Г.А. Воробьев

Культура информационной безопасности в современном обществе

В настоящее время цивилизованные страны находятся в процессе развития информационного общества – общества, построенного на знаниях и информации, высокоинтеллектуального социума, готового изменяться, создавать и продвигать инновации. Отличительными чертами такого общества являются превалирование стоимости информации и знаний в конечной цене продукции, увеличение роли информации, знаний и информационных технологий в жизни общества, увеличение доли ИКТ в структуре ВВП, нарастающая информатизация общества с

использованием телефонии, Интернета, всех категорий СМИ и коммуникаций, формирование глобального информационного пространства.

В условиях, когда роль и ценность информации столь высоки во всех сферах деятельности человечества, возникает необходимость обеспечения защиты этой информации и информационной безопасности ее носителей, потребителей и пользователей.

Таким образом, мы можем выделить два аспекта информационной безопасности: защита информации и защита от вредоносной информации. В обоих случаях необходимо понимать, что проблема обеспечения информационной безопасности является комплексной, а не чисто технической и технологической. Какими бы совершенными ни были технические средства защиты информации, информационная безопасность останется уязвимой без культуры обращения с этой информацией самих людей, т.е. культуры информационной безопасности.

Развитие культуры информационной безопасности сегодня является одной из первоочередных задач нашего государства. Совет безопасности Российской Федерации разработал проект государственной подпрограммы, посвященной данной проблеме.

Под культурой информационной безопасности, в данном проекте, понимаются знания и навыки граждан, в том числе находящихся при исполнении ими профессиональных обязанностей, или организаций, осуществляющих определенные виды деятельности, в области безопасного использования информационных и телекоммуникационных технологий для реализации конституционных прав и свобод в информационной сфере, достижения целей деятельности организаций, а также в области выявления и нейтрализации угроз применения информационных и телекоммуникационных технологий для нанесения ущерба интересам физических лиц и организаций, в том числе деятельности государственных органов власти.

Важной составляющей культуры информационной безопасности являются правила, нормы и стандарты безопасного использования информационных и телекоммуникационных технологий, в том числе этические нормы.

Государство видит следующие основные задачи в данной сфере:

- содействие формированию и укреплению у граждан навыков безопасного поведения в информационной сфере;
- содействие укреплению общепринятых этических норм в области информационно-телекоммуникационных взаимодействий, развития профессиональных правил и стандартов безопасного использования информационных и телекоммуникационных технологий, а

также поддержки общественных инициатив в области формирования культуры информационной безопасности, в том числе противодействия противоправному использованию данных технологий;

- создание системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, в первую очередь информационно-телекоммуникационных сетей, а также ликвидации последствий проявления угроз в информационной сфере.

Государственная политика в области формирования культуры информационной безопасности базируется на следующих принципах:

- координации деятельности государственных органов, бизнес-структур и институтов гражданского общества;
- дифференциации мероприятий государственной политики по основным социальным группам российского общества в рамках преодоления «цифрового неравенства».

Для решения вышеупомянутых задач необходимо осуществление ряда основных мероприятий:

- выработка типовых норм по обеспечению безопасности использования общедоступных и корпоративных информационных систем и информационно-телекоммуникационных сетей;
- стимулирование обмена опытом между организациями и учреждениями по вопросам культуры информационной безопасности.
- подготовка и реализация государственной программы повышения культуры информационной безопасности основных социальных слоев российского общества;
- разработка и реализация образовательных программ по формированию культуры информационной безопасности в рамках подготовки кадров в области обеспечения информационной безопасности в образовательных учреждениях среднего профессионального и высшего профессионального образования в соответствии с федеральными государственными образовательными стандартами;
- обеспечение доступности знаний в области культуры информационной безопасности для основных социальных слоев российского общества;
- стимулирование участия средств массовой информации в пропаганде культуры информационной безопасности;
- активизация возможностей глобальных информационно-телекоммуникационных сетей, прежде всего, социальных сетей, для популяризации культуры информационной безопасности.
- создание и популяризация порталов и сайтов, содействующих

оказанию информационно-консультативной помощи пользователям общедоступных и корпоративных информационных систем и информационно-телекоммуникационных сетей;

- государственная поддержка перспективных проектов негосударственных организаций, направленных на оказание информационно-консультативной помощи в обеспечении безопасного использования общедоступных и корпоративных информационных систем и информационно-телекоммуникационных сетей.

К вышеперечисленным мерам, по нашему мнению, обязательно надо добавить привлечение образовательных учреждений всех уровней, от дошкольного до высшего и послевузовского образования, к воспитанию и развитию культуры информационной безопасности людей всех возрастов и социальных слоев.

Огромную важность в информационном обществе приобретают проблемы защиты детей в информационном пространстве. Сегодня дети уже с дошкольного возраста приобретают навыки пользования информационно-коммуникационными технологиями, попадаю, в том числе, и в Интернет, где, зачастую, они имеют доступ к тем же ресурсам, что и взрослые.

Региональный научно-образовательный центр IT-культуры и инноваций в информатизации совместно с кафедрой информационных технологий, математики и средств дистанционного обучения разработал план мероприятий на 2012 год, нацеленных на повышение уровня культуры информационной безопасности и информационной культуры вообще среди детей и молодежи нашего региона.

В 2012 г. стартует серия дней информационной культуры и культуры информационной безопасности для школьников г. Пятигорска, которые будут проводить студенты общеуниверситетского отделения информационных технологий ПГЛУ.

В дальнейшем такие мероприятия будут проводиться при поддержке государственных структур и партнеров из ИКТ-бизнеса и общественных организаций и для взрослого населения.

В настоящее время теме информационной безопасности в повседневной жизни уделяется внимание и в рамках проекта «Тимуровцы информационного общества», проводимого ПГЛУ уже более двух лет для людей пенсионного возраста и социально уязвим категорий граждан.

Отдельные мероприятия планируются для повышения культуры информационной безопасности родителей.

В рамках данной статьи мы также приводим несколько простых шагов по защите детей от нежелательной информации и угроз в Интер-

нете.

Шаг 1. Определить, какие сайты не должен посещать ребенок в Интернете. Рекомендуется посетить некоторые сайты, предназначенные для детей, уделить особое внимание фактам сбора личной информации на сайтах. Прочесть уведомление о соблюдении конфиденциальности и, если вы не принимаете эти условия, потратить некоторое время на поиски, чтобы найти подобный сайт, на котором не запрашивается личная информация.

Одной из лучших защит от неподобающего содержимого является его блокировка до того, как его можно будет увидеть. В основном это можно осуществить с помощью функции родительского контроля, присутствующей во многих современных операционных системах, телевизорах и игровых приставках.

Шаг 2. Повышение безопасности и конфиденциальности. Кроме блокировки несоответствующего содержимого желательно блокировать доступ на сайты и загрузку файлов, которые могут представлять риск для вашей безопасности и конфиденциальности.

Бесплатные игры, бесплатная музыка, анимационные панели инструментов и другие загружаемые по сети файлы могут подвергать ваш компьютер угрозам со стороны программ-шпионов или другого нежелательного программного обеспечения. В зависимости от возраста ваших детей, вы можете научить их не загружать программы из неизвестных источников в Интернете или спрашивать разрешение перед загрузкой любых материалов из Интернета. Благодаря этому можно предотвратить установку нежелательного программного обеспечения на ваш компьютер.

Ребенок может случайно заразить компьютер, установив на него шпионскую или другую нежелательную программу. Некоторые популярные сайты для детей могут предпринимать попытки загрузки программ без разрешения. Чтобы предотвратить это, необходимо следить за тем, какие сайты посещает ребенок.

Обязательно необходимо использовать антивирус и антишпионское программное обеспечение,

Современные операционные системы позволяют создавать на компьютере несколько учетных записей пользователей. Каждый пользователь входит с использованием своего уникального профиля и имеет собственный рабочий стол и папку «Мои документы». Можно назначить для себя учетную запись администратора, а для детей предоставить учетные записи пользователей с ограниченными правами. Пользователи учетных записей администратора обладают полным контролем над ком-

пьютером. Пользователи с ограниченными правами не могут изменять настройки системы или устанавливать новые устройства или программное обеспечение, включая большинство игр, проигрывателей мультимедиа и программ для общения в чате.

Шаг 3. Напоминать детям о том, что нельзя общаться с незнакомцами в сети.Чаты в реальном времени, общение в социальных сетях, а также программы для обмена мгновенными сообщениями представляют собой отличный способ для детей обсудить свои интересы и обрести друзей. Однако анонимность Интернета также может подвергать детей риску стать жертвами нелегалов и преступников. Чтобы сделать детей менее уязвимыми, необходимо научить их соблюдать следующие меры предосторожности.

- Указывать только свое имя или псевдоним для идентификации.
- Никогда не сообщать номер телефона или адрес.
- Никогда не отправлять свои фотографии.
- Никогда не соглашаться на встречу с теми, с кем они общаются по сети, без контроля со стороны взрослых.

Соблюдение хотя бы таких элементарных правил повседневной информационной безопасности поможет уберечься от многих угроз современного информационного пространства.