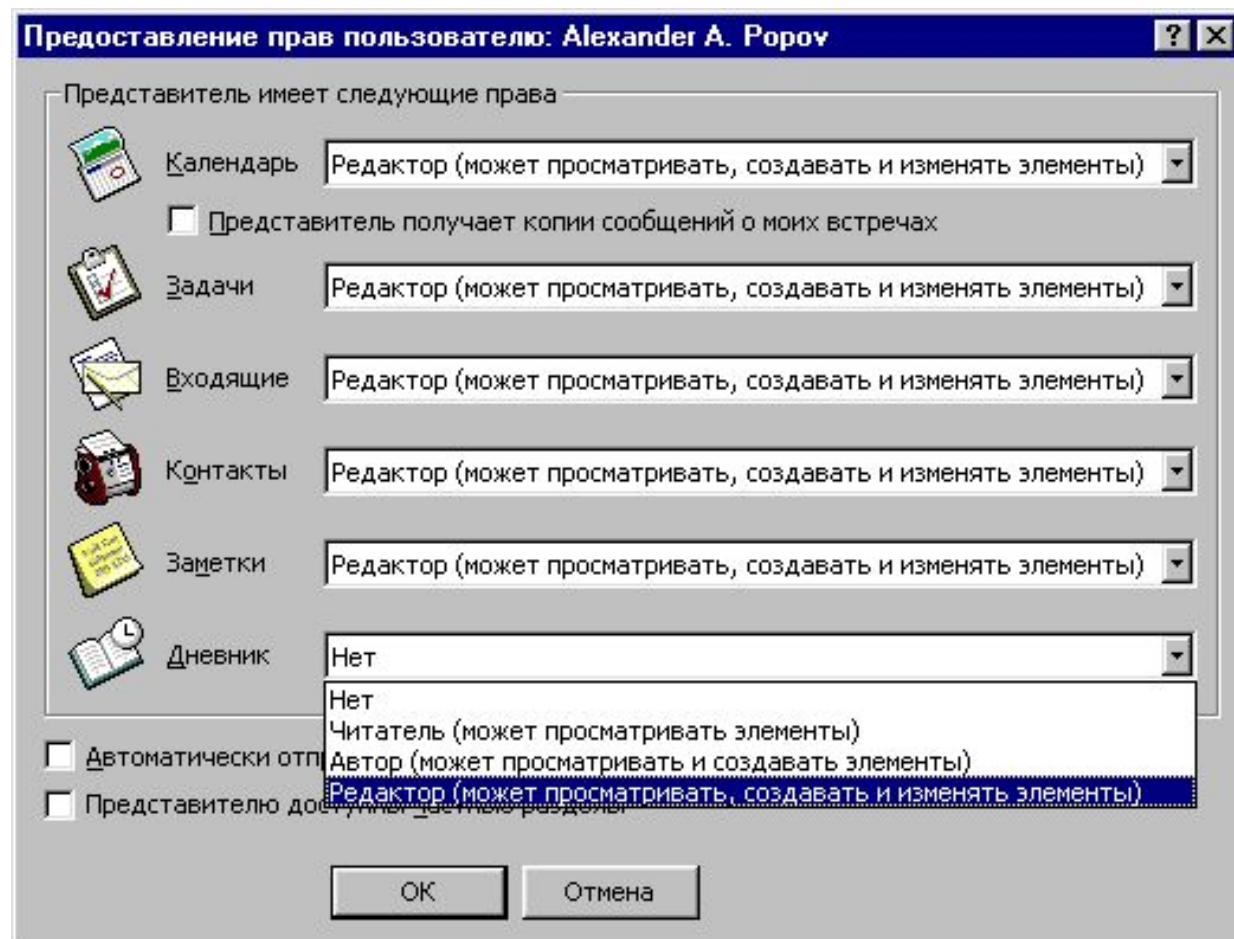


Настройка безопасности почтового клиента

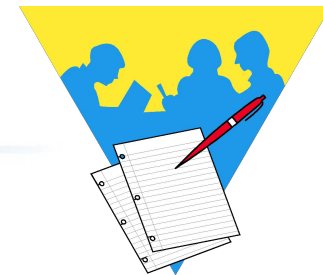


Практическая работа: Назначение (делегирование) прав доступа к личным папкам

Для изменения прав ранее введённого представителя следует выбрать имя этого пользователя и щёлкнуть по кнопке Permissions (Права доступа)



Настройка безопасности почтового клиента

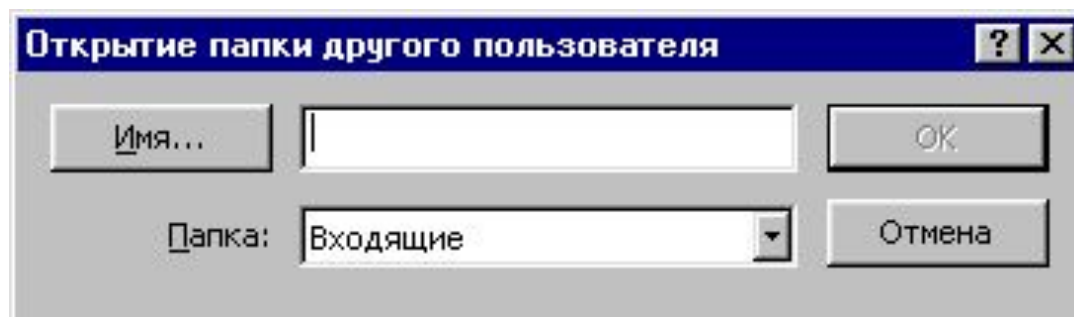


Практическая работа: Использование прав доступа к личным папкам

Цель работы – подключение к папкам другого пользователя почты после назначения вам, как представителю всех необходимых прав

Для этого следует:

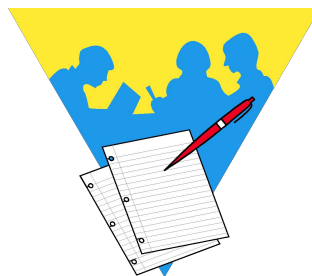
1. При помощи пунктов меню File, Open, Open Other User`s Folder (Файл, Открыть, Папка другого пользователя) открыть окно



2. Указать имя делегированного Вам ящика другого пользователя
Чужие папки открываются в отдельном окне и представителю одновременно доступны окно своего почтового ящика и окно доверенных ему папок.

Практическая работа № 17

Назначение (делегирование) прав доступа к личным папкам



Настройка безопасности почтового клиента

Централизованная настройка

Зоны безопасности

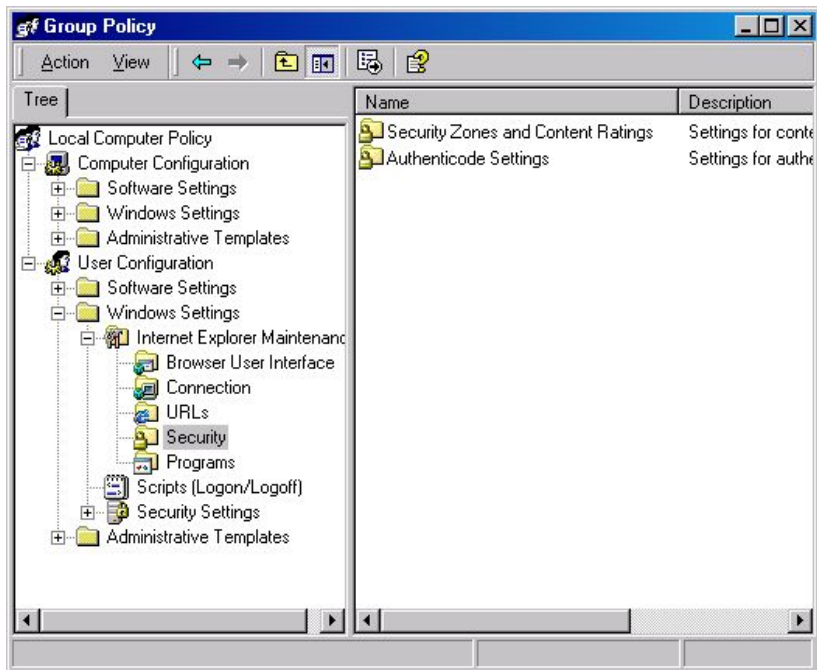
Разрешения файловой системы

Параметры и интерфейс приложений

Настройка безопасности почтового клиента

Централизованная настройка Зоны безопасности

User Configuration – Windows Settings – Internet Explorer Maintenance – Security



Настройка безопасности почтового клиента

Централизованная настройка Разрешения файловой системы

Computer Configuration – Windows Settings – Security Settings – File System

%CommonProgramFiles%*
%ProgramFiles%*
%systemroot%\system32\wscript.exe
%systemroot%\system32\cscript.exe
.....

ocfilesw.inf

Настройка безопасности почтового клиента

Централизованная настройка Параметры и интерфейс приложений

Административные шаблоны, входящие в Office Resource Kit

Template file name	Includes policies
Office10.adm	shared by Office XP components
Access10.adm	for Microsoft Access 2002
Excel10.adm	for Microsoft Excel 2002
Fp10.adm	for Microsoft FrontPage® 2002
Outlk10.adm	for Microsoft Outlook® 2002
Pub10.adm	for Microsoft Publisher 2002
Ppt10.adm	for Microsoft PowerPoint® 2002
Word10.adm	for Microsoft Word 2002
Gal10.adm	for Clip Organizer
Instlr11.adm	for Windows Installer 1.1

Настройка безопасности почтового клиента

Централизованная настройка Outlk10.adm

Tools | Options... – полностью дублирует содержимое диалогового окна Сервис | Параметры

Tools | Macro - безопасность сценариев (VBA)

Instant Messaging – настройка клиента IM

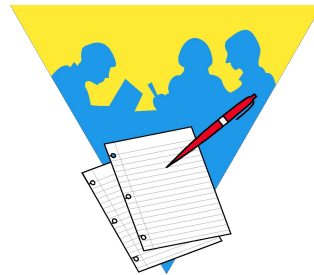
Customizable error messages – специализированные сообщения об ошибках (к примеру: Сбой соединения с сервером. Обратитесь к дежурному администратору. Телефон 555-3-55)

Disable items in user interface - позволяет отключать те или пункты меню;

Miscellaneous - дополнительные параметры, в том числе и запрет изменение профилей.

Практическая работа № 18

Настройка клиентских приложений



Вопросы ?

