# Вопросы безопасности в сети Интернет

- правила личной безопасности

# Вопросы безопасности в сети Интернет

- **Вредоносная программа** — программное обеспечение, злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.

- **Основные правила безопасности в сети Интернет :**
- Будьте аккуратны со ссылками, содержащимися в электронных посланиях. Они могут вести совсем не туда, куда указывает текстовая информация.
- Не отправляйте конфиденциальную личную или финансовую информацию, если только она не зашифрована (при работе на защищенном веб-сайте). Обычные письма по электронной почте не шифруются.

# Основные правила безопасности в сети Интернет

- При передаче конфиденциальной информации ищите символ замка в правом нижнем углу веб-страницы. Этот символ указывает на то, что сайт работает в защищенном режиме. Вы должны увидеть его ПРЕЖДЕ, чем Вы введете конфиденциальную информацию.
- Убедитесь, что веб-сайты, с которыми Вы работаете, содержат заявления о соблюдении конфиденциальности и безопасности, и внимательно их изучите.
- Убедитесь, что необходимый вам URL появляется в поле «адрес» или «узел» вашего браузера. Некоторые веб-сайты могут казаться похожими на необходимый Вам, но в действительности быть фальсифицированными.

*Потратьте несколько лишних секунд и напечатайте URL лично.*

- Используйте надежные пароли или ПИНы для Ваших счетов в Интернете. Выбирайте слова, которые другим будет трудно угадать, и используйте разный пароль для каждого Вашего счета. Используйте буквы и цифры, а также сочетание заглавных и строчных букв, если пароли или ПИНы различают строчные и заглавные буквы.
- При выходе из программы делайте это в соответствии с установленными процедурами. Не закрывайте браузер просто так! Выполняйте инструкции по выходу из безопасной зоны для обеспечения Вашей безопасности.
- Избегайте осуществления любых банковских операций в местах, где услуги Интернет являются общедоступными, например в Интернет-кафе.

## Основные правила обращения с Логином и Паролем

- Не сообщайте Ваш пароль другим лицам!

- Не отвечайте на послания по электронной почте с запросами о Ваших личных данных!

- Относитесь с подозрением к любой компании или лицу, запрашивающим Ваш пароль, номер паспорта или другую конфиденциальную информацию. Сотрудники компании NetByNet никогда не запрашивает информацию такого рода по электронной почте.

- Периодически проверяйте свой компьютер антивирусной программой на отсутствие программ-шпионов, крадущих пароли и личные данные.

- Все действия совершенные под Вашими логином/паролем юридически считаются совершенными Вами.

# Компьютерные вирусы

**Компьютерный вирус** — разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

*Неспециалисты к компьютерным вирусам иногда причисляют и другие виды вредоносных программ, такие как трояны, программы-шпионы и даже спам.*

*Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру, организуя вирусные эпидемии.*

# Троянская программа

 **Троянская программа** (троян, троянец, троянский конь, трой) — вредоносная программа, проникающая на компьютер под видом безвредной — кодека, скринсейвера, хакерского ПО и т. д.

*«Троянские кони» не имеют собственного механизма распространения, и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам, и «червей», которые копируют себя по сети. Впрочем, троянская программа может нести вирусное тело.*

**Троянская программа, будучи запущенной на компьютере, может:**

- мешать работе пользователя (в шутку, по ошибке или для достижения каких-либо других целей);
- шпионить за пользователем;
- использовать ресурсы компьютера для какой-либо незаконной (а иногда и наносящей прямой ущерб) деятельности.

# Программы-шпионы

- **Spyware** (шпионское программное обеспечение) — программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя.

- Spyware могут осуществлять широкий круг задач, например:

-собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);

-запоминать нажатия клавиш на клавиатуре (кейлоггеры) и записывать скриншоты экрана (screen scraper) и в дальнейшем отправлять информацию создателю spyware;

-несанкционированно и удалённо управлять компьютером (remote control software) — бэкдоры, ботнеты, droneware;

-инсталлировать на компьютер пользователя дополнительные программы;

## Программы-шпионы

- использоваться для несанкционированного анализа состояния систем безопасности (security analysis software) — сканеры портов и уязвимостей и взломщики паролей;

- изменять параметры операционной системы (system modifying software) — руткиты, перехватчики управления (hijackers) и пр.
- перенаправлять активность браузеров, что влечёт за собой посещение веб-сайтов вслепую с риском заражения вирусами.

*К 2006 году spyware стали одним из превалирующих угроз безопасности компьютерных систем, использующих Windows. Компьютеры, в которых Internet Explorer служит основным браузером, являются частично уязвимыми не потому, что Internet Explorer наиболее широко используется, но из-за того, что его тесная интеграция с Windows позволяет spyware получать доступ к ключевым узлам ОС.*

## Программы-шпионы

*До релиза Internet Explorer 7 браузер автоматически выдавал окно инсталляции для любого компонента ActiveX, который веб-сайт хотел установить. Сочетание наивной неосведомлённости пользователя по отношению к spyware и предположение Internet Explorer, что все компоненты ActiveX безвредны, внесло свой вклад в массовое распространение spyware. Многие компоненты spyware также используют изъяны в JavaScript, Internet Explorer и Windows для инсталляции без ведома и/или разрешения пользователя.*

*Реестр Windows содержит множество разделов, которые после модифицирования значений ключей позволяют программе исполняться автоматически при загрузке ОС. Spyware могут использовать такой шаблон для обхождения попыток деинсталляции и удаления.*

*Spyware обычно присоединяют себя из каждого местонахождения в реестре, позволяющего исполнение. Будучи запущенным, spyware контролирует периодически, не удалено ли одно из этих звеньев. Если да, то оно автоматически восстанавливается. Это гарантирует, что spyware будет выполняться во время загрузки ОС, даже если некоторые (или большинство) звенья в реестре автозапуска удалены.*

- **Adware** (Advertisement Software)- Вид программного обеспечения, при использовании которого пользователю принудительно показывается реклама.

## Логическая бомба

- **Логическая бомба** (Logic bomb) — программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных).

*Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определенное время или при выполнении определенных условий, например, в пятницу 13-го или в день смеха.*

## Логическая бомба

- **Логическая бомба** (Logic bomb) — программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных).

*Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определенное время или при выполнении определенных условий, например, в пятницу 13-го или в день смеха.*

# Спам

**Спам** (spam) — массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать.

*Легальность массовой рассылки некоторых видов сообщений, для которых не требуется согласие получателей, может быть закреплена в законодательстве страны. Например, это может касаться сообщений о надвигающихся стихийных бедствиях, массовой мобилизации граждан и т. п.*

*В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Незапрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM (англ. Spam over IM).*

# Спам

*Первоначально слово «SPAM» появилось в 1936 г. Оно расшифровывалось как SPiced hAM (острая ветчина) и было товарным знаком для мясных консервов компании Hormel Foods — острого колбасного фарша из свинины.*

*После Второй мировой войны остались огромные запасы данных консервов, которыми снабжались американские солдаты. Для того, чтобы сбыть свою продукцию не первой свежести, компания Hormel Foods провела первую в своем роде рекламную кампанию. Слово «SPAM» бросалось в глаза на каждом углу, с витрин всех дешёвых магазинов, оно было написано на бортах автобусов и трамваев. Это слово можно было прочесть на фасадах домов и в газетах. Реклама консервов «SPAM» беспрерывно транслировалась по радио. В 1986 г. в конференциях Usenet появилось множество одинаковых сообщений от некоего Дэйва Родеса, который рекламировал новую финансовую пирамиду. Заголовок гласил: «Заработай кучу денег», а в письмах содержалась инструкция, как это сделать. Автор с завидным упорством продолжал дублировать свои тексты, и они настолько приелись подписчикам, что их стали сравнивать с рекламируемыми в скетче консервами.*

*Так за словом «спам» закрепилось новое значение, позднее перешедшее в компьютерную терминологию для обозначения назойливых рекламных рассылок.*

# Фишинг

**Фишинг** (phishing) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

*Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков (Ситибанк, Альфа-банк), сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте).*

*В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. Оказавшись на таком сайте, пользователь может сообщить мошенникам ценную информацию, позволяющую получить доступ к аккаунтам и банковским счетам.*

*Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.*

## Основные правила антивирусной безопасности

- Устанавливайте зарекомендовавшие себя антивирусные программы
- Несмотря на большой выбор антивирусных систем, следует использовать только безусловно зарекомендовавшие себя на нашем рынке пакеты.

*Следует также отдавать предпочтение хорошо поддерживаемым продуктам именно нашего региона, поскольку, несмотря на глобальность сети, большая часть вирусов присуща именно Рунету (русскоязычному Интернету).*

- Периодически обновляйте Вашу антивирусную программу
- Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные которой содержатся в антивирусной базе. *Этого недостаточно для гарантии абсолютной защиты - хотя бы потому, что появляются новые виды вирусных программ*. Поэтому обновлять антивирусные базы надо регулярно.
- Будьте осторожны с файлами в письмах электронной почты. Никогда не открывайте подозрительные файлы, пришедшие от незнакомых Вам людей.
- Никогда не запускайте программы, присланные неизвестным лицом!

*Однако файлы, полученные от «надежных» корреспондентов (знакомых, коллег, друзей), также могут быть инфицированы. Ваши знакомые могут не знать, что с их компьютера несанкционированно отправляются письма: вирус способен осуществлять отправку от чужого имени незаметно для владельца компьютера!*

## Основные правила антивирусной безопасности

- Перед открытием любого файла необходимо проверить его антивирусными средствами.

*Хорошие антивирусные пакеты производят проверку автоматически.*

- Ограничьте круг лиц, пользующихся Вашим компьютером

- Идеальным вариантом является ситуация, когда никто, кроме вас, не имеет доступа к вашему компьютеру. Однако, если это невозможно, необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц.

- Делайте регулярное резервное копирование

*Выполняя это правило, Вы сможете сохранить данные не только при поражении компьютера каким-либо вирусом, но и в случае серьезной поломки в аппаратной части компьютера.*

- Не паникуйте! =)

# Антивирусная программа (антивирус)

- **Антивирусная программа** (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

*Многие современные антивирусы расширяют набор своих функций, позволяя обнаруживать и удалять также троянские и прочие вредоносные программы. Идёт и процесс интеграции антивирусных функций в другие программы — например, файрволы.*

- **Межсетевой экран** (Брандмауэр, Файрволл) — фильтры, их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

*Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать сотни тысяч вирусов, но ни одна из них не даст 100 % защиты.*

# Антивирусная программа (антивирус)

**Методы обнаружения вирусов**

*Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:*

- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах;

-Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

*Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах.*

*Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания), и могут пропускать угрозу от новых, ещё неизвестных им вирусов (эвристическое сканирование не даёт гарантии защиты от всех новых видов вредоносного кода).*

# Антивирусная программа (антивирус)

- **Рекомендуемые мной антивирусные программы:**

**Антивирус Касперского**
**Dr.Web**
**Eset NOD32**
**Symantec**
**Panda Software**