Лекция 1. Основные понятия

Структура сети Интернет

Интернет происходит от словосочетания Interconnected networks (связанные сети).

Глобальная сеть – объединения компьютеров, расположенных на удаленном расстоянии, для общего использования мировых информационных ресурсов, глобальное сообщество малых и больших компьютерных сетей.

Услуги Интернет предоставляют специализированные организации – провайдеры.

Провайдер имеет высокоскоростную сеть, к которой подключает своих абонентов.

Через эту сеть абоненты имеют доступ к другим сетям по всему земному шару.

В физическом (аппаратном) плане Интернет состоит из узловых компьютеров (серверов), коммуникационных линий (телефонные линии, выделенные каналы, спутниковая связь) и устройств, обслуживающих сетевые соединения (маршрутизаторов, концентраторов, повторителей).

Через линии связи компьютер-клиент подключается к ближайшему узловому компьютеру-серверу, который передает запрос клиента по сети, пока запрос не достигнет конечного узла, т.е. компьютера с необходимой информацией.

URL адрес

У каждого Web-документа и у каждого объекта, встроенного в такой документ в Интернете есть свой уникальный адрес – он называется унифицированным указателем ресурса URL (Uniformed Resource Locator) или, сокращенно, URL-адресом. Обратившись по этому адресу, можно получить хранящийся там документ.

URL-адрес документа состоит из трех частей и читается слева направо.

В первой части указано имя прикладного протокола, по которому осуществляется доступ к данному ресурсу. Для службы World Wide Web это протокол передачи гипертекста HTTP (HyperText Transfer Protocol). У других служб – другие протоколы. Имя протокола отделяется от остальных частей адреса двоеточием и двумя косыми чертами.

Второй элемент – доменное имя компьютера, на котором хранится данный документ. Элементы доменного имени разделяются точками. После доменного имени ставится косая черта.

Последний элемент адреса – путь доступа к файлу, содержащему Web-документ, на указанном компьютере.

В Windows принято разделять каталоги и папки символом обратной косой черты «\», а в Интернете положено использовать обычную косую черту «/».

Адрес URL формально выглядит так: http://klyaksa.net/htm/exam/answers/images/a23_1.gif

С каждой гиперссылкой в Сети связан Web-адрес некоторого документа или объекта (файла с рисунком, звукозаписью, видеоклипом и т. п.). При щелчке на гиперссылке в Сеть отправляется запрос на поставку того объекта, на который указывает гиперссылка. Если такой объект существует по указанному адресу, он загружается и воспроизводится. Если его нет в природе (например, он перестал существовать по каким-то причинам), выдается сообщение об ошибке – тогда можно вернуться на предыдущую страницу и продолжить работу.

Технология World Wide Web

Популярнейшая служба Интернета – World Wide Web (сокращенно WWW или Web) – Всемирная паутина.

Технология WWW позволяет создавать ссылки (их также называют гиперссылками), которые реализуют переходы не только внутри исходного документа, но и на любой другой документ, находящийся на данном компьютере и, что самое главное, на любой документ любого компьютера, подключенного в данный момент к Интернету.

В качестве указателей ссылок, то есть объектов, активизация которых вызывает переход на другой документ, могут использоваться не только фрагменты текста, но и графические изображения.

Серверы Интернета, реализующие WWW-технологию, называются Web-серверами, а документы, реализованные по технологии WWW, называются Web-страницами.

Всемирная паутина – это десятки миллионов Web-серверов Интернета, содержащих Web-страницы, в которых используется технология гипертекста.

Создание Web-страниц осуществляется с помощью языка разметки гипертекста (Hyper Text Markup Language – HTML).

Web-страница может быть мультимедийной, то есть может содержать ссылки на различные мультимедийные объекты: графические изображения, анимацию, звук и видео.

Интерактивные Web-страницы содержат формы, которые может заполнять посетитель.

Динамический HTML использует объектную модель документа, то есть рассматривает документ как совокупность объектов, свойства которых можно изменять. Это позволяет создавать динамические Web-страницы, то есть страницы, которые могут меняться уже после загрузки в браузер.

Тематически связанные Web-страницы обычно бывают представлены в форме Web-сайта, то есть целостной системы документов, связанных между собой в единое целое с помощью гиперссылок.

Гиперссылка (Hyperlink) - элемент документа для связи между различными компонентами информации внутри самого документа, в других документах, в том числе и размещенных на различных компьютерах.

Гипертекст (Hypertext) - понятие, описывающее тип интерактивной среды с возможностями выполнения переходов по ссылкам. Ссылки (адреса формата URL), внедренные в слова, фразы или рисунки, позволяют пользователю выбрать (установить указатель и нажать левую кнопку мыши) текст или рисунок и немедленно вывести связанные с ним сведения и материалы мультимедиа.

Гипертекстовая система - представление информации в виде некоторого графа, в узлах которого содержатся текстовые элементы (предложения, абзацы, страницы или даже целые статьи либо книги), а между узлами имеются связи, с помощью которых можно переходить от одного текстового элемента к другому.

Основные сервисы сети Интернет

WWW – (Worl Wide Web, Всемирная паутина) – сервис для публикации информации.

E-mail – сервис для обмена текстовыми сообщениями в виде электронных писем.

Доступ к файлам по FTP-протоколу – сервис, который позволяет передавать, получать и редактировать файлы на удаленном компьютере по FTP-протоколу.

WWW (World Wide Web) – Всемирная Паутина, предназначенная для гипертекстового связывания мультимедиа-документов со всего мира и устанавливающая легкодоступные и независимые от физического размещения документов универсальные информационные связи между ними.

Адрес страницы – данные, точно определяющие логический адрес сайта или Web-страницы в Internet.

Браузер (Browser) – средство просмотра. Более полно: программное обеспечение, предоставляющее графический интерфейс для интерактивного поиска, обнаружения, просмотра и обработки данных в сети.

Веб-клиент – программа, позволяющая пользователю запрашивать документы с веб-сервера.

Веб-сервер – программа, запущенная на компьютере, предназначенная для предоставления документов другим компьютерам WWW, которые посылают соответствующие запросы.

Веб-страница – одиночный документ, содержащий гиперссылки, размещенный в WWW и определяемый с помощью адреса URL. Его можно открыть и просмотреть содержание с помощью программы просмотра - браузера. Как правило, это мультимедийные документы, включающие в себя текст, графику, звук, видео, анимацию, гиперссылки на другие документы.

Протокол HTTP (Hypertext Transfer Protocol) – метод, с помощью которого гипертекстовые документы передаются с сервера для просмотра на компьютеры к отдельным пользователям.

Логин (login) – имя пользователя, псевдоним, необходимый для входа в сеть или на удаленный компьютер.

Электронная почта – способ передачи адресованных сообщений с помощью ЭВМ и средств связи.

Имя_пользователя

Имя_сервера

Протокол FTP (File Transfer Protocol) – метод, используемый для обеспечения передачи файлов между разнообразными системами.

Интернет-телефония – технология, позволяющая использовать сети Интернета в качестве средства организации и ведения международных и междугородных телефонных разговоров и передачи факсов в режиме реального времени. При этом звук переводится в цифровую форму и передается аналогично тому, как пересылаются цифровые данные.

Удаленный доступ – технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети.

Лекция 2. Блоги и сайты

Интернет(Internet) – это всемирная информационная сеть.

Сегодня любой человек, обладающий доступом к компьютеру с модемом, может использовать в своей деятельности огромные информационные ресурсы, предоставленные Интернетом.

Телекоммуникации – это общение между людьми, приборами, компьютерами, находящимися в удалении друг от друга, исключающие непосредственный контакт.

Благодаря, развивающимся с огромной скоростью, технологиям Интернета, информационные ресурсы Сети связываются все теснее. Если раньше компьютерные сети в основном служили для обмена письмами по электронной почте, то сегодня мы рассматривает Интернет как единую систему ресурсов. Это и чаты, и телеконференции, и сетевые новости, и форумы, и электронная коммерция.

Сегодня через социальные сети происходит и распространение больших объемов информации. В электронных версиях периодических изданий и блогах широкое распространение получила функция «Поделиться», т. е. распространить информацию в социальных сетях. В последнее время подобная возможность предоставляется на самых разнообразных сайтах. Цель – распространить информацию в широких кругах, привлечь к ней внимание пользователей, получить возможность непосредственного контакта с аудиторией. Сегодня на многих официальных сайтах присутствуют ссылки на аккаунты Facebook, Youtube, Twitter, Flickr и т. п. С помощью этих ссылок можно оперативно размещать информацию в социальных сетях.

Также можно входить на сайт через социальные сети. Сегодня для доступа ко многим сайтам не требуется процедур регистрации и входа в традиционном понимании.

Широкое использование возможностей социальных сетей является одной из характерных тенденций развития Интернета в наши дни. Социальные сети перестали быть данью моде, и используется в качестве эффективного средства коммуникации в самых разных областях: журналистике, политике, торговле, шоу-бизнесе.

Возможности социальных сетей широко используются для публикации информации.

Наиболее популярными социальными сетями у русскоязычных пользователей являются три проекта – ВКонтакте, Одноклассники и Facebook.

Блог (англ. blog, от web log – интернет-журнал событий, интернет-дневник, онлайн-дневник) – веб-сайт, основное содержимое которого – регулярно добавляемые записи, содержащие текст, изображения или мультимедиа.

Блог является одной из разновидностей сайта.

У сайтов – публикация какой-либо информации, не подразумевающая общение с посетителями. В блоге тоже публикуется информация, но она выглядит как обращение от первого лица, даже если авторов блога несколько.

Блог дает возможность ухода от стандартной схемы создания контента сайта, который строится на основе четко определенных семантических ядер и необходимости подбора ключевых слов для точного вхождения по различным запросам. Блог позволяет автору использовать различные художественно-литературные стили, которые не используют в контенте сайта.

Ведение блога подразумевает ответственность автора за достоверность и полноту публикуемой информации, которая обычно основывается на собственном опыте или знаниях. Уровень ответственности влияет на репутацию и на популярность, как блога, так и его автора.

Блог – это один из способов самореализации его автора, с помощью которого он в Интернете показывает свое мировоззрение и высказывает собственное мнение от своего имени по какой-либо тематике. Это интернет-дневник. В последнее время много самостоятельных блогов, несущих и определенную тематическую нагрузку. Чаще всего блоги не просто дневники, а информативные странички.

Сайт это чаще всего крупный проект, несущий информацию определенной тематики. Информация на сайте подается официальным языком. Общение автора с читателями не предусмотрено. При наличии форума, читатели общаются друг с другом, но не с автором проекта.

Блог – это проект одного человека, пишущего на темы, в которых он разбирается. Блог подразумевает диалог автора и посетителя. Авторы блогов не только разрешают комментарии, но и поощряют обсуждения своих статей. Живое общение с читателем и простота – главное отличие блога. Сайт чаще всего, плод трудов целой команды.

Сайт может наполняться либо существовать в том виде, в котором он есть на данный момент времени.

Блог пополняется регулярно и есть смысл в том, чтобы подписываться на новые статьи. Новые статьи блога, как последующие главы книги – продолжают развивать мысль автора.

Создание странички в Instagram

Зарегистрироваться в социальной сети Instagram можно несколькими способами.

Регистрация с мобильного устройства или планшета проще, чем с персонального компьютера.

Для того что бы зарегистрироваться с мобильного устройства поддержки Apple или андроид нужно зайти в Apple Store (Apple), Google Play (андройд) иWindows (магазин) нужно ввести в поиске «Instagram» и установить приложение.

Лекция 3. Защита данных в сетях

Методы защиты данных в сетях

Практически в любой операционной системе есть ошибки. Ошибки могут быть использованы, чтобы атаковать компьютер. Подобные атаки называются атаками на отказ в обслуживании (Denial of Service).

Атака на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

Многие начинающие пользователи ошибочно полагают, что поскольку у них на компьютере «красть нечего», никто не будет их взламывать. К сожалению, это утверждение ошибочно. Сейчас в Сети производится огромное количество атак. Основная цель этих атак – захват управления компьютером пользователя с целью его дальнейшего использования для каких-либо нежелательных действий:

- рассылки спама,
- участия в DDoS-атаке на какой-либо сайт,
- сбор информации о владельце компьютера или поиск других компьютеров для захвата.

Угрозы безопасности информации при работе в Интернете

Говоря о безопасности при работе в Internet, выделяют три основных вида угроз безопасности:

- это угрозы раскрытия,
- целостности,
- отказа в обслуживании.

Основные способы проникновения опасных файлов на компьютер следующие:

Социальная инженерия

Пользователю присылается по почте (или предлагается скачать с сайта) файл, который выдается за что-либо нужное. После запуска этого файла либо ничего не происходит вообще, либо выдается какое-нибудь сообщение об ошибке. В результате – пользователь считает, что файл повредился при скачивании и забывает о нем. На самом деле при запуске данный файл скачает с Интернета и запустит еще одну программу, которая и будет незаметно выполнять все нежелательные действия.

Почтовая программа

Вредоносная программа также присылается по почте, но для ее запуска используются уязвимости (ошибки) почтовых программ. Причем в этом случае никаких действий от пользователя не требуется, ему достаточно просто открыть такое письмо.

Браузер

Браузеры также могут содержать уязвимости, которые при заходе на специально сформированную с учетом этих уязвимостей страницу, позволяют выполнить код. Этот код скачает и запустит вредоносную программу. Некоторые браузеры могут предлагать пользователю исполняемые дополнения, которые также могут содержать вредоносный код.

Ошибки операционной системы

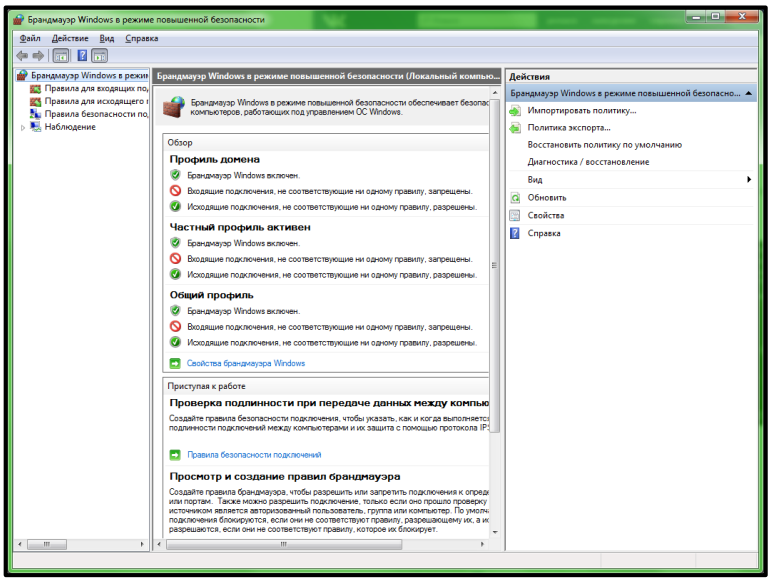
В операционных системах иногда обнаруживаются ошибки, которые позволяют запустить на компьютере вредоносный код вообще без каких-либо действий со стороны пользователя.

Меры защиты:

- Никогда не запускать присланные файлы с расширениями EXE, COM, BAT, WSH, JS, VBS, SCR, PIF, пришедших с незнакомых адресов, даже в том случае, если внешне они выглядят как самораспаковывающиеся архивы ZIP или RAR. Запуск такого файла приведет к тому, что на компьютере может выполниться произвольный код, который скорее всего, окажется вредоносным. Особое внимание нужно обратить на размер файла. Наиболее характерный размер для вирусов - от 20 до 100 Kb.
- Не запускать файл, если он пришел со знакомого адреса, но пришел неожиданно и письмо имеет довольно странное содержание (например, одно слово Hello). Следует связаться с отправителем письма и поинтересоваться, действительно ли он отсылал этот файл. Необходимость такой проверки объясняется тем, что многие вирусы и прочие вредоносные программы используют адресную книгу установленной на компьютере почтовой программы для дальнейшей рассылки своих копий.
- Не открывать присланные файлы прямо из почтовой программы. Один из самых распространенных способов заражения компьютера – это отправка файла с двойным расширением. Например, «picture.jpg.exe». Расширением файла считается то, что стоит после последней точки (.exe). Но пользователь может его просто не увидеть, т.к. из-за длинного имени оно не уместится в окне. Поэтому рекомендуется сохранить файл на диск, просмотреть его свойства (нажатием клавиш Alt+Enter), убедиться, что это не исполняемый файл, и только после этого – открывать двойным щелчком.
- Пользоваться более современным ПО. Вероятность обнаружения уязвимости в программе прямо пропорциональная количеству пользователей, пользующихся этой программой. Именно поэтому наиболее часто уязвимости обнаруживаются в браузере Internet Explorer (MSIE) и почтовой программе Outlook. Большинство автоматизированных атак используют именно эти программы. И если использовать в качестве основного браузера и почтовой программы что-либо другое, вероятность быть атакованным через уязвимости данных программ снижается в десятки раз.

Например, в качестве браузера можно использовать Opera, Mozilla Firefox, в качестве почтовой программы – The Bat, Thunderbird, Becky Mail.

- Устанавливать какое-либо дополнение к браузеру (элемент ActiveX или plug-in), следует только в том случае, если есть полное доверие.
- Использовать персональный firewall (брандмауэр). В случае, если на компьютер все же попадет вредоносная программа, firewall оповестит вас о попытках ее доступа в Сеть (или доступа к ней из Сети) и можно будет легко заблокировать все ее действия. Также firewall помогает защититься от некоторых уязвимостей в операционных системах за счет блокировки доступа к открытым портам, через которые и осуществляются атаки с использованием этих уязвимостей.



Вирусная угроза при работе в Сети

Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, подтолкнуть пользователя к запуску зараженного файла.

Средства защиты информации

- **Технические (аппаратные) средства защиты информации.**

Это различные по типу устройства (механические, электромеханические, электронные и др.), которые на уровне оборудования решают задачи информационной защиты, например, такую задачу, как защита помещения от прослушивания. Они или предотвращают физическое проникновение, или, если проникновение все же случилось, препятствуют доступу к данным, в том числе с помощью маскировки данных. Первую часть задачи обеспечивают замки, решетки на окнах, за-

щитная сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, перекрывающих потенциальные каналы утечки информации (защита помещения от прослушивания) или позволяющих их обнаружить.

- **Программные и технические средства защиты информации от внешних и внутренних угроз.**

Включают в программы для идентификации пользователей, контроля доступа и шифрования информации, удаления временных файлов, тестового контроля системы защиты и др. Преимущество программных средств защиты – универсальность, надёжность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможна зависимость от типов компьютеров и операционной системы.

- **Смешанные аппаратно-программные средства защиты информации.**

Реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства, такие как защита помещения от прослушивания.

- **Организационные средства защиты информации.**

Складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

Firewalls - **брандмауэры** (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Proxy-servers (proxy - доверенность, доверенное лицо).

Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Также этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

Лекция 4. Электронная почта

Электронная почта – сервис сети Интернет

Электронная почта – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети.

Электронный почтовый адрес

Все сервисы сети интернет основаны на тех или иных принципах адресации. Не стала исключением и электронная почта, как составная его часть.

Типичный почтовый адрес пользователя электронной почты выглядит следующим образом: *имя_пользователя_@имя_почтового_сервера*.

Например, почтовый адрес имеет вид: «scorpig@mail.ru», что означает – пользователь «scorping» зарегистрирован на почтовом сервере «www.mail», который располагается в национальной доменной зоне «.ru».

Символ «@» – адресный разделитель, по-английски он обозначает предлог «at» – коммерческое «на», знак принадлежности. Этим разделителем адрес четко делится на две составляющие – имя самого почтового сервера в глобальной сети и имя пользователя на данном сервере.

Адрес вводится на английском языке, без учета регистра (то есть без разницы – заглавными или строчными), без пробелов, без запятых, двоеточий, кавычек и тд.

Адрес необходимо писать правильно – ведь по адресу с опечатками письмо ни куда не дойдет, а будет блуждать в сети, пока не вернется назад к отправителю.

При этом на разных почтовых серверах может быть зарегистрирован один и тот же пользователь.

Но только уникальной сочетание имени конкретного пользователя с именем конкретного сервера и делает почтовый адрес неповторимым нигде в сети.

Адрес почтового ящика может соответствовать как одному человеку, так и группе людей, организации, автомату-обработчику и т.д. – при этом на виде адреса это никаким образом не отображается.

Один и тот же человек может иметь несколько почтовых адресов, как на одном сервере (но с другим именем), так и на разных серверах (в этом случае можно использовать одно имя).

Доступ к своему зарегистрированному почтовому ящику можно получать разными способами.

Первый способ – использование веб-браузера.

Второй способ – использование специализированный почтовой программы.

Почтовые вложения

С особой осторожностью стоит относиться к пересылке вложений.

Потенциально любое вложение может оказаться вредоносной программой, и беспечность совершенно неуместна.

При пересылке вложений нельзя:

1. Посылать вложение при первом обращении к незнакомому человеку или в организацию.
2. Посылать текстовый документ как вложение, если текст можно включить непосредственно в сообщение.
3. Посылать вложения большего объема (более 100 Кбайт) без предварительного согласования с корреспондентом.
4. Посылать в качестве вложений исполняемые файлы любых типов (двоичные, пакетные, сценарные).
5. Открывать и запускать вложения, если они поступили от незнакомого человека (организации) или же полученное сообщение не соответствует общему духу переписки с данным корреспондентом.
6. Открывать и запускать вложение без предварительной антивирусной проверки.
7. Открывать вложения прямо из почтовой программы.

При пересылке вложений рекомендуется:

1. Заранее уведомить корреспондента о своем желании отправить вложение, независимо от объема и содержания файла.
2. Упаковать пересылаемые файлы ZIP-архив и переслать в качестве вложения именно его.
3. Удалить вложение, не открывая и не проверяя его, если есть хотя бы малейшие сомнения в безопасности.
4. Сохранить нужное вложение на жестком диске и потом открыть его в удобное время и желательно, в отсутствие подключения к Интернету.

Этикет электронной почты

С помощью электронной почты нередко приходится переписываться со знакомыми, малознакомыми и даже совсем незнакомыми людьми. При этом эффективность общения может критично зависеть от того, насколько участники общения соблюдают приятный этикет. Для разных видов общения принят разный этикет: то, что можно сказать с глазу на глаз, не всегда доверишь телефону и, тем более, бумаге. Есть свой этикет и у электронной почты.

Во-первых, в электронной почте *не гарантируется тайна переписки*. Нельзя сказать, что все сообщения куда-то записываются, а потом на досуге перечитываются любопытными и спецслужбами.

Во-вторых, правила этикета наиболее важны при общении с незнакомыми людьми или малознакомыми людьми, а также в официальной переписке. Прежде всего, приветствуется и ценится *краткость и точность*.

Обращаться по электронной почте к незнакомым людям допустимо, если адрес корреспондента получен из источника, на который можно сослаться. Отсутствие ответа на личное сообщение следует воспринимать как нежелание, невозможность или нецелесообразность продолжения переписки. Повторно отправлять свое послание в таком случае невежливо.

При переписки с официальными организациями повторная отправка сообщения возможно, но не следует этим злоупотреблять. Каждая организация сама устанавливает для себя срок, который считает допустимым для повторных обращений.

Если пришло сообщение от незнакомого человека, решение о том, нужен ли ответ, принимается в каждом случае индивидуально. Сообщения с рекламным содержанием и непрошенными советами следует рассматривать как «спам» и полностью игнорировать.

Вежливость требует всегда кратко, но точно *указывать тему сообщения*. Если поле темы оставлено пустым, это считается нарушением этикета. Такие сообщения можно уничтожать, не читая.

Не рекомендуется использовать нейтрально сформулированные темы, например «Деловое письмо», «Важный вопрос», «Выгодное предложение». Такая тема ни чего не говорит о том, что на самом деле содержится в письме, и к тому же звучит подозрительно похоже на рекламу. Автоматические системы рассылки рекламных сообщений часто генерируют подобные темы, так как не способны выразить их более внятно. Если сообщение посвящено конкретному вопросу, явно укажите его в поле темы.

При обмене сообщениями принято широко использовать цитирование полученных сообщений. Все почтовые программы и системы Web-mail обеспечивают автоматическую вставку цитат в текст при ответе на сообщения и при их пересылке. Это позволяет получателю сразу понять, о чем идет речь.

Ответ без цитаты считается нарушением этикета, так как создает получателю неудобства. При продолжительной переписке в сообщении могут накапливаться обширные наборы цитат из разных сообщений. При личной переписке принято «чистить» сообщения, удаляя из них цитаты, относящиеся к устаревшим вопросам. В служебной переписке используется полное цитирование: исходное сообщение включается в ответ целиком. В этом случае даже документальная ценность сообщения, а не экономия на объеме пересылаемых данных.

Иногда после обмена рядом посланий тема сообщений перестает соответствовать их реальному содержанию. В этом случае ее имеет смысл сменить. При смене темы принято указывать ее в следующем формате: *Re: новая тема (Was: старая тема).*

Указание прежней темы позволяет не утратить преемственность переписки. В последующих сообщениях старое название темы можно больше не указывать.

Если на полученное сообщение нужно ответить, с ответом лучше не затягивать. Этикет требует *отвечать* на сообщение при первой же возможности, желательно *в течение суток* после получения. При этом предполагается, что корреспонденты не обращаются к электронной почте чаще чем раз в сутки, и более высокую частоту обмена сообщениями следует рассматривать скорее как удачу, чем как требование этикета.

С другой стороны, задержка ответа на несколько дней нарушением этикета тоже не считается. Если долгожданный ответ не приходит, *посылать сообщение повторно не принято*. Допустимый способ поторопить корреспондента – отправить еще одно сообщение с дополнительными вопросами, но не повторение прежнего сообщения.

Не стоит своих корреспондентов в неудобное положение. Если нет возможности немедленно ответить по существу, ответа придется некоторое время подождать.

Защита от почтовых вирусов и спама

Первая угроза – это почтовые вирусы. Поэтому, чтобы оберечь себя от них, нужно следовать следующим пунктам:

1. Использовать в качестве поставщика услуг электронной почты компанию, выполняющую централизованную проверку всех поступающих сообщений на наличие в них опасного содержимого.
2. Установить надежную антивирусную программу, например «Антивирус Касперского» и настроить в ней функцию постоянной защиты. Это обеспечит проверку поступающих почтовых сообщений. Регулярно обновлять базы данных антивирусной программы.
3. Не стоит обновлять операционную систему Windows. Критически относится к заявлениям компании Microsoft о том, что обновленная версия системы более безопасна и надежна чем предыдущая.
4. Не желательно отправлять почтовые сообщения в формате HTML самостоятельно. Только форматом простого текста.
5. Отключить в почтовой программе возможность автоматического открытия поступивших сообщений. Внимательно просматривать заголовки поступившей почты и отрывать только то, что не вызывает сомнения.
6. Особое внимание уделять поступающим почтовым вложениям. Механизм их использования имеет исключительный характер. Извлекать вложения, только если точно есть сведения от кого они поступили, по какому поводу и что в них находится.

Вторая угроза, специфичная для электронной почты, – это спам.

Так называют не запрошенную и ненужную корреспонденцию, поступающую из сомнительных источников. Как правило, она носит рекламный характер. Распространители спама находят адреса электронной почты в разных источниках и используют их для массовой рассылки. Каждое спам-послание само по себе – обычное сообщение электронной почты, по этой причине их достаточно трудно отсеивать автоматически.

Это заставляет принимает специальные меры по борьбе со спамом. Условно их можно разделить на три основные категории.

Первая категория – это *ограничение известности своего электронного адреса*. Как правило, спамеры заимствуют адреса из доступных источников. В частности, адрес может стать известным:

– при его представлении в средствах массовой информации или публикации на веб-сайте;

– при отправке сообщений в группы новостей;

– при регистрации в некоторых веб-службах.

Если электронный адрес используется для любой из этих задач, его попадание в руки спамеров – лишь вопрос времени. Эффективная мера предосторожности – *использование временных, вспомогательных адресов*, зарегистрированных специально для цели публикации.

Вторая мера предосторожности – *корректная реакция на спам*. Лучшая реакция – полное *игнорирование спама*. Не в коем случае не отвечать спамеру, высказывая свое несогласие, возмущение или иные чувства.

Третья мера самозащиты – *использование фильтров*. Определенный уровень защиты обеспечивают системы Web-mail, которые, как правило, централизованно отфильтровывают очевидный спам.

Существуют специальные программы (в том числе и бесплатные), с помощью которых создаются системы фильтров, отсеивающих злокачественный спам от доброкачественных сообщений электронной почты.

Популярными представителями программ этого класса являются: LockSpam (www.polesoft.com) и ChoiceMail (www.digiportal.com).

Практическая работа

1. Создать папку
2. Набрать в адресной строке (самое верхнее поле) URL адрес

http://yandex.ru

↓

Нажать Enter

↓

Нажать треугольную кнопку (Показать автозаполнение адресной строки)

↓

Посмотреть на какие сайты раньше заходили

↓

Нажмите **Ctrl+T** (откроется новая вкладка)

↓

Щелкнуть на кнопку Создать вкладку (у Вас должно быть три открытых вкладки)

↓

(Если не нашли Сделать стартовой)

↓

Нажать на кнопку **Севис**

↓

Выбрать **Свойства браузера**

↓

Вкладка **Общие**

↓

выбрать **Текущая** (или то, что нужно)

↓

(Потом будет открываться, когда нужно с Домика)

↓

(Можно в адресной строке набрать русскими буквами, что ищите)

↓

Наберите в адресной строке (вверху) Кимры компьютерные курсы

↓

Выберите ссылку о курсах

↓

Добавить в Избранное (**нажать на звёздочку**) или Ctrl+D

↓

Откройте Избранное (щёлкните по звёздочке)

↓

Щёлкните правой кнопкой мыши

↓

Выберите **Создать папку**

↓

Назовите Курсы

↓

откройте Избранное

↓

Щёлкните Ctrl+B

↓

Откроется окно Упорядочить Избранное

↓

Создайте папку **Курсы 2 ***

↓

наберите в адресной строке http://lenta.yandex.ru (появится лента новостей в формате RSS)

↓

Вернитесь (домой). Пролистайте страницу вниз **клавиша Пробел или Page Down**

↓

Прейдите в начало страницы клавишей **Home**

↓

Перейдите к предыдущей странице клавишей **BackSpace**

↓

Нажмите клавиши Ctrl+F откроется окно поиска, введите любое слово (что найти)

↓

Нажмите Картинки

↓

Выберите Картины Пикассо

↓

Выберите, что Вам нужно, например, Новый год

↓

нажмите Карты

↓

Выберите Кимры – Музеи

↓

Нажмите Ещё

↓

Выберите Телепрограмма

↓

Нажмите Маркет

возвращайтесь стрелочкой или домиком

↓

Наберите ноубук

↓

Посмотрите цены

↓

Открыть « гугл» Google (любым способом – щёлкнуть если есть слово или набрать в поисковой строке на любомязыке)

↓

Нажать Картинки

↓

Написать Пироги

↓

Выбрать любой (например, ягодный)

↓

Откройте Почту

↓

Нажмите Ещё

↓

Выберите Посмотреть Темы

↓

«Прокрутите»

↓

Выберите новую тему для ящика

↓

Наберите Skype

↓

Google. Выберите YouTube

↓

Наберите Работа в Word

↓

Посмотрите ролик обучающий. Посмотрите комментарии

↓

Сохраните в Избранное (нажать на звёздочку)

↓

Google

↓

Набрать Рецепт пирог

↓

Выбрать любой

↓

Файл (вверху окна)

↓

Сохранить как

↓

Выбрать Свою папку

↓

Посмотреть в папке (как сохранилось)