

Аспекты информационной безопасности в курсе информатики и информационных технологий

Виктор Павлович Поляков, ведущий научный сотрудник Института информатизации образования Российской академии образования, доцент, кандидат технических наук

По мере развития информационных и коммуникационных технологий, роста темпов их внедрения во все социально значимые сферы жизнедеятельности современного общества всё значимей становятся проблемы обеспечения информационной безопасности и защиты информации.

Система подготовки в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образовательной деятельности, как общего (пропедевтика, базовый и профильный курсы информатики), так и профессионального образования: среднего, высшего, послевузовского, дополнительного.

В процессе информационной подготовки на этапе общего образования закладываются основы компьютерной грамотности и компьютерной компетентности как **фундамент информационной культуры личности**. В стандарте основного общего образования по информатике и информационным технологиям отмечается, что «изучение информатики и информационных технологий в основной школе должно быть направлено на воспитание ответственного отношения к информации с учётом правовых и этических аспектов её распространения; избирательного отношения к полученной информации». А в обязательный минимум содержания основных образовательных программ включены дидактические единицы, рассматривающие информационные процессы в обществе («информационные ресурсы общества, образовательные информационные ресурсы; личная информация, информационная безопасность, информационные этика и право»). В требованиях к уровню подготовки выпускников школы учтены их умения по применению мер антивирусной безопасности, использованию приобретённых знаний и умений в практической деятельности с соблюдением соответствующих правовых и этических норм. Однако далеко не всегда качество информационной подготовки выпускников школ

соответствует требованиям стандарта, в том числе и в части вопросов информационной безопасности. Актуальными остаются задачи формирования нетерпимости к противоправным действиям в области информационных технологий, ликвидации правового нигилизма и **повышения правовой грамотности** в вопросах использования средств информационных и коммуникационных технологий, защиты интеллектуальной собственности, применению типовых методов и средств обеспечения защиты информации при работе на персональном компьютере, в локальных и глобальных сетях. Поэтому подготовка в области информационной безопасности и защиты информации нуждается в существенном совершенствовании и развитии.

В самом широком плане на государственном уровне под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Для обеспечения национальных интересов в информационной сфере выделены четыре составляющих: *гуманистическая*, направленная на обеспечение конституционных прав и свобод личности, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма; *политическая*, включающая информационное обеспечение государственной политики по доведению достоверной информации до российской и международной общественности; *технологическая*, обеспечивающая развитие современных информационных технологий и отечественной индустрии информации; *секьюритологическая*, рассматривающая задачи защиты информационных ресурсов от несанкционированного доступа, обеспечение безопасности использования информационных и телекоммуникационных систем.

Все вышеперечисленные составляющие информационной безопасности должны найти адек-

ватное отражение в информационной подготовке выпускников. В контексте информационной безопасности должны быть рассмотрены **проблемы компьютерной этики**, призванной ответить на вопросы этического использования компьютерных технологий как социального, так и личностного характера. Одним из основных результатов изучения **социальных аспектов информационной безопасности** должно быть осознание обучаемыми того, что безопасность информационных систем и технологий не является их врождённым свойством, а является результатом комплексной системы защиты информации.

Обязательный компонент подготовки по информационной безопасности — **изучение основ её правового обеспечения**. Неуклонно растёт правоприменительная практика в области борьбы с противоправными деяниями против свободы, чести и достоинства личности, конституционных прав и свобод человека и гражданина, реализуемых в информационной сфере. Эти обстоятельства определяют обязательность изучения основ правового обеспечения информационной безопасности. В контексте информационного права должны изучаться аспекты информационной безопасности в системе национальной безопасности России, соответствующие конституционные нормы и правовые акты, ответственность за компьютерные правонарушения, а также уровни правового регулирования и система государственных органов в области информационной безопасности. Изучение правовых аспектов информационной безопасности должно быть направлено на устранение правового нигилизма, воспитания осознанного восприятия школьниками всех тех ограничений, которые существуют в силу существования государственной, банковской, коммерческой, профессиональной, служебной, личной тайн и авторского права.

В рамках изучения **технологических аспектов обеспечения информационной безопасности** компьютерных систем и технологий предметом изучения должны стать принципы и содержание организационного обеспечения информационной безопасности (политика безопасности, контроль, разграничение и ограничение доступа к информационным ресурсам); принципы создания комплексных систем защиты информации; методы и средства обеспечения информационной безопасности (аутентификация и идентификация пользователей и технических средств, организация защиты информации в персональных компьютерах, криптографичес-

кое преобразование информации и электронная подпись); особенности защиты информации в базах данных и в сетях телекоммуникаций; основы компьютерной вирусологии, методы и средства защиты от компьютерных вирусов и вредоносных программ; требования к пользователям информационными и коммуникационными технологиями и рекомендации по обеспечению личной информационной безопасности.

Для углубления знаний и навыков в области информационной безопасности в рамках курса информатики и информационных технологий необходимо, с учётом интегративного подхода, использовать имеющиеся внутрипредметные связи, прослеживаемые между традиционными разделами информатики и проблематикой информационной безопасности, акцентируя внимание на таких вопросах, как безопасность операционных систем, безопасность офисных приложений, безопасность в базах данных, безопасность при работе в локальных и глобальных сетях, сети и т.п. Особое внимание при этом может быть уделено работе в сети с цифровой подписью, парольной защите документов, шифрованию баз данных, практическому ознакомлению с мерами безопасности в Интернете, в том числе и при работе с электронной почтой, защите от спама, использованию современных средств архивирования и копирования информации, а также пакетов антивирусной защиты.

Серьёзного внимания заслуживают вопросы, связанные с методикой и средствами обучения основам информационной безопасности, т.к. по понятным причинам в обычных компьютерных классах оно может проводиться со значительными ограничениями.

Для изучения правовых основ информационной безопасности целесообразно использовать справочные правовые системы типа «КонсультантПлюс», «Гарант», «Кодекс». Демонстрационные версии этих систем, размещённые на сайтах соответствующих фирм-производителей или на рекламных дисках, позволяют составить перечень документов, регулирующих отношения в сфере информационной безопасности и защиты информации, составить тезаурус по этой предметной области. Кроме того, информация о правовых актах по обеспечению информационной безопасности имеется на сайте Федеральной службы по техническому и экспортному контролю (преемнице Гостехкомиссии при Президенте РФ), может быть найдена на Интернет-порталах <http://www.sec.ru> и <http://www.infosafe.ru>, сайтах ведущих компаний. Интернет-ресурсы по информационной безопасности могут

быть использованы как преподавателями при подготовке к занятиям, так и обучаемыми — для подготовки рефератов.

Весьма актуальны и важны в практическом плане вопросы антивирусной защиты. Для получения навыков антивирусной защиты и ознакомления с состоянием вирусной опасности могут быть рекомендованы сайты соответствующих фирм-производителей антивирусов: ДИАЛОГ-НАУКА (DrWeb), Лаборатория Касперского (AVP), ESET (NOD32), Стокона (Stocopa Antivirus). Обращение к сайтам позволяет актуализировать знания о типах вредоносных программ и методах борьбы с ними.

Важное практическое значение имеет использование для защиты документов возможностей программных средств общего назначения (операционной системы компьютера и интегрированного пакета MS Office). Возможности операционной системы Windows XP по обеспечению информационной безопасности достаточно обширны. Для практического изучения может быть рекомендовано использование её возможностей по разграничению доступа пользователей к ресурсам компьютера (созданию профилей пользователя); скрытие папок и файлов на жёстких дисках; использование стандартных средств архивации, проверки диска, восстановления удалённых файлов.

В числе возможностей пакета MS Office по защите документов и их фрагментов целесообразно изучить использование полей форм в документах Word (в т.ч. и в шаблонах документов); общие средства защиты документа в Word (ограничения на форматирование и редактирование, открытие документа); стандартные средства, обеспечивающие защиту и контроль подлинности документов (лицензии, цифровые подписи и сертификаты); защиту листов и ячеек от изменений в таблицах Excel; шифрование базы данных в Access.

Для практической отработки навыков по обеспечению безопасности в сети целесообразно изучить настройки браузера (Internet Explorer) и электронной почты (Outlook Express), а также подключения брандмауэра операционной системы.

Для ознакомления с реальными средствами защиты информации можно использовать учебные и рекламные материалы фирм-разработчиков (источники: сайты ведущих фирм, например 1С, АНКАД, ЭЛВИС+, КРОК, Крипто-ПРО, Инфосистемы Джет, ЛАНИТ и т.п., материалы выставок, например Softool и презентаций). Кроме

того, перспективным представляется использование программ-имитаторов средств защиты, работа которых, в простейшем случае, имитируется последовательной сменой слайдов, отображающих этапы работы со средством защиты. Совершенствование таких программ-имитаторов должно осуществляться за счёт организации интерактивности. Хороший обучающий эффект может дать лабораторная работа по укомплектованию системы защиты информации организации соответствующими средствами, данные о которых обучаемый должен почерпнуть из каталогов фирм-поставщиков.

Таким образом, несмотря на жёсткие временные рамки реализации учебного плана по информатике и информационным технологиям, тематика информационной безопасности должна стать органической частью информационной подготовки выпускников, необходимым компонентом формирования информационной культуры личности в условиях постиндустриального общества. □