Т. А. Ми шов а, С. А. Охрименко, С. А. Тутунару, К. Ф. Склифос

Молдавская экономическая академия г. Кишинев, Молдова

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УСПЕШНОГО ВЕДЕНИЯ БИЗНЕСА

Приведен анализ опыта, накопленного в лаборатории информационной безопасности Молдавской экономической академии по подготовке специалистов в области информационной безопасности.

The present report provides the analysis of the experience which has been accumulated in the Laboratory of Information Security at Academy of Economic Studies of the Republic of Moldova during the specialists training in the of information security field.

Развитие информационных и коммуникационных технологий радикальным образом изменило повседневную жизнь, превратилось в доминирующий фактор устойчивого развития общества. Новые технологии обеспечивают сбор, обработку и хранение огромных объемов самой разнообразной информации (технической, научной, медицинской и др.). Все это приводит к необходимости построения системы информационной безопасности, поскольку существующие информационные системы небезопасны не из-за их технического и технологического несовершенства, а из-за ошибок при использовании технологий. Это означает, что процедуры безопасности должны быть интегрированы не только в технологические операции, но и в деятельность самих информационных систем. При этом проблемы информационной безопасности приобрели принципиальное значение не только для общества и государства, но и для личности. В большинстве стран информационная безопасность рассматривается как составная часть национальной безопасности, наравне с такими составляющими, как энергетическая, продовольственная и др., требует обеспечения безопасности производственно-технических и социально-экономических систем, формируемых обществом.

В связи с этим повышенное внимание привлекает проблема кадрового обеспечения информационной безопасности. Кроме того, повсеместно ощущается потребность увеличения численности профессионалов в данной предметной области на базе непрерывного совершенствования образовательного процесса, поскольку теория и практика защиты информационных ресурсов непрерывно и интенсивно развиваются. Особые требования выдвигаются со стороны малого и среднего бизнеса, поскольку их деятельность базируется на процессах сбора, обработки и анализа рыночной информации, формировании портфелей заказов и т. д. Владельцы предприятий малого и среднего бизнеса требуют разработки комплекса организационно-технических мероприятий, обеспечивающих целостность, доступность и конфиденциальность информации.

В практике подготовки специалистов по информационной безопасности выделяются два основных направления. Первое, академическое, предусматривает получение высшего образования по следующим ступеням: бакалавр, магистр, доктор и предполагает изучение разнообразных дисциплин, ознакомление с научно-техническими достижениями и, в конечном счете, формирование специалиста с высоким уровнем теоретических знаний и практических навыков.

Вторым направлением подготовки специалистов являются курсы ведущих компаний, специализирующихся в области информационных технологий, которые предполагают приобретение достаточных знаний и их совершенствование в целях соответствия требованиям уровня развития информационных технологий и международным и национальным стандартам.

К сожалению, в Республике Молдова в номенклатуре специальностей отсутствует направление «Информационная безопасность», хотя государственные и коммерческие информационные системы остро нуждаются в подобных специалистах, способных должным образом защитить информационные ресурсы от несанкционированного доступа и использования.

Для студентов специальности «Экономическая кибернетика» предложен специализированный курс «Информационная безопасность», предусматривающий проведение лекций и лабораторных занятий.

Технологической базой для проведения лабораторных занятий выбрана платформа Moodle, которая обеспечивает выполнение следующих функций:

- проведение удаленной идентификации и аутентификации пользователей;
- дистанционную работу в пользовательском режиме;
- использование разнообразной справочной информации:
- создание прототипа системы электронного документооборота;
- организацию форума для участников;

• контроль знаний студентов.

Для студентов экономических специальностей, таких как «Маркетинг» и «Менеджмент», предусмотрено изучение специальной темы, в которую включено рассмотрение комплекса вопросов, характеризующих основы информационной безопасности.

В результате изучения специализированного курса специалист должен:

• знать правовые основы защиты информации, стандарты и модели безопасности, владеть организационными, техническими, программными методами защиты информации в современных информационных системах, и сетях, методами идентификации пользователей, методами защиты ресурсов от программных злоупотреблений, инфраструктурой систем, построенных с использованием публичных и секретных ключей;

• уметь применять на практике полученные знания об известных методах и средствах информационной безопасности, проводить их сравнительный анализ и выбор соответствующих средств и методов, оценивать уровень защиты информационных ресурсов;

• иметь представление об основных направлениях и перспективах развития методов и средств информационной безопасности.

Программа подготовки должна включать следующие основные разделы:

1) правовое обеспечение информационной безопасности;
2) организация системы информационной безопасности;
3) анализ угроз и оценка риска;
4) стандарты и метрики информационной безопасности;
5) разработка организационно-распорядительной документации по защите информации.

Правовое обеспечение определяет и регламентирует отношения, возникающие при сборе, передаче, обработке, накоплении, хранении, актуализации, купле и продаже информации, возникающие в процессе создания, внедрения и эксплуатации информационных систем, других систем обработки и передачи информации.

В первую очередь, тщательному изучению подлежат международные и национальные законодательные акты, регламентирующие отношения в области информационных и коммуникационных технологий.

При изучении основ построения и функционирования системы информационной безопасности основное внимание должно быть уделено следующим вопросам:

• *политика* (набор формальных правил, регламентирующих функционирование механизма информационной безопасности);

• *идентификация* (определение каждого участника информационного взаимодействия);

• *аутентификация* (обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно);

• *контроль доступа* (создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам);

• *авторизация* (формирование профиля прав для конкретного участника процесса информационного обмена);

• *аудит и мониторинг* (отслеживание событий, происходящих в процессе обмена информацией (аудит предполагает анализ событий постфактум, а мониторинг реализуется в режиме реального времени));

• *реагирование на инциденты* (совокупность процедур или мероприятий, выполняемых при нарушении или подозрении на нарушение информационной безопасности);

• *управление конфигурацией* (создание и поддержание среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности);

• *управление пользователями* (обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности);

• *управление рисками* (обеспечение соответствия возможных потерь от нарушения информационной безопасности);

• *обеспечение устойчивости* (поддержание среды информационного обмена в минимально работоспособном допустимом состоянии).

Анализ угроз является одним из основных и в нем должна быть представлена информация, характеризующая классификацию угроз информационной безопасности, с выделением таких признаков, как преднамеренные и случайные, по составу и последствиям, типу, целям, характеру и месту возникновения, объекту воздействия, причине возникновения и многим другим. Но основное внимание, по нашему мнению, должно быть сконцентрировано на преднамеренных угрозах. Весь спектр угроз должен рассматриваться через призму уязвимостей (технических и программных) с выходом на идентификацию и управление риском, моделирование

аварийных ситуаций, подготовку и поддержку решений. Анализ риска должен строиться с учетом моделей возможного нарушителя и его действий, а также потенциальных потерь.

Изучение материала, характеризующего стандарты и метрики информационной безопасности, предполагает следующее:

- определение целей обеспечения информационной безопасности информационных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью.

Последовательность рассмотрения данного раздела может базироваться на Международном стандарте безопасности ISO/IEC17799, BSI, COB IT и включать следующие вопросы:

- организационные меры по обеспечению безопасности;
- классификация и управление ресурсами;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и техническая поддержка вычислительных систем;
- политика безопасности;
- управление непрерывностью бизнеса;
- соответствие системы основным требованиям.

Разработка организационно-распорядительной документации является завершающим разделом, в нем интегрируются теоретические знания и практические навыки, полученные при изучении предшествующих разделов. В первую очередь, речь идет о разработке концепции обеспечения безопасности информации конкретной информационной системы, в которой описаны общие принципы и подходы к обеспечению безопасности информации и информационных ресурсов. Содержание данного документа составляет основу построения целостной системы информационной безопасности.

Таким образом, уровень теоретических знаний должен приближаться к требованиям бизнес-процессов, соответствовать запросам настоящего времени, а подготовку следует ориентировать на овладение теоретическими знаниями и практическими навыками, используемыми для преодоления кризисных ситуаций, возникающих в процессе функционирования бизнес-информационных систем..

В Молдавской экономической академии открыта лаборатория информационной безопасности, призванная решать комплекс задач, основной из которых является активизация научно-исследовательской деятельности студентов, аспирантов и молодых ученых в области информационной безопасности, выбор молодых специалистов для работы с системами информационной безопасности в государственных и коммерческих структурах.

Ежегодно лаборатория информационной безопасности проводит международную конференцию и конкурс студенческих работ, посвященных исследованию проблем информационной безопасности. За прошедшее время в работе конференции принимали участие студенты и аспиранты различных вузов (Молдовы, Болгарии, Украины, Франции, Индии, США, России). В рамках данных мероприятий рассматривается следующая тематика:

- правовые основы информационной безопасности;
- формирование политики безопасности информационных систем;
- защита интеллектуальной собственности;
- организационные меры в области информационной безопасности;
- тестирование и сертификация продуктов и услуг в области информационной безопасности;
- криптографические средства защиты информации;
- оценка и управление рисками в информационных системах;
- анализ информационных угроз и средств противодействия;
- аудит безопасности информационных систем;
- экономика информационной безопасности.

Последняя тема, по нашему мнению, является на сегодняшний момент наиболее актуальной, поскольку специалисты уделяют все большее внимание вопросам экономической эффек-

тивности систем информационной безопасности. Отмечается общая тенденция роста стоимости работ по информационной безопасности, так как процессы проектирования, внедрения и эксплуатации системы информационной безопасности сопряжены с огромными затратами на программные и технические средства, требуют наличия высококвалифицированных кадров и т. д. В рамках данного направления выделяются работы, связанные с исследованием комплекса показателей экономической эффективности, разработкой экономико-математических моделей, управлением риском и др. [1; 2].

Экономика информационной безопасности, как самостоятельное научное направление, получила развитие относительно недавно. Истоками данного направления следует считать комплекс исследований и практических разработок, связанных со следующими факторами:

• процессами совершенствования организационных форм использования вычислительной техники;

• заменой вычислительной базы и переходом к использованию новых информационных и коммуникационных технологий;

• разработкой операционных систем для персональных компьютеров;

• появлением и разработкой программно-технических угроз;

• реализацией атак на информационные системы и другие.

Приведенные факторы во многом взаимосвязаны. Например, появление персональных компьютеров привело к персонализации вычислительных процессов, а это вызвало изменения в организационных формах использования не только вычислительной техники, но и организации технологических процессов сбора, регистрации, обработки и хранения информации.

Параллельно с конференцией организуется конкурс, конечной целью которого является проверка уровня знаний информационных и коммуникационных технологий. Информационный спонсор конкурса предоставляет защищенный сервер, на котором размещается специальная информация, которую необходимо отыскать и представить организационному комитету. Другими словами, после регистрации участники конкурса имеют возможность организовать атаку на удаленный (выделенный) сервер, выполнить анализ операционной среды, определить ресурсное наполнение и найти небольшой по объему текстовый файл. Как показала практика проведения данного конкурса, от его участников требуются углубленные теоретические и практические знания и навыки по таким направлениям, как операционные системы и среды, программирование, организация вычислительного процесса, безопасность информационных систем и другие.

В перспективе предусматривается открытие центра сертификации ключей для электронной цифровой подписи, которыми будут пользоваться студенты в процессе практической работы. Предусматривается разработка комплекса лабораторных работ, охватывающих практические аспекты использования цифровой подписи для передачи файлов, создание зашифрованного логического диска и т. д.

Лаборатория информационной безопасности в качестве основной цели своей деятельности видит изучение современных правовых, организационных, технических, программных и других методов и средств защиты информации. В свою очередь, основными задачами подготовки специалистов являются следующие:

• формирование современного подхода к информационной безопасности как систематической научно-практической деятельности, носящей прикладной характер;

• изучение теоретических основ, лежащих в основе управления информационной системой и ресурсами, а также информационной безопасности;

• дать представление о современных методах и средствах защиты информации;

• научить использованию распространенных программных продуктов и услуг в области информационной безопасности.

Список литературы

1. Панасенко, С. **П.** Основы криптографии для экономистов /СП. Панасенко. В. П. Батура. - М. : Финансы и статистика, 2005.

2. **Council,** C. Implication for the Future of CobiT Systems in Higher Education : Putting Critical Research and Theory Into Practice / C Council // Information Systems Control. - Vol. 1. - 2007.-P. 33-35.