Основы информационной безопасности в сети Интернет

Существование и развитие информационного общества на современном этапе характеризуется использованием информационных сетей, глобальных компьютерных сетей и сетей связи. К сетям предъявляются не только требований по обеспечению надёжности передачи данных, стабильности работы, качества и масштабов охвата, но и информационной безопасности. Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Сеть Интернет применяется в повседневной работе и быту большинства людей, и каждый абонент среды Интернет сталкивается с вопросами обеспечения информационной безопасности.

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей и подростков.  Детская аудитория Интернета составляет более 9 млн. человек. Из них большая часть пользуются ресурсами без контроля со стороны родителей.

Самая распространённая проблема, связанная с интернетом: Интернет-угроза. В подобных случаях нужны программы, которые будут анализировать интернет ресурс и при нахождении вируса обновлять свои данные. В таких случаях лучше использовать брандмауэры, потому что это будет самым эффективным способом защиты.

Можно выделить 5 основных правил, соблюдение которых позволит сделать нахождение в сети более безопасной.

1. Надежный пароль. Пароль — это основа безопасности, которой многие пренебрегают, используя простые пароли или одинаковые для всех ресурсах. По совету экспертов пароль должен состоять не менее чем из восьми символов, включающие в себя буквы в разном регистре, цифры и специальные символы в хаотичном порядке или порядке понятном только пользователю. Пароли должны быть разными для разных сайтов.
2. Антивирус. Специалисты советуют устанавливать антивирусы сторонних разработчиков, потому что они более эффективны, благо сейчас есть из чего выбрать, в том числе и бесплатные версии, например Avira Free Antivirus или Avast Free Antivirus.
3. Безопасное соединение. Одним из важнейших аспектов безопасности при работе в интернет, а также сохранностью вашего логина и пароля при работе в различных интернет-сервисах, является использование им зашифрованного соединения по протоколу HTTPS, которое можно проверить в адресной строке, отображается в виде замка.
4. Дополнительные меры. В большинстве крупных интернет-сервисах есть дополнительные меры защиты, одна из которых привязка вашего аккаунта к номеру мобильного телефона, которая на данный момент считается самой надежной из имеющихся, к примеру, того же кодового слова, которое, по сути, является вторым паролем. в почтовых сервисах и социальных сетях сейчас есть возможность привязки к номеру мобильного.
5. Лицензионное ПО. В нашей стране не принято платить за интеллектуальный труд и большинство предпочитает качать его бесплатно с различных торрент трекеров. В одном только не лицензионном Windows XP специалисты находили до 63 всевозможных вирусов, троянов, программ-шпионов и прочего вредоносного кода. При этом, при скачивании, и установке такой “пиратки” антивирусные программы не видят большую часть вредоносного кода, поэтому если пользователи нелицензионного ПО находятся в зоне риска.

В онлайн-опросе, проведенном компанией Mail.Ru Group, в котором приняли участие 1783 человека в возрасте от 15 до 64 лет, которые заходят в интернет хотя бы один раз в неделю пользователи становились жертвами мошенничества по трем причинам: использовали простые пароли, скачали вирусы, переходили на мошеннические сайты.

Литература: Яцук К. В., Смирнов Д. К., Цымбалий А. О. Защита информации в сети // Молодой ученый. — 2018. — №10. — С. 29-32. — URL https://moluch.ru/archive/196/48678/ (дата обращения: 15.11.2018).