В середине 90-х годов еще только начинали говорить о широком распространении компьютерных сетей, телекоммуникаций, банковских систем, автоматизации торговой деятельности. На сегодняшний день глубокого понимания природы асинхронных процессов и вытекающих из нее механизмов корректной работы [2] должны добиться не только специалисты, разрабатывающие программное обеспечение, но и пользователи программных средств.

В отличие от обстановки 70-80 годов уже прошедшего столетия, в нашем насыщенном техникой мире общество испытывает необходимость в большом количестве специалистов, владеющих навыками работы с компьютерами. Большинство людей, использующих в работе вычислительную технику, не пишет собственных программ, но разумное применение пользователями программного обеспечения, ориентированного на помощь в различных сферах человеческой деятельности, должно быть сформировано как важная составляющая культуры взаимодействия в мире компьютеров.

Разработка программного обеспечения уже не является привилегированным занятием небольшого количества подготовленных специалистов. На сегодняшний день уже в школьном возрасте можно выделить немногочисленную, но с горячим энтузиазмом использующую свои собственные программы группу детей, которым нравится управлять работой компьютера. Им, как предполагаемым специалистам в области программирования, особенно необходимо понимание сути работы с машиной.

Разработка и создание многочисленных исполнителей, заполняющих систему обучения параллельному программированию, возможны силами продвинутых старшеклассников по предложенным проектам учителей, а также группами студентов. Но такого рода механизм подходит лишь для экспериментальной обкатки методики преподавания. Разработка качественного учебного программного обеспечения должно соответствовать общетехническим и психолого-педагогическим требованиям. Потребность во все более мощных компьютерах определяется запросами коммерческих приложений и интенсивных по вычислениям научных и технических приложений требуют разработки методов параллельной обработки информации многопроцессорных вычислительных средств.

Для адекватного восприятия современного технического потенциала необходимо начинать подготовку специалистов именно в раннем школьном возрасте, чтобы опередить формирование навыков приведения процессов к последовательным программам. Эту задачу можно успешно решить, используя методику создания игровой среды обучения, в которой взаимодействуют различные исполнители, решающие одну общую задачу. Невозможно сказать, какой глубины знания информатики потребуются нам в ближайшее время. Области применения компьютеров все ширятся и в каждой из этих областей могут потребоваться различные уровни владения программированием.

Литература

1. Звенигородский Г.А. Первые уроки программирования. М.: Наука, 1985.
2. Olszewski J. CSP Laborotory // The Papers of the 24-th SIGCSE Techn. Sympos/ on Computer Scu Education, Indianapolis, Indiana, Feb/ 18 s 19, 1993. s. Indianapolis, 1994.
3. Городняя Л.В., Тихонова Т.И. О перспективе применения языка Робик для обучения параллельному программированию // Программные системы. Новосибирск: Ин-т систем информатики СО РАН, 1995, – с. 37-45.
4. Тихонова Т.И. Применение исполнителей для обучения параллельному программированию// III международная конференция памяти академика А.П. Ершова PSI-99 – г. Новосибирск, 1999. – с.43-44

Федулова К.А., Шайдуров А.А.

ПОНЯТИЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»: СОВРЕМЕННЫЙ АСПЕКТ

ФГАОУ ВПО «Российский государственный профессионально-педагогический университет» (РГППУ)

г. Екатеринбург

Выявление ценности информации, в контексте жизненной позиции в современном информационном мире, все большее значение в обучении и воспитании приобретают информационные технологии. Очень сложно сейчас представить процесс подготовки будущего специалиста без использования всех возможностей персонального компьютера. Эта динамика обусловлена как скоростью изменения социальных процессов, так и стремительным приростом объема знаний. Но наряду с положительными моментами внедрения информационных технологий в педагогический процесс возникают и проблемы, связанные с конфиденциальностью информации, сохранением авторских прав, исчезновением или потерей необходимой информации. Поэтому вопросы безопасности информации и ее защиты сейчас особо актуальны в педагогической среде.

Многие авторы рассматривают понятие «информационная безопасность» как состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы

автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.) [1,2,4,8]; другие [3,5,9] как деятельность, направленную на обеспечение защищенного состояния объекта (в этом значении чаще используется термин «защита информации»).

В представлении Петренко С.А. [6,7] информационная безопасность — это *состояние* защищённости информационной среды, *защита информации* представляет собой *деятельность* по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть *процесс*, направленный на достижение этого состояния.

Информационная безопасность организации — состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

В современном социуме информационная сфера имеет две составляющие [4]: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность.

1. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям.
2. Целостность: обеспечение достоверности и полноты информации и методов её обработки.
3. Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Под защитой информации, в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Наряду с понятием «информационная безопасность» в последнее время стали употреблять понятия «безопасность информации при применении информационных технологий» (состояние защищенности информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована) и «безопасность автоматизированной информационной системы» (состояние защищенности автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность её ресурсов).

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность информационных технологий.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Выделяют и не всегда обязательные категории модели безопасности:

- неотказуемость или апеллируемость (англ. *non-repudiation*) — невозможность отказа от авторства;
- подотчётность (англ. *accountability*) — обеспечение идентификации субъекта доступа и регистрации его действий;
- достоверность (англ. *reliability*) — свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность (англ. *authenticity*) — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Таким образом, информационная безопасность — это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств её обработки.

Галатенко В.А. в своем исследовании предлагает определение «безопасности информации при работе в сети Интернет или локальной сети» как свойство (состояние) передаваемой, накапливаемой,

обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам [2].

Подведя итог, можно сказать, что понятие «информационная безопасность» должно трактоваться как защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура - системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т.д., а также обслуживающий персонал. Неприемлемый ущерб - ущерб, которым нельзя пренебречь.

Стремительное развитие отраслей производства, экономики, банковского дела, космической и военной промышленности, общества и образования способствует накоплению большого количества информации, а ввиду инноваций в области передачи данных вся эта информация должна быть доступна в любое время и в любой точке, но только определенному кругу лиц. В то же время вместе с совершенствованием средств коммуникации начались и негативные процессы (хакерство, промышленный шпионаж, дезинформация). Данные процессы требуют обеспечения сохранности, неизменимости, конфиденциальности и безопасности информации и ее источников, а также достаточного уровня подготовленности современных специалистов некомпьютерных специальностей к правильной организации систем информационной безопасности.

Все это говорит о необходимости обучения студентов дисциплине «Информационная безопасность».

Литература

1. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с.
2. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с.
3. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х тт.
4. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с.
5. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с.
6. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с.
7. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с.
8. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с.
9. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с.
10. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с.

Харисова Г.Г.

ИСПОЛЬЗОВАНИЕ ИКТ В ОБУЧЕНИИ ИНОСТРАННОМУ ЯЗЫКУ В НЕЯЗЫКОВОМ ВУЗЕ.

luisa@intramail.ru
ГОУ ВПО Южно-Уральский Государственный Университет (ЮУрГУ)
г. Нижневартовск

Интеграция российской высшей школы в единое общеевропейское образовательное пространство требует использования новых методик и организационных форм учебного процесса. Преподаватель перестаёт быть основным источником знаний для обучаемых и решение большинства проблем современного образования видится возможным на основе перехода к новым информационным образовательным технологиям. Использование ИКТ на всех стадиях учебного процесса, на наш взгляд, оправдано и позволяет повысить глубину и прочность знаний, расширить уровень развития студентов, дифференцируя процесс обучения, стимулировать их познавательную активность и самостоятельность, прививая навыки исследовательской деятельности. Однако, в учебном процессе важны не сами по себе информационно-коммуникативные технологии, а то, каким образом и насколько способствует их использование достижению поставленных образовательных целей. Применение интерактивных компьютерных средств и пособий, систем тестового контроля достижений, с одной стороны, вынуждает обучаемых находиться в режиме поисковой работы, постоянно отвечая на вопросы и поддерживать обратную связь. С другой стороны, формирование информационной культуры преподавателя