Е. М. Носова, Н. С. Погожин

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВУЗАХ РОССИИ

Тема, вынесенная в название данной статьи, обязывает нас, прежде всего, определиться с понятием «информационная безопасность». Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № ПР-1895, вводит определение данного термина применительно к государству в целом, понимая под ним «состояние защищенности ее (Российской Федерации) национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В то же время в 2006 г. был принят Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть I. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335–1–2006), определяющий информационную безопасность как «все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки».

Очевидно, что применительно к рассматриваемой нами проблематике понятие информационной безопасности будет являться некоторым объединением приведенных формулировок, сведенным к информационному пространству высшего учебного заведения. При этом не следует также пренебрегать фактом «двойственности» информации, т. е. необходимостью говорить как о защите информации, так и о защите от нее.

Почему мы придаем такое большое значение проблемам информационной безопасности в вузах России? Казалось бы, во всех тех вузах, которые имеют дело с закрытой информацией и режимными работами, учреждены специальные службы и сформированы соответствующие подразделения, т. е. решение задач безопасности информации обеспечено. Вообще говоря, это так, но лишь отчасти, поскольку это — решение вчерашнего дня.

В последнее время произошли такие изменения, которые, с одной стороны, настоятельно требуют существенного изменения самого взгляда на проблемы безопасности и качественного совершенствования способов, методов и средств ее обеспечения, а с другой — для решения этих задач к настоящему времени созданы необходимые объективные предпосылки.

Основные аспекты, которые предопределяют объективную необходимость нового подхода к решению проблемы информационной безопасности, следующие.

Первое и, пожалуй, наиболее существенное обстоятельство связано с теми изменениями, которые в последние годы произошли в нашей стране в связи с развитием рыночных отношений и конкуренции во всех сферах хозяйственной деятельности. Причем в данном вопросе хотелось бы выделить два основных момента. Первый — резкое изменение форм собственности, существенно повлиявшее на содержательную часть понятия безопасности информации: если раньше защите подлежали преимущественно военные секреты, то сейчас, наряду с этим, защите подлежат тайны коммерческие, промышленные, банковские и другие; защищать надо авторские права и право собственности на информацию. Возникает необходимость защиты конфиденциальной информации, персональных данных и т. д. Второй момент, связанный с изменениями в стране, заключается в том, что, сделав наше общество весьма открытым, мы тем самым создали благоприятные условия для деятельности спецслужб иностранных государств и разного рода внутренних злоумышленников.

Принципиальное значение с точки зрения актуальности обсуждаемых проблем имеет также всеобщая компьютеризация, охватившая практически все сферы общественной деятельности, в том числе и высшую школу.

С точки зрения организации и обеспечения информационной безопасности это обстоятельство порождает, по меньшей мере, четыре новые задачи.

Во-первых, все большие массивы информации хранятся на машинных носителях и обрабатываются по электронной технологии. При этом, как известно, порождается большое количество каналов, которыми может воспользоваться злоумышленник, а перекрытие этих каналов требует сугубо специфических знаний и навыков.

Во-вторых, в связи с массовым использованием персональных компьютеров интенсивно идет процесс слияния традиционных и автоматизированных технологий обработки информации. Отсюда возникает принципиально новая задача обеспечения безопасности информации в интегрированных информационных технологиях. Имеющийся опыт дает основания утверждать, что эта задача далеко не из простых, а в ее решении большая роль принадлежит руководителям подразделений, обеспечивающих защиту информации.

В-третьих, весьма серьезной представляется задача, обусловленная использованием персональных компьютеров специалистами различных профилей, не имеющими профессиональных знаний по вопросам защиты информации. Нет необходимости доказывать, что в решении и этой задачи главная роль принадлежит руководителям соответствующих специальных подразделений.

В-четвертых, к нашему стыду, надо назвать и такое явление, как хищение вычислительной техники. И здесь главная задача — это решение вопросов по предупреждению таких противоправных действий…

Говоря об актуальности проблем информационной безопасности, нельзя не обратить внимание на следующее обстоятельство. Как известно, в настоящее время наша страна буквально наводнена

средствами вычислительной техники. Положительным здесь является то, что мы получаем в свое распоряжение достаточно совершенные (хотя и не самые новые) средства обработки информации. Но есть здесь и весьма настораживающие моменты. Массовый импорт вычислительной техники, мягко говоря, отнюдь не способствует развитию отечественной электронной промышленности.

Массовое оснащение предприятий, учреждений и других организаций импортными средствами электронной вычислительной техники таит в себе реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и злоумышленного вмешательства в них. Последнее особо опасно в связи с тем, что наблюдаемые в последние годы тенденции в развитии информационных технологий приводят к активному росту качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, вытекающих в так называемые информационные войны.

К вышеизложенному прямое отношение имеет тот общепризнанный и доказуемый факт, что благодаря достижениям микроэлектроники и техники программирования открылись широкие возможности злоумышленного включения в состав средств вычислительной техники вредоносных аппаратных и программных закладок, получивших название электронных вирусов, бомб, троянских коней и т. п.

Обнаружить и обезвредить такие закладки подчас очень и очень сложно, причем сделать это могут только специалисты высочайшей квалификации, а ущерб от воздействия подобного вредоносного программного обеспечения может быть очень большим. Например, в один момент техника по команде извне может выйти из строя (как произошло с автоматизированной системой управления средствами ПВО Ирака во время войны в Персидском заливе). Информация, находящаяся в ЭВМ, может бесконтрольно уничтожаться или искажаться, обрабатываемая информация может фиксироваться и выдаваться злоумышленнику. Данная проблема актуальна также и для вузов.

Можно еще привести целый ряд обстоятельств, аргументирующих актуальность проблем информационной безопасности. Таковым, например, является затронутый выше вопрос информационных войн.

Поэтому применительно к вузам представляется целесообразным обратить внимание на следующий аспект информационной безопасности, выходящий за рамки общераспространенного представления о проблеме. Давно известно, а к настоящему времени строго научно доказано, что информация может оказывать очень большое влияние на мировоззрение, психоэмоциональное состояние и поведение не только отдельно взятых индивидуумов, но и коллективов людей и даже общества в целом. При современном состоянии средств массовой информации открываются практически неограниченные возможности информационного воздействия в глобальном масштабе. Вузы имеют дело с большими коллективами молодых людей, особенно поддающихся такому воздействию. Поэтому игнорировать данный вопрос просто преступно. Проблема эта не только очень сложная, но и весьма деликатная, поскольку речь идет о целенаправленном вмешательстве во внутренний мир человека. К сожалению, она не только в практическом, но и в теоретическом плане разработана недостаточно. Здесь есть над чем задуматься ученым. Видимо, вузовская наука должна включать данные аспекты общей информационной безопасности в сферу своего пристального внимания. В частности, в межвузовской программе по проблемам информационной безопасности следует выделить самостоятельное направление исследований.

Таким образом, в современных условиях обеспечение информационной безопасности в вузах должно носить комплексный характер, причем как по целям, так и по способам и используемым средствам, включающим традиционные и новые, ориентированные на обеспечение информационной безопасности в автоматизированных системах. Принципиальное значение имеет и упомянутый нами вопрос о том, что в современных условиях информационная безопасность не может быть сведена

к уже ставшей традиционной защите информации. Важнейшей составляющей информационной безопасности становится защита от информации, заключающаяся в предупреждении разрушающего воздействия информации на электронные средства, системы и на людей (отдельно взятого человека, коллектив, общество). Необходимо иметь в виду, что защита от информации становится все более актуальной проблемой.

Пути решения проблем информационной безопасности

Само собой разумеется, что при такой важности, сложности и острой актуальности рассматриваемых проблем для их эффективного решения необходим прочный и достаточно развитый научно-методический базис. Учитывая это обстоятельство, Госкомвуз еще в 1992 г. включил в план научных работ межвузовскую программу «Методы и технические средства обеспечения безопасности информации». В программу входило проведение исследований в широком диапазоне проблем — от формирования целостной теории защиты информации и защиты от информации до точных перспективных методов и средств решения соответствующих задач.

В целях аккумулирования, систематизации и распространения достижений в области безопасности информации в МИФИ созданы факультет информационной безопасности и Учебно-научный центр Рособразования по комплексной защите информации. На данный факультет возложены обязанности по разработке и организации основы кадрового обеспечения проблемы информационной безопасности. Следует отдать должное профессорско-преподавательскому составу факультета, который в короткие сроки разработал и опубликовал научно-методические основы решения данной задачи. В настоящее время совершенствуются разработанные учебные программы по соответствующему направлению. Учитывая повышенное влияние на информационную безопасность всеобщей компьютеризации, на факультете создана и ведет большую учебную и научно-исследовательскую работу кафедра компьютерного права.

Большое значение для повышения эффективности работ по обеспечению безопасности информации имеет регулярный обмен опытом как практического решения соответствующих задач, так и теоретических исследований в этом направлении на разного рода симпозиумах, конференциях и семинарах, а также в журнальных и газетных статьях.

Несколько слов о вопросах кадрового обеспечения решения проблем безопасности информации. Организация этих работ и подлежащие анализу задачи настолько сложны и специфичны, что требуют для своей реализации глубоких профессиональных знаний. Исходя из этого, в системе высшей школы организована подготовка кадров соответствующего профиля по нескольким специализациям. Такая подготовка ведется в МИФИ и ряде вузов страны, а в целях обеспечения научно-методического руководства МИФИ определен головным вузом с соответствующими обязанностями и правами.

Говоря о кадровом обеспечении безопасности информации, хотелось бы остановиться на следующем весьма важном вопросе. Совершенно очевидно, что эффективные системы безопасности могут создавать только специалисты-профессионалы и они должны это делать хорошо. Однако обеспечение комплексной информационной безопасности не может быть достигнуто лишь их усилиями в области безопасности. Необходимо непосредственное участие тех руководителей и специалистов, которые организуют и осуществляют процесс сбора, передачи, хранения, обработки и использования информации.

Но очевидно также, что в обработке защищаемой информации участвует широкий круг специалистов самого различного профиля. Поскольку понятие безопасности информации (информационной безопасности) становится все более широким и многоаспектным, а технологии обработки информации все более автоматизируются, то практически всем специалистам необходим некоторый минимум знаний по безопасности информации (информационной безопасности).

Для этого необходимо читать соответствующий курс студентам всех факультетов вузов страны. Такой опыт есть в МИФИ. Здесь 32-часовой курс по основам информационной безопасности читается для всех студентов, причем студенты проявляют к нему повышенный интерес. Такая работа также проводится в некоторых других вузах России.

Думается, что данный вопрос заслуживает серьезного внимания, причем инициирующая роль, несомненно, должна принадлежать организаторам учебного процесса. На их плечи также ложится задача согласования перечня и объемов преподаваемых дисциплин с реальными требованиями, предъявляемыми к молодым специалистам в области информационной безопасности. Так, практика последних лет показывает, что зачастую выпускники вузов не готовы работать в реальных условиях, обладая глубокими теоретическими знаниями лишь по отдельным аспектам защиты информации.

Например, практически не рассматриваются в учебных курсах вопросы экономической эффективности разрабатываемых или используемых систем защиты. В большинстве случаев дается лишь указание на то, что данный анализ необходим. Аналогичная ситуация зачастую складывается и с вопросами использования международных стандартов. Подробно изучая разработанные методы криптографической защиты информации, дипломированные специалисты зачастую не могут решать проблемных задач при работе с системами, ориентированными на международный уровень.

Вопрос выработки у студентов практических навыков является одним из наиболее острых в учебном процессе. В действующих государственных программах время, отводимое для прохождения студентами практики, несравнимо со временем, отводимым для теоретического изучения материала. И решение данного вопроса осложняется тем, что в связи с лавинообразным развитием техники и технологий в области информационной безопасности многие теоретические наработки достаточно быстро теряют свою актуальность.

Из всего сказанного и вытекают те задачи, которые должны решаться вузами России.

Первое и главное — это сохранность государственных секретов.

Второе и не менее важное — это организация контроля передачи информации по техническим каналам и ее сохранения.

Третье — это обеспечение экономической безопасности вуза.

Четвертое — это разработка нового «стандарта специалиста», обладающего не только глубокой теоретической базой, но и практически свободно ориентирующегося в вопросе.

Пятое — это переподготовка преподавательского состава вузов, а также широкое привлечение к проведению занятий практиков в данной предметной отрасли.

И, наконец, шестое — это физическая защита вуза.

Есть и другие задачи, которые также должны решаться внутри вуза, их рассмотрению и будет посвящена следующая статья.