ОСНОВЫ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

Гурский В.М., Гуща А.В., Гурский М.С. (Республика Беларусь, Минск, Академия МВД Республики Беларусь; Республика Беларусь, Минск, БГУИР)

В современном, стремительно развивающемся мире, ключевую роль занимает новая тенденция, заключающаяся во все большей информационной зависимости человечества в целом и отдельного человека, в частности. Как следствие, появляются новые понятия, такие как «информационная политика», «информационная безопасность», «информационная война» и множество других, в той или иной мере связанных с информацией и информатизацией.

Если взглянуть на информацию как на товар, то можно с уверенностью констатировать, что информационная безопасность приводит к огромной экономии средств, в то время как ущерб, нанесенный ей, приводит к невосполнимым затратам. Информационная безопасность – это одна из важнейших проблем, с которой сталкивается современный бизнес и общество в целом. Причины возникновения этой проблемы нам видятся в повсеместном использовании автоматизированных средств накопления, хранения, обработки и передачи информации. Запросы человечества растут – растет и необходимость в улучшении передачи данных. На сегодняшний день не надо дорогостоящих девайсов, чтобы почитать новости, посмотреть фильм, послушать музыку, пообщаться с друзьями. Достаточно просто подключиться к Интернету и найти то, что тебя интересует. Но безопасно ли брать что-то из сети? Безопасная работа в сети Интернет - это еще одна из проблем, с которой сталкивается современное общество.

При работе в Интернете надо помнить, что ресурсы сети Интернет открыты каждому пользователю, но при этом и ресурсы его компьютерной системы могут быть доступны всем, кто обладает необходимыми средствами, навыками и умениями.

Для безопасной работы в сети Интернет можно дать следующие рекомендации:

- всегда устанавливайте файрволл (firewall - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами). Правда, в Windows, начиная с XP есть встроенный файрволл, но его функционал далек от идеального. Некоторые из подобных программ распространяются бесплатно.
- в обязательном порядке используйте антивирус. Он должен быть свежим (последняя версия) и регулярно устанавливать свои базы с обновлениями. Антивирус должен работать постоянно, с момента запуска при загрузке Windows и до окончания работы пользователя, проверяя все используемые программы. Из бесплатных антивирусов можно рекомендовать Avast!, Avira AntiVir, AVG Antivirus и др. Платные антивирусы отличаются от бесплатных тем, что они имеют дополнительные модули безопасности и чаще обновляются. После выбора и установки антивируса, обязательно выполните полную проверку всех жестких дисков на своем компьютере (большинство антивирусов проводит ее автоматически при первом запуске). Кроме того, необходимо регулярно проводить (хотя бы раз в месяц) полную проверку компьютера, а так же всех используемых внешних накопителей (флеш-накопители, внешние диски и т.д.). Это - дополнительная защита ваших данных. Иногда бывает, что антивирус обнаруживает новые вирусные угрозы, только после полной проверки данных компьютера.

У неопытных пользователей сразу же возникает мысль установить два, а порой и три антивируса для лучшей защиты. Однако нельзя устанавливать одновременно на компьютер два антивируса, они будут конфликтовать друг с другом, а это приведет к сбою в системе. Антивирус и брандмауэр могут устанавливаться вместе, т.к. они выполняют разные задачи. Брандмауэр контролирует выход программ в Интернет и защищает его от сетевых атак. Начиная с Windows XP, Microsoft устанавливает свой штатный брандмауэр.

Для проверки и лечения системы можно дополнительно использовать специальные антивирусные утилиты, например Dr.Web CureIt, Kaspersky Virus Removal Tool и др. Они

сканируют и лечат операционную систему, но для ежедневного использования не подойдут, т.к. они не устанавливаются на компьютер.
- отключите или остановите ненужные службы Windows, которые не используете, например, службу доступа к файлам и принтерам и т. п.
- своевременно устанавливайте обновления для Windows, Internet Explorer и т. п.
- осторожно пользуйтесь выходом в сеть в интернет-кафе, в местах доступа Wi-Fi.
- нельзя открывать подозрительные письма, пришедшие на электронный ящик, открывать «прикрепленные» файлы, отвечать на спам и «письма счастья».
- не используйте простые пароли. Существует целый ряд программ созданных специально для подбора комбинации, которые взломают его за считанные секунды. Пароль должен быть не менее 6 символов и желательно с использованием регистра. Нельзя использовать один и тот же пароль во всех приложениях, почтовых ящиках, на все случаи жизни.
- для работы с электронными кошельками, установите специализированные программы для работы с ними (webmoney keeper или интернет-кошелёк для яндекса) – это уменьшит риск кражи данных, чем использовать обычный доступ через браузер.
- не посещайте ресурсы с сомнительной тематикой (сайты интим-услуг, мгновенный заработок в интернете и т.д.). Эти сайты и есть основной источник распространения вирусов пользователям интернета, при помощи использования «дыр» в Internet Explorer и других подобных программах.
- всегда отслеживайте состояния вашего подключения к сети интернет – по непонятному возрастанию трафика можно судить о активности вредоносного кода в операционной системе. Отключайте интернет-соединение, когда оно вами не используется.
- всегда отключайте автозапуск с внешних носителей. Используя чужую флеш-карту на своем компьютере, при автоматическом запуске может автоматически начать работу и вирус.

К сожалению, на современном этапе развитии IT-технологий, никто не даст вам 100% гарантии защиты ваших данных от заражения объектом вируса. На мой взгляд, самой надежной защитой была, и пока остается, своевременная архивация данных. Храня важную информацию на двух, трех разных носителях, вы существенно уменьшаете риск потери этих данных.

СРЕДСТВА ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ В IT–СФЕРЕ

Данилова Г.В. (Республика Беларусь, Минск, БГУИР)

Подготовка компетентных IT-специалистов является важной задачей для Республики Беларусь. Процесс обучения в высших учебных заведениях направлен, в первую очередь, на формирование компетенций студентов в заданных областях. Компетенция – это знания, умения, опыт, личностные качества, необходимые для решения теоретических и практических задач.

Область подготовки IT-специалистов уникальна тем, что происходит быстрое обновление и развитие средств IT-технологий.

Для развития личностных качеств студентов, необходимых для решения теоретических и практических задач, повышения уровня мотивированности студентов к получению знаний и умений, увеличения уровня самостоятельной работы студентов, коммуникативности и ответственности широко используются активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой. Также хорошо стимулирует регулярное обнародование результатов работы группы: обсуждение наиболее удачных работ, анализ слабых работ, общая тенденция группы студентов и индивидуальные изменения. В этом случае хорошо налаженный поток общения преподаватель – студент удачно дополняют поток парной работы студент-студент и поток групповой работы. Интересным решением является также оценивание собственной работы самим студентом и обоснование этой оценки. В процессе такой коммуникации можно откалибровать представления студента о своей работе с оценкой экспертов (преподавателя, одногруппников). Также в этом процессе студент может узнать иные пути и решения поставленной задачи, способы её оптимизации,