ПРЕПОДАВАНИЕ ДИСЦИПЛИНЫ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» В УНИВЕРСИТЕТАХ РОССИИ И США

Н. В. Медведев

Московский государственный технический университет имени Н. Э. Баумана
Москва, Россия
E-mail: medved@bmstu.ru

Обеспечение информационной безопасности (ИБ) является важной международной проблемой. Ценные и значимые информационные ресурсы могут стать жертвами атак хакеров, кибертеррористов, инсайдеров, социально-политических организаций определенного толка, расположенных по всему миру. Атаки на информационные системы и сети обострялись в течение последних нескольких лет. Критические элементы национальной инфраструктуры (например, электрические сети, ГЭС, химические и ядерные установки, системы трубопроводов, объекты здравоохранения), а также правительственные организации, предприятия и финансовые учреждения уязвимы для кибернетических атак, которые могут вызвать разрушительные последствия.

РФ и США стоят на технологически передовых позициях в указанном аспекте. Обе страны имеют серьезный дефицит специалистов, которые адекватно подготовлены не только для понимания рисков нарушения информационной безопасности, разработки политики ИБ, осуществления контроля безопасности и анализа инцидентов, *но и в понимании мотивов такой деятельности*. Информационная безопасность является междисциплинарной областью и включает в себя несколько дисциплин: теоретическую информатику, компьютерные науки, уголовное и гражданское право, судебную медицину, математику, системный и схемотехнический анализ и синтез, деловое администрирование, психологию (список далеко не полон). Существует необходимость интеграции подходов к дисциплинам в области ИБ в разных странах для

адекватного международного сотрудничества. Совсем недавно правительства России и США провели активную совместную работу по решению этой проблемы.

Образовательные системы двух стран имеют свои уникальные достоинства. Российское образование, базирующееся на лучших традициях советской высшей школы, имеет преимущество в фундаментальных физико-математических науках, признаваемое США. В то же время имеется определенное преимущество США в области прикладных наук и деловом администрировании. Одновременно существуют идеологические различия у людей, имеющих дело с понятиями конфиденциальности и информационной безопасности. Совместная деятельность с целью разработки учебных программ по России и Соединенным Штатам поможет в привлечении сильных сторон этих двух стран при подготовке специалистов по информационной безопасности и окажет помощь в сокращении идеологических различий.

Различия в вопросах коммуникации, языка, ресурсов и культуры, создают очевидные препятствия для такой деятельности. Однако эти барьеры преодолимы. Официальное соглашение, подписанное министрами образования США и РФ, привело к разработке совместного проекта, в котором участвуют МГТУ имени Н. Э. Баумана и Университет штата Нью-Йорк (State University of New York).

В рамках проекта, стартовавшего в ноябре 2010 г., предусмотрена совместная разработка ряда электронных курсов дистанционного образования в области ИБ; прошедшим обучение предполагается выдавать соответствующий сертификат, признанный двумя странами. В настоящее время происходит активный обмен знаниями между двумя университетами, идет совместная разработка учебных программ и контента в формате дистанционного обучения. Студенты из двух стран будут заниматься совместно с использованием работы через интернет-форумы. Они также примут участие в летней 4-недельной практике по изучению языка для студентов МГТУ в Олбани, а для студентов SUNY в Москве.

Предметом нашего рассмотрения является информационная безопасность автоматизированных систем. Под автоматизированной системой обработки информации (АС) [1] мы будем понимать совокупность следующих объектов:

1) средств вычислительной техники;
2) программного обеспечения;
3) каналов связи;
4) информации на различных носителях;
5) персонала и пользователей системы.

Информационная безопасность АС рассматривается как состояние системы, при котором:

1. Система способна противостоять дестабилизирующему воздействию внутренних и внешних угроз.

2. Функционирование и сам факт наличия системы не создают угроз для внешней среды и для элементов самой системы.

На практике информационная безопасность обычно рассматривается как совокупность следующих трех базовых свойств защищаемой информации [2]:

− **конфиденциальность**, означающая, что доступ к информации могут получить только легальные пользователи;

− **целостность**, означающая, что во-первых, защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями, а во-вторых, информация внутренне непротиворечива и (если данное свойство применимо) отражает реальное положение вещей;

− **доступность**, гарантирующая беспрепятственный доступ к защищаемой информации для законных пользователей.

Деятельность, направленную на обеспечение информационной безопасности, принято называть **защитой информации**. Методы обеспечения информационной безопасности весьма разнообразны.

Сервисы сетевой безопасности представляют собой механизмы защиты информации, обрабатываемой в распределенных вычислительных системах и сетях. Инженерно-технические методы ставят своей целью обеспечение защиты информации от утечки по техническим каналам – например, за счет перехвата электромагнитного излучения или речевой информации. Правовые и организационные методы защиты информации создают нормативную базу для организации различного рода деятельности, связанной с обеспечением информационной безопасности.

Курс «Теоретические методы обеспечения информационной безопасности» [3], в свою очередь, решают две основные задачи. Первая из них – это формализация разного рода процессов, связанных с обеспечением информационной безопасности. Так, например, формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе – а значит, гарантировать выполнение требуемых свойств безопасности. Отсюда непосредственно вытекает вторая задача – строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищенности. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.

Специалисты в области информационной безопасности США и России поддерживают и создают новые базовые оценочные и управленческие стандарты, используемые при проектировании, реализации, оценке, поддержке, управлении и эксплуатации автоматизированных систем. Современные стандарты являются бесценным источником оптимальных и заведомо эффективных решений, а потому их использование во многих случаях может чрезвычайно упростить практическую деятельность специалиста в области информационной безопасности. Тот факт, что в России стандартизация в данной области идет по пути поэтапного принятия международных стандартов, не может не сказываться самым позитивным образом на развитии отрасли в целом.

ЛИТЕРАТУРА

1. *Девянин, П. Н.* Теоретические основы компьютерной безопасности / П. Н. Девятин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. М.: Радио и связь. 2000.

2. *Ronald, R. Krutz.* The CISSP Prep Guide–Mastering the Ten Domains of Computer Security / Russell Dean Vines. – John Wiley and Sons, Inc., 2001.

3. *Грушо, А. А.* Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. М.: Яхтсмен, 1996.

4. *Ховард, М.* Защищенный код / М. Ховард, Д. Лебланк. М.: Русская редакция, 2004.