Министерство образования и науки Российской Федерации
ФГБОУ ВПО «Уральский государственный лесотехнический университет»
Кафедра Информационных технологий и моделирования

Г.Л. Нохрина

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания по выполнению контрольных работ для студентов 09.03.03 «Прикладная информатика», 38.03.05 «Бинес-информатика» всех форм обучения

ЕКАТЕРИНБУРГ 2014 г.

Содержание

Введение

Данные методические указания предназначены в помощь студентам специальности 080801.65, направлений 080800.62 и 230700.62 при выполнении лабораторных работ по курсу «Информационная безопасность». Кроме того, эти методические указания можно использовать и студентам специальности 080502 (Экономика на предприятии химико-лесного комплекса) при выполнении лабораторных работ по курсу «Защита информации».

В методических указаниях содержатся краткие теоретические сведения, необходимые при выполнении той или иной работы, и задания по выполнению лабораторных работ.

Тема I. Настройка безопасности и конфиденциальности при работе с программой INTERNET EXPLORER 6.0

Часть 1. Цифровые сертификаты

1.1. Назначение цифровых сертификатов

В настоящее время в России для прохода в большинство учреждений, предприятий, учебных заведений необходимо предъявить пропуск с фотографией, подписаний соответствующими службами безопасности и заверенный печатью.

Цифровой сертификат используемся для аналогичных целей, он применяется для подтверждения соответствия в электронных коммуникациях. Конкретные цели могут быть различными. К основным относится применение цифровых сертификатов для подтверждения подлинности веб-узлов и для подтверждения подлинности пользователя. Например, при посещении веб-узла Интернет-магазина покупатель перед отправкой данных платежной карты может запросить подтверждение подлинности этого веб-узла. Для подтверждения подлинности веб-сервер внсылает клиенту цифровой сертификат, заверенный электронной цифровой подписью (ЭЦП) центра сертификации.

При обращении на защищенный веб-узел в Internet Explorer появляется диалоговая панель Предупреждение безопасности. В ней содержится сообщение, что передаваемые данные (например, номер кредитной карты) не будут доступны третьим лицам, так как предварительно шифруются. В строке состояния отображается значок закрытого замка.

Сертификат содержит серийный номер, информацию о владельце, срок действия, а также может содержась ряд других данных.

1.2. Типы цифровых сертификатов

В Internet Explorer используются личные сфтификаты и сертификаты веб-узлов.

Личный сертификат. Личный сертификат применяется для подтверждения личности пользователя при его обращении на веб-узел, требующий подтверждения пользователя. Личные сертификаты также позволяют пользователям применять цифровые подписи для передачи сообщений электронной почты, шифрования сообщений электронной почты, идентификации пользователя для удаленного компьютера. Личные сертификаты бывают разных уровней. Сертификат *низшего уровня* содержит минимум данных о его владельце. Сертификат *высшего уровня* кроме данных о владельце сертификата может содержать данные о его кредитоспособности. Получение сертификата платное, при этом цена зависит от уровня сертификата. Корневой сертификат — это самоподписной сертификат таких центров сертификации, для которых нет вышестоящей инстанции. В Internet Explorer установлены корневые сертификаты известных центров сертификации, например, VeriSign, GlobalSign NV, Twate Certification и др. Получив файл или сообщение, заверенное одним из этих центров сертификации, можно убедиться в его подлинности.

Сертификат веб-узла. Цифровой сертификат веб-узла подтверждает подлинность клиентам по их запросу. Цифровые сертификаты веб-узлов могут быть следующих типов:

- корпоративные сертификаты, которые идентифицируют организации или их подразделения;
- сертификаты сервера SSL (Secure Sockets Layer [Level]) — уровень защищенных гнезд, протокол безопасных соединений). Этот сертификат удостоверяет, что защищенный SSL-сервер принадлежит конкретной компании, при этом между веб-сервером компании и веб-браузером пользователя используется защищенное соединение по протоколу SSL;
- сертификат беспроводного сервера. Он подтверждает, что между беспроводными клиентами и сервером установлена защищенная связь!

1.3. Где получить цифровой сертификат

Возможны три способа получения цифрового сертификата:

- если организация имеет свой центр сертификации, являющийся отделом службы безопасности, то возможно получение сертификата от своей организации;
- получение сертификата при помощи коммерческого центра сертификации, такого как VeriSign, GlobalSign NV, Twate Certification и др.;
- некоторые приложения, например, некоторые версии Microsoft Office, позволяют самостоятельно создавать цифровой сертификат. В Microsoft Office для этого используется программа SELFCERT.exe.

1.4. Процедура получения личного сертификата при помощи коммерческого центра

Для получения личного сертификата следует обратиться на веб-сервер издателя сертификата (например, www.verisign.com, www.globalsign.net, www.twate.com) и сообщить данные, необходимые для получения сертификата определенного разряда, а также выбрать длину закрытого ключа. Перед отправкой браузер пользователя сгенерирует открытый (публичный) и закрытый ключи и внесет их в защищенную базу данных. Закрытый ключ должен быть известен только владельцу сертификата и никому больше. Открытый ключ распространяется открыто, в том числе помещается в сертификат. Получив оплату за сертификат, сертификационный центр выпускает сертификат и указывает URL, по которому его можно получить. Браузер пользователя автоматически запускает процедуру установки сертификата сразу после его получения.

Лабораторная работа №1. Установка и удаление сертификатов в INTERNET EXPLORER

Чтобы пользователь сам мог посылать зашифрованные или подписанные ЭЦП сообщения и файлы, он должен получить личный сертификат и настроить Internet Explorer (IE) для работы с ним.

Цель лабораторной работы: научиться устанавливать и удалять цифровые сертификаты.

Задание к лабораторной 1

1. Создание папок и Отчета

На диске С в папке «Мои документы» создайте папку с названием группы, в этой папке создайте папку со своей фамилией, в этой папке создайте документ Word. Назовите его Отчет по работе № 1

2. Запуск программы Internet Explorer

Активизировать программу IE можно, установив указателькурсора на значке программы на рабочем столе и дважды нажав а левую клавишу мыши либо выполнив команды ***Пуск ► Программы ► IE.***

Запустите программу Internet Explorer.

3. Вызов справки

В главном меню программы IE выберите пункт ***Справка ►Вызов справки.***

4. В окно введите ключевое слово для поиска введите слово сертификаты, получение личного сертификата и нажмите кнопку ***Показать.***
5. В открывшейся справа панели ознакомьтесь с получением личного сертификата. Использование сертификатов для обеспечения конфиденциальности поместите в свой отчет по работе.
6. Аналогично получите справку по безопасным узлам, введя в окно для поиска ключевое слово ***Сертификаты, безопасные узлы.***
7. Поместите в свой отчет сведения о безопасных узлах.
8. Работа с диалоговой панелью ***Сертификаты.***

Возвратитесь в главное меню программы Internet Explorer и выполните команды ***Сервис ► Свойства обозревателя.***

9. Нажмите кнопку ***Общие*** и в разделе ***Сертификаты*** выберите кнопку ***Сертификаты*** (рис. 1).

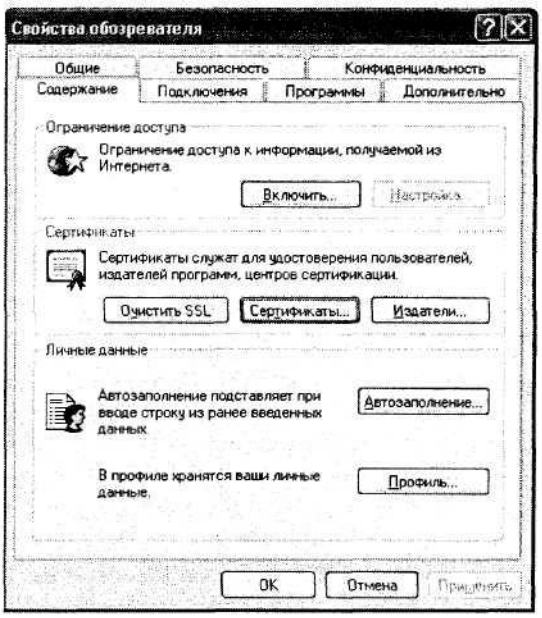

Рис. 1. Кнопка Сертификаты на панели Свойства обозревателя

10. Нажмите на кнопку ***Сертификаты.*** **В** открывшейся панели ***Сертификаты*** (рис. 2) доступны вкладки: ***Личные, Другие пользователи, Промежуточные центры сертификации, Доверенные корневые центры сертификации*** и др.

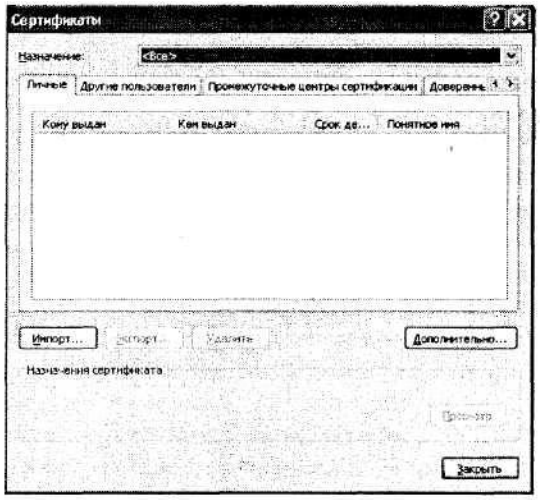

Рис. 2 Панель Сертификаты

11. Сертификаты в категории ***Личные*** имеют открытые ключи. Информация, подписанная посредством личного сертификата, идентифицируется открытым ключом пользователя. По умолчанию IE автоматически размещает все сертификаты, идентифицирующие пользователя, в категорию Личные. Ознакомьтесь с содержимым окна, которое появляется при выборе категории ***Личные.*** Во вкладке Доверенные корневые центры сертификации помещаются данные о корневых сертификатах — ***Кому выдан, Кем выдан, Срок действия, Понятное имя.***
12. Выберите один из корневых сертификатов, поместив на него указатель курсора, и дважды нажмите левую клавишу мыши. Можно также навести указатель курсора на один из корневых сертификатов и нажать кнопку ***Просмотр.***
13. **В** появившейся панели **Сертификат,** ***Сведения о сертификате*** (рис. 3) ознакомьтесь с выбранным корневым сертификатом.

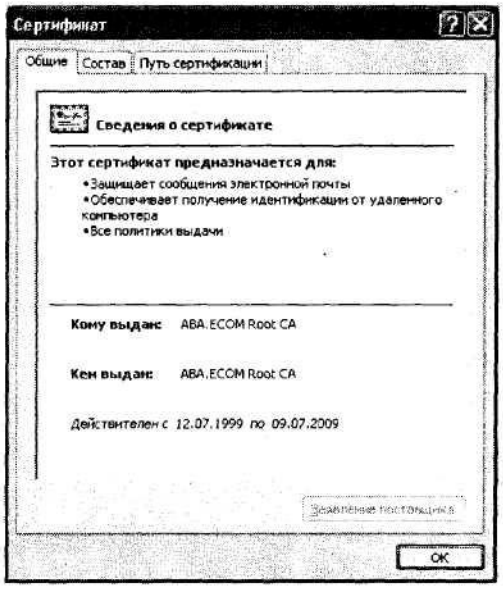

Рис. 3. Панель Сертификат, Сведения о сертификате

14. Ознакомьтесь с выбранным сертификатом — кем выдан, кому выдан, срок действия сертификата. Поместите эти сведения в свой отчет и нажмите кнопку ОК. В результате происходит возврат в диалоговую панель ***Сертификаты.***

15. Для импорта и экспорта сертификатов в IE необходимо вызвать программу менеджера импорта и экспорта. Для этого в диалоговом окне ***Сертификаты*** нажмите на кнопку ***Импорт.***

16. В открывшемся диалоговом окне вас приветствует Мастер импорта сертификатов (рис. 4), следуйте указаниям Мастера. Он позволяет устанавливать или удалять личные сертификаты и сертификаты центров сертификации.

17. Сертификат удаляется в случаях, когда истек срок его Действия или он перестал быть надежным. Однако, если удалить сертификат, то больше не удастся расшифровать данные, зашифрованные при помощи этого сертификата.

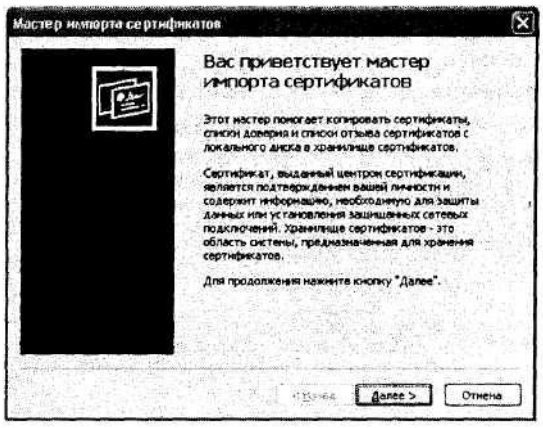

Рис. 4. Окно Мастера импорта сертификатов

18. Выберите один из корневых сертификатов и нажмите на кнопку *Просмотр.*

19. В открывшейся панели *Сертификат,* выберите закладку *Состав* (рис. 5). В открывшемся окне приведены сведения о сертификате. Ознакомьтесь с характеристиками выбранного сертификата.

20. В панели ***Сертификат*** (рис. 5) выберите пункт ***Открытый ключ.*** Наведите указатель курсора на этот пункт и дважды нажмите левую клавишу мыши.

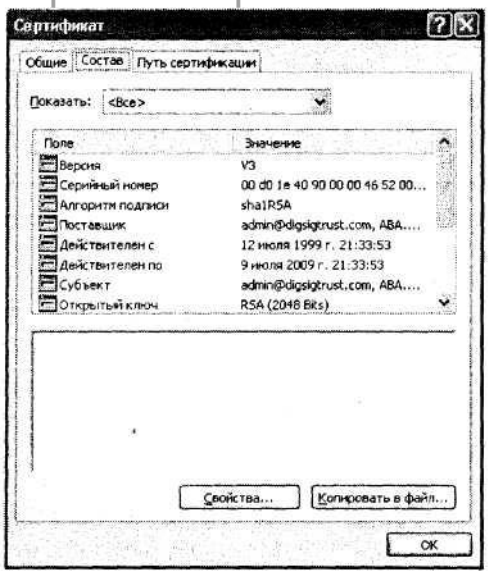

Рис. 1.5. Сведения о сертификате

21. Ознакомьтесь с открытым ключом этого сертификата. Для корневого сертификата ABA.ECOM Root CA открытый ключ показан на рис. 6.

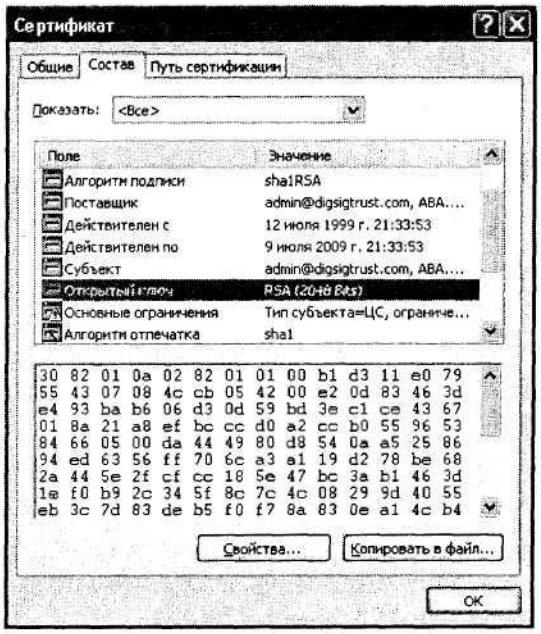

Рис. 6. Открытый ключ сертификата

Лабораторная работа №2 Настройка начальной страницы и рабочего окна обозревателя (браузера) Internet Explorer 6.0

Цель задания: научиться настраивать начальную страницу обозревателя так, чтобы при начальной загрузке программы INTERNET EXPLORER никакая веб-страница не загружалась, научиться настраивать внешний вид рабочего окна программы INTERNET EXPLORER, изменять содержимое панели инструментов.

Задание к лабораторной 2.

1. Активизируйте программу INTERNET EXPLORER. Для этого следует выполнить команды ***Пуск*** ► ***Программы*** ► ***INTERNET EXPLORER*** либо на рабочем столе навести курсор на значок программы INTERNET EXPLORER и дважды нажать левую клавишу мыши.

а) Если в строке ***Адрес*** записано about:blank, то дальнейшая настройка адреса начальной страницы не требуется.

б) Если при запуске INTERNET EXPLORER происходит загрузка начальной страницы, то нажатием на кнопку Стоп прервите загрузку веб-страницы. В строке *Адрес* можно прочитать URL-адрес страницы, которую обозреватель использовал в качестве начальной. Для того чтобы при начальной загрузке не загружалась никакая веб-страница, необходимо:

1) Выполнить команды ***Сервис*** ► ***Свойства обозревателя.*** **В** открывшемся диалоговом окне ***Свойства обозревателя*** откройте вкладку ***Общие.***

2) Нажмите на кнопку ***С пустой.*** **В** поле *Адрес* появится запись about:blank. Это значит, что при начальной загрузке INTERNET EXPLORER никакая веб-страница загружаться не будет.

3) Нажмите кнопку ***Применить.*** После этого закройте диалоговое окно Свойства обозревателя.

4) Повторно запустив программу INTERNET EXPLORER, убедитесь, что никакая веб-страница не загружается и в поле *Адрес* записано about:blank.

2. Активизируйте программу INTERNET EXPLORER. Для этого следует выполнить команды ***Пуск*** ► ***Программы*** ► ***INTERNET EXLORER*** либо на рабочем столе навести курсор на значок программу INTERNET EXPLORER и дважды

нажать левую клавишу мыши.

3. Выполните команду ***Вид*** ► ***Панели инструментов.*** **В** раскрывшемся меню следует убедиться, что пункты ***Обычные кнопки*** и ***Адресная строка*** отмечены флажками, а в остальных пунктах они отсутствуют.

4. Выполните команду ***Вид*** ► ***Панели инструментов*** ► ***Настройка.*** Открывается диалоговое окно ***Настройка панели инструментов***

5. В списке этого окна *Текст* ***кнопки*** следует выбрать ***Без подписей к кнопкам.*** Подписи будут видны при наведении указателя курсора на кнопку.

6. В раскрывшемся списке ***Размер значка*** следует выбрать пунк ***Мелкие значки.***

7. Поместите на панель инструментов командные кнопки. Полный список кнопок, которые могут быть помещены на панель инструментов, приведен в списке ***Имеющиеся кнопки.*** С помощью кнопок ***Добавить*** **и** ***Удалить*** командные кнопки из ***Имеющегося списка*** помещаются в список ***Панель управления.***

8. На панели инструментов следует оставить только пять кнопок, связанных с навигацией в **WWW.** Это кнопки ***Назад, Вперед Остановить, Обновить, Журнал.***

9. Нажав на кнопку ***Закрыть,*** закрыть диалоговое окно ***Настройка панели инструментов.***

10. Нажмите на кнопку ***Переход*** правой клавишей мыши. Кнопка ***Переход*** расположена справа от поля Адрес. В открывшемся меню нужно снять галочку у пункта Кнопка «Переход».

11. Закройте программу INTERNET EXPLORER.

Лабораторная работа №3 Настройка уровня безопасности, конфиденциальности и эффективности работы программы INTERNET EXPLORER

Цель задания: научиться выполнять первичные настройки обозревателя INTERNET EXPLORER, связанные с безопасностью работы в Интернете. Научиться назначать веб-узлу зону безопасности. Научиться выполнять первичные настройки обозревателя IE, связанные с безопасностью работы в Интернете. Настройки выполняются на вкладках ***Безопасность, Дополнительно*** **и** ***Содержание*** и другие.

Использование и настройка журнала соединений

Программа INTERNET EXPLORER выполняет учет посещенных пользователем сайтов. Список посещений заносится в журнал соединений. Если посторонний пользователь имеет доступ к вашей учетной карточке, то он может узнать о посещаемых вами сайтах и времени посещения. Журнал посещений открывается в результате выполнения команд ***Вид*** ► ***Панели обозревателя*** ► ***Журнал.*** **В** открывшейся панели *Журнал,* нажав на кнопку ***Вид,*** можно выбрать сортировку сайтов по дате, по узлу, по посещаемости, по порядку посещения. Если нажать на кнопку *Поиск,* то можно осуществить поиск конкретных сайтов.

Настройка функции Автозаполнение

Программа INTERNET EXPLORER предназначена для экономии времени пользователя путем автоматического заполнения адресов серверов, которые ранее посещались пользователем. Однако эта функция может представлять угрозу безопасности и конфиденциальности пользователя. Для отключения этой функции следует выполнить команды ***Сервис*** ► ***Свойства обозревателя*** ► ***Содержание*** ► ***Автозаполнение.*** В появившемся диалоговом окне ***Настройка автозаполнения*** (рис. 7) нужно отключить все функции автозаполнения, сняв галочки в соответсвующих окошках — веб-адресов, форм, имен пользователей и паролей в формах. Очистить журнал автозаполнения, нажав на кнопки **Очистить формы** и **Очистить пароли.** Нажимается кнопка ОК, после чего панель закрывается.

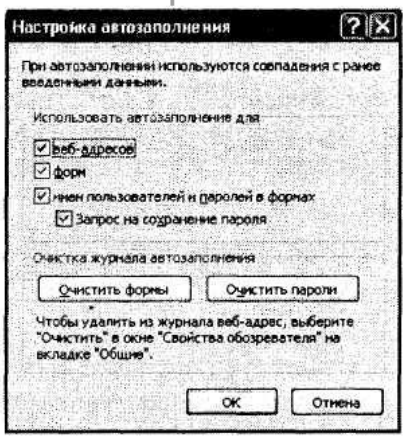

Рис.7. Панель Настройка автозаполнения

Сведения о настройке параметров безопасности, использовании и настройке журнала соединений, настройке функции Автозаполнение поместите в свой Отчет.

Настройка зон безопасности

Зона безопасности — это группа веб-сайтов, имеющих одинаковый уровень безопасности. В программе INTERNET EXPLORER приняты четыре зоны безопасности — зона Интернет, местная интрасеть, надежные узлы и ограниченные узлы.

Надежные узлы — %то веб-узлы, которые не могут причинить вред вашему компьютеру. По умолчанию для этой зоны принимается низкий уровень безопасности.

Ограниченные узлы — это веб-узлы, которые могут причинить вред вашему компьютеру. По умолчанию для этой зоны принимается высокий уровень безопасности.

Местная интрасеть — это веб-узлы вашей локальной сети. Для этой зоны принимается пользовательская настройка уровня безопасности. Для настройки уровня безопасности для этой зоны следует выбрать Другой и в открывшейся панели ***Параметры безопасности*** указать параметры.

Зона Интернета включает все веб-узлы, которые не вошли в остальные зоны безопасности. По умолчанию для этой зоны принимается средний уровень безопасности. Если средний уровень безопасности для этой зоны нас не устраивает, то для настройки уровня безопасности этой зоны следует нажать на кнопку ***Другой*** и в открывшейся панели ***Параметры безопасности*** указать параметры.

Задание к лабораторной 3

Настройка параметров безопасности

1. Активизируйте программу INTERNET EXPLORER. Для этого следует выполнить команды ***Пуск*** ► ***Программы*** ► ***INTERNET EXPLORER*** либо на

рабочем столе навести курсор на значок программы INTERNET EXPLORER и дважды нажать левую клавишу мыши.

2. Выполните команды ***Сервис ► Свойства обозревателя.*** **В** открывшемся окне ***Свойства обозревателя*** выбирается закладка ***Дополнительно.*** Она располагается наверху окна, справа (рис. 8).

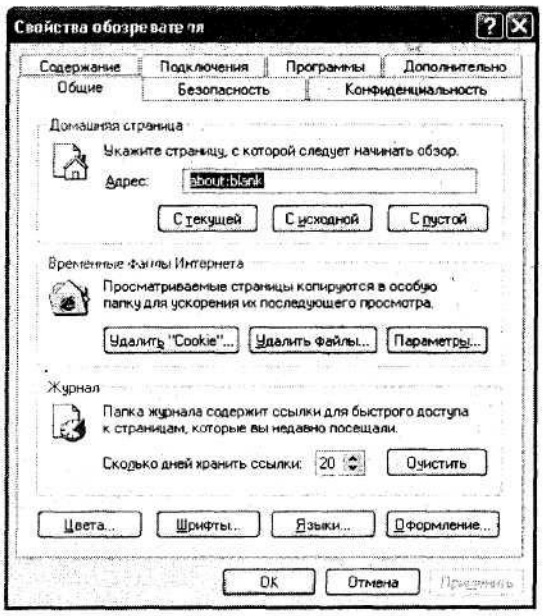

Рис. 8 Панель Свойства обозревателя

3. В разделе ***Безопасность*** окна ***Свойства обозревателя,*** появляющемся после нажатия на закладку ***Дополнительно,*** имеется 12 параметров безопасности. Среди них можно выделить параметры, связанные с безопасностью цифровых сертификатов, и параметры, связанные с включением протоколов безопасности SSL. Для настройки параметров безопасности, связанных с цифровыми сертификатами, проставьте галочки в окошках ***Предупреждать о недействительных сертификатах узлов, Проверять аннулирование сертификатов издателей, Проверять аннулирование сертификатов серверов.*** Для настройки параметров, связанных с протоколами безопасности, укажите, нужно ли использовать протоколы SSL 2.0 и SSL 3.0 для обмена данными с защищенными узлами.

Назначение веб-узлу зоны безопасности

Выполнение:

1. Выполните команды ***IEV*** *Сервис ► Свойства обозревателя.*

2. Откройте вкладку ***Безопасность,*** а затем в открывшемся окне

Свойства обозревателя выберите *Надежные узлы* (можно *Ограни ченные узлы* или *Местная интрасеть).*

3. Нажмите кнопку *Узлы.*

4. В окно *Добавьте узел в зону* введите URL-адрес добавляемого узла. Например, https://www.rambler.ru.

5. Нажмите кнопку *Добавить.*

6. Нажмите кнопку *ОК.*

7. Результаты работы поместите в свой Отчет.

Настройка средств безопасности программы IE

Выполнение:

1. Активизируйте программу **IE.** Для этого следует выполнитькоманды **Пуск ► Программы IE** либо на рабочем столе навести курсор на значок программы **IE** и дважды нажать левую клавишу мыши.

2. Выполните команды **Сервис ► Свойства обозревателя. В** открывшемся окне **Свойства обозревателя** выбирается закладка **Дополнительно.** Она располагается наверху окна, справа.

3. В окне **Свойства обозревателя,** появляющемся после нажатия на закладку **Дополнительно,** следует снять галочку **Задействовать профиль. В** этом случае программа **IE** не будет передавать сведения о личности пользователя по запросам удаленных серверов.

4. В том же окне снимается галочка **Автоматически проверять обновления Internet Explorer.** В этом случае программа IE не будет обращаться к «своему» серверу без ведома пользователя.

5. В том же окне снимите галочку **Использовать встроенное автозаполнение.** Если эту галочку оставить, то посторонние лица могут узнать адреса, по которым обращался владелец ПК.

Настройки пользовательского уровня зоны безопасности

Указатель курсора поместите на закладку **Безопасность,** расположенную в верхней части диалоговой панели. Дважды нажимается левая клавиша мыши. В открывшейся диалоговой панели в разделе **Выберите зону Интернет, чтобы присвоить ей уровень безопасности** следует выбрать зону **Интернет.** Нажимает-

ся кнопка **Другой,** расположенная в нижней части панели. Открывается диалоговая панель **Параметры безопасности. В** этой панели проставьте указатели в разделах:

1. Загрузка — Разрешить.
2. Проверка подлинности пользователя — Автоматический вход

в сеть с текущим именем пользователя.

3. Сценарии:

- Активные сценарии — предлагать;
- Выполнять сценарии приложения Java — предлагать;
- Загрузка неподписанных элементов ActiveX — отключить;
- Загрузка подписанных элементов ActiveX — предлагать;
- Запуск элеметов ActiveX — разрешить;
- Использование элементов ActiveX, не помеченных как безопасные, — отключить.

Настройка личных данных при помощи закладки Содержание

В диалоговом окне **Свойства обозревателя** указатель курсора помещается на закладку **Содержание** и нажимается левая клавиша мыши. В появившейся панели нажимается кнопка **Профиль,** расположенная в нижней части панели. В результате открывается панель, в которой представлены персональные данные о пользователе, известные ПК. Эти данные могут стать доступными другим лицам.

С учетом этого следует откорректировать данные, приведенные в этой панели. Нажимается кнопка ОК.

Настройка конфиденциальности

Выполнить команды **Справка ► Вызов справки ► Указатель.**

В поле поиска введите *Файлы cookie.* В панели Найденные разделы выберите раздел *Общие сведения о файлах cookie.* Ознакомьтесь с назначением файлов *cookie.*

В разделе ***Конфиденциальность*** диалоговой панели ***Свойства обозревателя*** установите средний уровень конфиденциальности. Для этого нажмите на кнопку

По умолчанию. **В** появившейся панели ***Свойства обозревателя*** передвиньте ползунок на нужный уровень (рис. 9).

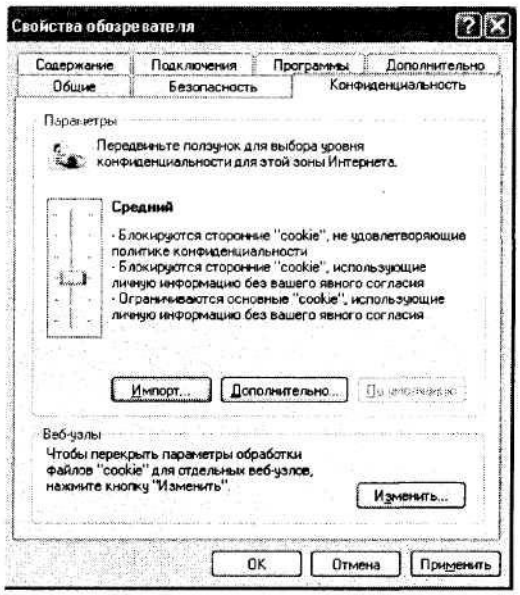

*Рис..**9** Панель для установления уровня **конфиденциальности***

Для установления особых параметров конфиденциальности в разделе ***Конфиденциальность*** диалоговой панели ***Свойства обозревателя*** нажмите на кнопку ***Дополнительно.*** В появившейся панели ***Дополнительные параметры конфиденциальности:***

- установите галочку в разделе *Перекрывать автоматическую обработку файлов cookie;*
- установите *Запрашивать* для основных и сторонних файлов *cookie;*
- поставьте галочку в разделе *Всегда принимать сеансовые файлы* cookie (рис. 10).

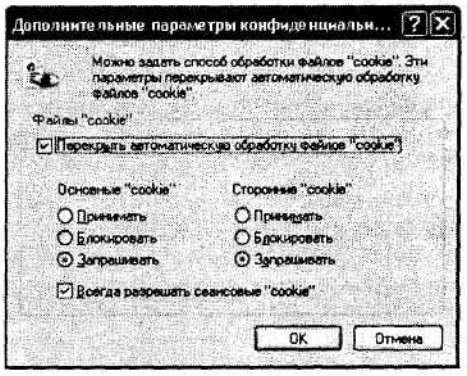

Рис. 10. Панель Дополнительные параметры конфиденциальности

Закройте все окна и завершите работу с IE.

Тема 2. Просмотр и сохранение веб-страниц

Лабораторная работа 4. Просмотр и сохранение веб-страниц

Цель работы:

- научиться загружать веб-страницы при помощи ввода их URL-адреса, а также при помощи пункта меню Избранное;
- научиться сохранять веб-страницы на жестком диске полностью или только текст;
- научиться приемам навигации в www (World Wide Web) при помощи гиперссылок и кнопок навигации, а также запоминать адреса избранных веб-страниц в списке избранных ссылок.

Выполнение:

Поиск веб-страницы по ее URL-адресу

В поле адресной строки программы INTERNET EXPLORER введите URL-адрес сайта, веб-страницы которого нужно посмотреть. Например, адрес электронного магазина, торгующего детскими товарами, www.lukoshko.ru. Нажимается клавиша Enter. Начинают загружаться веб-страницы электронного магазина. Процесс загрузки отображается на линейном индикаторе, расположенном внизу окна. Процесс загрузки можно остановить, нажав на кнопку **Остановить**. На экране будут отображены только те элементы страницы, которые успели загрузиться. Для продолжения загрузки снова нажимается клавиша Enter. Кнопка **Обновить** позволяет вывести на экран страницу повторно. При выполнении работы следует использовать эти кнопки:

а) остановить процесс загрузки сайта, нажав на кнопку **Остановить**, и после ознакомления с загруженной частью веб-страницы продолжить загрузку;

б) нажав на кнопку **Обновить**, повторно загрузить веб-страницу;

в) ознакомиться с сайтом www.lukoshko.ru. Познакомиться с навигацией по сайту при помощи гиперссылок;

г) ознакомиться с работой кнопок **Назад, Вперед, Домой**, расположенных на панели инструментов программы INTERNET EXPLORER. Кнопка

Назад последовательно вызывает на экран предшествующую из просмотренных веб-страниц.

Кнопка **Вперед** последовательно возвращает страницы, просмотренные с помощью кнопки **Назад**. Кнопка Домой выводит на экран домашнюю страницу. Эта страница была установлена в Задании 1.

В отчете по работе следует описать поиск сайта по его адресу, загрузку сайта, действия кнопок **Остановить, Обновить, Назад, Вперед, Домой**, навигацию по сайту при помощи гиперссылок.

Поиск веб-страницы при помощи поисковой системы

1) В поле адресной строки программы INTERNET EXPLORER введите URL-адрес поисковой системы Рамблер или Яндекс (или любой другой). В первом случае вводится www.rambler.ru, во втором случае www.yandex.ru.

2) После загрузки сайта поисковой системы Rambler или Yandex в поле Поиск окна поисковой системы введите ключевые слова «электронная коммерция». После того как поиск будет закончен, запишите и поместите в свой отчет, сколько документов найдено по этим ключевым словам.

3) аналогично запишите и поместите в свой отчет по работе, сколько документов найдено по ключевому слову «электронная» исколько по ключевому слову «коммерция».

Сопоставьте результаты поиска и объясните различие результатов поиска.

В отчете по работе следует описать поиск сайта при помощи поисковой системы, навигацию при помощи гиперссылок, действие кнопок **Назад, Вперед,** обосновать различие в количестве документов, найденных по ключевым словам «электронная коммерция», «электронная», «коммерция», результаты поиска поместить в отчет.

Навигация по www

1. В поле Поиск поисковой системы введите ключевые слова электронная коммерция. После загрузки веб-страницы просмотрите содержимое первой страницы и перейдите на другую страницу. Для этого следует активизировать номер страницы в одном из окошек с номерами страниц в нижней части окна. Указатель курсора наведите на один из пунктов выбранной страницы. Если цвет

указанного пункта изменился, то это означает возможность перехода по этой гиперссылке. Дважды нажмите левую клавишу мыши при расположении указателя курсора на гиперссылке. Произойдет переход на веб-страницу, связанную с выбранной гиперссылкой. Процесс загрузки новой веб-страницы отображается на линейном индикаторе, расположенном в нижней части окна. Ознакомьтесь с содержимым выбранной веб-страницы.

2. Для возврата на веб-страницу «электронная коммерция» нажмите кнопку **Назад** в панели инструментов программы INTERNET EXPLORER. Произойдет переход на ранее выбранную веб-страницу.

3. Нажав на кнопку **Вперед,** снова возвращаемся к веб-странице, просмотренной последней.

4. Элементы навигации для многих сайтов включаются в содержимое веб-страницы. Поместите в отчет найденные в выбранном сайте элементы навигации и поясните их действие.

Сохранение веб-страницы

Перейдите на веб-страницу «электронная коммерция». Наведите указатель курсора на одну из гиперссылок и откройте веб-страницу, связанную с этой гиперссылкой, дважды нажав на гиперссылку левой клавишей мыши. Сохраните веб-страницу в папке со своей фамилией.

1. Для сохранения веб-страницы полностью выполните команды: **Файл ► Сохранить как**. Откроется диалоговая панель Сохранение веб-страницы. В окне Папка укажите папку со своей фамилией. В строке Имя файла задается имя файла, например, Платежные системы. В строке Тип файла указывается веб-страница полностью. Нажмите кнопку Сохранить. В папку пользователя будут помещены две папки. Одна папка содержит текст задания веб-страницы на языке HTML, вторая папка содержит файлы встроенных объектов(рисунков и др.).

2. Если в окне Тип файла задать HTML, то будет сохранен только файл с заданием веб-страницы на языке HTML. Файл со встроенными объектами не сохраняется;

3. Если в окне Тип файла задать Текстовый файл, то сохраняется только

текст документа. Он может быть просмотрен в любом текстовом редакторе. Файл со встроенными объектами не сохраняется.

В папке пользователя нужно сохранить веб-страницу по пп. 1—3. Навести указатель курсора на сохраненный документ и нажать правую клавишу мыши. В появившемся меню выбрать пункт **Свойства**. Записать объем документов по пп. 1—3 в отчет. Сопоставить их, объяснить различие в объемах.

Изменение внешнего вида окна программы INTERNET EXPLORER

Дополните панель инструментов кнопкой **Домой**. Для этого следует выполнить команды **Вид ► Панели инструментов ► Настройка**. При помощи кнопки **Добавить** перенесите кнопку **Домой** из списка **Имеющиеся кнопки** в список **Панель управления**.

На панели инструментов программы INTERNET EXPLORER нажмите на значок **Домой**. В результате попадаете на домашнюю (начальную) страницу. Нажмите клавишу F11 на клавиатуре. Вид окна изменится. Этот режим называется полноэкранным. В этом режиме не выводятся интерфейсные элементы окна (строка меню, панель инструментов и др.) и панель задач Windows. В результате остается больше места для отображения веб-страницы.

Чтобы в этом режиме использовать кнопки панели инструментов, нужно переместить указатель мыши в верхний край экрана. Появляется панель инструментов в уменьшенном виде. При перемещении указателя курсора вниз панель пропадает.

Чтобы в полноэкранном режиме вывести панель задач Windows, нужно указатель курсора переместить в нижний край экрана.

Чтобы восстановить стандартный вид окна, нужно выйти из полноэкранного режима. Для этого нажимается кнопка Восстановить или клавиша F11.

Добавление адреса веб-страницы в Избранное

Выделить адрес последнего посещаемого сайта, выполнить команды **Избранное ► Добавить в избранное**. Адрес будет помещен в раздел Избранное.

Тема 3. Основы криптографической защиты информации

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифрования. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключем в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово ЛУНАТИК, получим следующую таблицу

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче

сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Последовательность действий пользователя:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N=pq$; $M=(p-1)(q-1)$.

2. Получатель выбирает целое случайное число d, которое является взаимопростым со значением M, и вычисляет значение e из условия $ed=1(\text{mod } M)$.

3. d и N публикуются как открытый ключ, e и M являются закрытым ключом.

4. Если S –сообщение и его длина: $1<\text{Len}(S)<N$, то зашифровать этот текст можно как $S'=S^d(\text{mod } N)$, то есть шифруется открытым ключом.

5. Получатель расшифровывает с помощью закрытого ключа: $S=S'^e(\text{mod } N)$.

Лабораторная работа №5

Цель работы: Исследование основных методов криптографической зашиты информации.

Задание к лабораторной: На языке VBA или C++ написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем. В качестве примера в п. 4 приводится алгоритм шифрования методом гаммирования.

Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.

9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

Алгоритм дешифрации аналогичен алгоритму шифрации за исключением того, что из ASCII –кода вычитаем 256 и проверяем больше ноля или нет.

Open Filename For Input As # FileNumber –открытие файла для чтения.

Out Put –для вывода.

В ASCII –коде символы 10 и 13 (возврат каретки).

Надо открывать файлы как двоичные, ключевое слово Binary.

Line Input # FileNumber, A$ -переменная строковая.

Print –для записи.

Для чтения и записи двоичного файла объявляем переменную типа Variant.

Put # NF,, VA

Get # NF,, VA

Close –закрытие файла.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.