ВМЕСТО ПРОЛОГА

А нынче все умы в тумане,
Мораль на нас наводит сон,
Порок любезен — и в романе,
И там уж торжествует он.
. . . . . .
Не мысля гордый свет забавить,
Вниманье дружбы возлюбя,
Хотел бы я тебе представить
. . . . . .
Небрежный плод моих забав,
. . . . . .
Ума холодных наблюдений
И сердца горестных замет.

А.С. Пушкин «Евгений Онегин»

В конце 80-х годов прошлого века произошло знаменательное событие. Стартовал активный процесс перехода человечества к новой фазе развития, которая получила общепризнанное сейчас название постиндустриального (информационного) общества.

Сегодня мы можем констатировать, что основы такого общества сформированы. Нам уже сложно представить нашу жизнь без персональных компьютеров, мобильных телефонов и Интернета. А ведь всего каких-нибудь 15 лет назад все это только начиналось. Можно предположить, что продолжение этого развития будет еще более захватывающим. Не за горами то время, когда все мы и шагу ступить не сможем, чтобы не использовать те или иные, как сейчас принято говорить, сервисы, предоставляемые нам современными информационно-коммуникационными технологиями (ИКТ). И не только в личной жизни. Производство, энергетика, транспорт, связь, финансы — все окажется замкнутым на ИКТ, практически вся жизнь общества станет в сильнейшей степени зависеть от этих технологий.

Хорошо это или плохо? Куда это в конечном счете нас приведет? Все это — острые вопросы нашей современности, определяющие характер будущего общества, систему его ценностей, организацию экономики, геополитику. Но совершенно ясно одно — в условиях все возрастающей информационной зависимости всех сфер деятельности общества надежность и безотказность работы ИКТ, качество информации, которой мы пользуемся, сохранение секретов

приобретают первостепенное значение. Мы должны доверять всем этим информационным сервисам. Иначе последствия для общества и каждого отдельного человека могут быть просто катастрофическими. Таким образом, одной из самых главных проблем развития информационного общества становится обеспечение информационной безопасности личности, общества и государства.

Все мы являемся свидетелями того, как в последние годы обостряется проблема безопасности компьютеров, которые являются объектами, наиболее часто подвергающимися нападению. Нарастают симптомы развивающейся информационной войны. И это не случайно. Интенсивное расширение числа абонентов глобальной сети Интернет несет с собой увеличение уязвимости различного рода информационных и управляющих систем, а использование современного персонального компьютера дает в руки злоумышленникам уникальный по своим возможностям инструмент разведки и различного рода деструктивной деятельности, в том числе подготовки и реализации террористических актов. Довольно широко в этих целях используется и распространение в Сети программ-вирусов, разрушающих данные, носители информации, оборудование и даже наносящих вред здоровью пользователей. В настоящее время появились новые, связанные с этим термины: киберпреступность, кибертерроризм, кибербезопасность.

Чтобы успешно противостоять всему этому потоку вызовов и угроз, каждому члену информационного общества необходимо обладать определенным минимумом знаний, соответствующей информационной культурой и быть готовым к активной борьбе за чистоту ИКТ от различного рода кибермошенников, киберпреступников, кибертеррористов и просто киберхулиганов. В то же время, как показывают статистика и социологические исследования, при быстро возрастающем уровне использования глобальных информационно-коммуникационных сетей (сегодня, например, в России число пользователей сети Интернет достигает 70 миллионов человек) уровень информационной грамотности пользователей и их информационной культуры оказывается чрезвычайно низким (опять же в России только около 10 процентов пользователей Интернета имеют хотя бы минимальное представление об угрозах, которым они подвергаются сами или подвергают других, работая в Сети).

Положение усугубляется еще и тем, что в обществе не сформировалось единой или, по крайней мере, предпочтительной точки зрения на концепцию развития информационных технологий и всего процесса информатизации. Диапазон мнений простирается от требо-

вания полной либерализации свободы действий в глобальных сетях (что как бы определяется демократическими ценностями) до полной регламентации всех действий и введения системы строгих запретов («Уж коли зло пресечь — забрать все книги бы, да сжечь»*). Очевидно, что, как и во всех подобных ситуациях, истина будет лежать где-то посередине. Таким образом, положительной задачей данной книги является попытка представить вопрос о формировании в обществе культуры информационной безопасности с трех различных точек зрения. Первая из них, назовем ее консервативной, опирается на систему жесткого регулирования. Другая, либеральная, первенствующее значение придает соблюдению так называемых «прав человека» и абсолютной свободе слова. Наконец, третья, которую можно назвать рациональной, пытается найти середину между этими полюсами и соблюсти все правила безопасности, опираясь на демократические процедуры.

Материал данной книги представлен в форме бесед «*пользователя*» и трех собеседников, олицетворяющих упомянутые точки зрения, которые названы соответственно «*либералом*», «*консерватором*» и «*профессионалом*». В концептуальном и содержательном планах изложение материала основано на резолюции Генеральной Ассамблеи ООН*, принятой в декабре 2002 года и утвердившей принципы формирования глобальной культуры кибербезопасности. По мнению Генеральной Ассамблеи ООН, этих принципов должны придерживаться все члены глобального информационного общества (государственные органы, предприятия, организации и индивидуальные пользователи), которые создают информационные системы и сети, поставляют их, владеют и управляют ими, обслуживают или используют их. Глобальная культура кибербезопасности в трактовке данной резолюции формируется на основе девяти взаимодополняющих элементов:

- *осведомленность* об угрозах и подходах к обеспечению безопасности информационных систем и сетей;
- *ответственность* пользователей за безопасность информационных систем и сетей сообразно с ролью каждого из них;

---

* А.С. Грибоедов. Горе от ума. — СПб.: Издательская группа «Лениздат», 2016 — 192 с.

* Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Создание глобальной культуры кибербезопасности». http://daccessdds.un.org/doc/UNDOC/GEN/N02/738/25/PDF/N0273825.pdf?OpenElement

- *реагирование*, подразумевающее принятие своевременных и совместных мер по предупреждению инцидентов, затрагивающих безопасность;
- *этика* как учет законных интересов других сторон и признание каждым участником, что его действия или бездействие могут причинить вред другим;
- *демократия* как непременное следование ценностям демократического общества, включая свободу обмена мыслями и идеями и свободный доступ к информации;
- *оценка риска*, предполагающая обязательную оценку потенциального риска любых действий, выявление угроз и факторов уязвимости;
- *проектирование и внедрение средств обеспечения безопасности* как важнейший элемент планирования и проектирования, эксплуатации и использования информационных систем и сетей;
- *управление обеспечением безопасности* на основе комплексного подхода, охватывающего все уровни деятельности членов информационного общества и все аспекты их операций в информационной сфере;
- *переоценка* как своевременное внесение надлежащих изменений в политику, практику, меры и процедуры обеспечения безопасности.

Генеральная Ассамблея ООН предложила всем соответствующим международным организациям и государствам-членам Организации учитывать эти элементы в рамках их усилий по развитию в обществе культуры кибербезопасности. ***Сегодня компетентность в сфере информационных технологий и информационной безопасности становится необходимым условием успешной социализации личности в новой информационной среде общества.***

* * *

При написании книги автором использовался материал учебного пособия, изданного им в 2015 году*, а также материал монографии по вопросам этики в сфере информационных технологий, изданной в 2011 году в соавторстве с О.Ю. Полянской и И.Ю. Алексе-

* Малюк А.А. Защита информации в информационном обществе. — М.: Горячая линия — Телеком, 2015. — 230 с.

евой**. Использовались также материалы исследовательских работ студентов Национального исследовательского ядерного университета «МИФИ» В. Тюхменева, А. Хориной, С. Игнатущенко, А. Калинина, М. Литвинова и Финансового университета при Правительстве Российской Федерации Е. Костенко, И. Сарычева, А. Ивановой, К. Мозгалевой. Заинтересованные читатели найдут в книге сведения по основным проблемам защиты информации в компьютерных сетях, информационно-вычислительных системах и отдельных компьютерах, получат представление о возможных угрозах их безопасности. Исходя из накопленного на сегодняшний день опыта проектирования и эксплуатации компьютерных сетей, в книге рассмотрены основные подходы к защите данных и программ, а также выделены апробированные методы и средства ее обеспечения.

** Малюк А.А., Полянская О.Ю., Алексеева О.Ю. Этика в сфере информационных технологий. — М.: Горячая линия — Телеком, 2011. — 344 с.